



Active IQ Unified Manager文档

Active IQ Unified Manager

NetApp
October 15, 2025

目录

Active IQ Unified Manager文档	1
发行说明	2
开始使用	3
VMware 安装快速入门说明	3
系统要求	3
安装Active IQ Unified Manager	3
Linux 安装的快速入门说明	4
系统要求	4
安装Active IQ Unified Manager	4
Windows 安装快速入门说明	5
系统要求	5
安装Active IQ Unified Manager	5
在 VMware vSphere 系统上安装 Unified Manager	7
Active IQ Unified Manager简介	7
Unified Manager 服务器的功能	7
安装顺序概述	7
安装 Unified Manager 的要求	8
虚拟基础设施和硬件系统要求	8
VMware 软件和安装要求	9
支持的浏览器	10
协议和端口要求	10
完成工作表	12
安装、升级和删除 Unified Manager 软件	14
部署过程概述	15
部署 Unified Manager	15
升级 Unified Manager	19
重新启动 Unified Manager 虚拟机	21
删除 Unified Manager	21
在 Linux 系统上安装 Unified Manager	23
Active IQ Unified Manager简介	23
Unified Manager 服务器的功能	23
安装顺序概述	23
安装 Unified Manager 的要求	24
虚拟基础设施和硬件系统要求	24
Linux 软件和安装要求	25
支持的浏览器	27
协议和端口要求	28
完成工作表	30
安装、升级和删除 Unified Manager 软件	32

安装过程概述	32
设置所需的软件存储库	33
NFS 和 CIFS 共享上的 SELinux 要求	35
在 Linux 系统上安装 Unified Manager	37
在 Red Hat Enterprise Linux 上升级 Union Manager	43
安装 Unified Manager 后升级第三方产品	48
重新启动 Unified Manager	49
删除 Unified Manager	49
删除自定义 umadmin 用户和维护组	50
在 Windows 系统上安装 Unified Manager	51
Active IQ Unified Manager 简介	51
Unified Manager 服务器的功能	51
安装顺序概述	51
安装 Unified Manager 的要求	52
虚拟基础设施和硬件系统要求	52
Windows 软件和安装要求	53
支持的浏览器	55
协议和端口要求	55
完成工作表	57
安装、升级和删除 Unified Manager 软件	59
安装过程概述	59
在 Windows 上安装 Unified Manager	60
更改 JBoss 密码	63
Unified Manager 版本支持的升级路径	64
升级 Unified Manager	64
升级第三方产品	66
卸载第三方产品	67
重新启动 Unified Manager	67
卸载 Unified Manager	68
执行配置和管理任务	70
配置 Active IQ Unified Manager	70
配置序列概述	70
访问 Unified Manager Web UI	70
执行 Unified Manager Web UI 的初始设置	71
添加集群	73
配置 Unified Manager 以发送警报通知	75
更改本地用户密码	82
设置会话不活动超时	83
通过 CLI 设置会话超时	83
更改 Unified Manager 主机名	84
启用和禁用基于策略的存储管理	87

配置 Unified Manager 备份	88
管理功能设置	88
启用基于策略的存储管理	88
启用 API 网关	89
指定不活动超时	89
启用 Active IQ 门户事件	89
启用和禁用安全设置以实现合规性	90
启用和禁用脚本上传	91
添加登录横幅	91
使用维护控制台	91
维护控制台提供哪些功能	91
维护用户执行的操作	92
诊断用户功能	92
访问维护控制台	92
使用 vSphere VM 控制台访问维护控制台	93
维护控制台菜单	93
在 Windows 上更改维护用户密码	98
在 Linux 系统上更改 umadmin 密码	98
更改 Unified Manager 用于 HTTP 和 HTTPS 协议的端口	99
添加网络接口	99
向 Unified Manager 数据库目录添加磁盘空间	100
管理用户访问	103
添加用户	104
编辑用户设置	105
查看用户	105
删除用户或组	105
什么是 RBAC	106
基于角色的访问控制的作用	106
用户类型的定义	106
用户角色的定义	107
Unified Manager 用户角色和功能	108
管理 SAML 身份验证设置	109
身份提供者要求	109
启用 SAML 身份验证	110
更改用于 SAML 身份验证的身份提供者	111
Unified Manager 安全证书更改后更新 SAML 身份验证设置	112
禁用 SAML 身份验证	113
从维护控制台禁用 SAML 身份验证	113
SAML 身份验证页面	114
管理身份验证	115
编辑身份验证服务器	115

删除身份验证服务器	115
通过 Active Directory 或 OpenLDAP 执行的身份验证	116
审核日志记录	116
远程身份验证页面	118
管理安全证书	121
查看HTTPS安全证书	121
下载 HTTPS 证书签名请求	122
安装 CA 签名并返回的 HTTPS 证书	122
安装使用外部工具生成的 HTTPS 证书	123
证书管理的页面描述	125
监视和管理存储	128
Active IQ Unified Manager简介	128
Active IQ Unified Manager健康监控简介	128
Active IQ Unified Manager性能监控简介	129
使用 Unified Manager REST API	130
Unified Manager 服务器的功能	130
了解用户界面	131
典型窗口布局	131
窗口布局自定义	132
使用 Unified Manager 帮助	133
为您最喜欢的帮助主题添加书签	133
搜索存储对象	133
将存储数据导出为报告	135
过滤库存页面内容	136
从通知铃查看活动事件	137
从仪表板监控和管理集群	137
信息板页面	138
直接从 Unified Manager 管理ONTAP问题或功能	140
管理集群	146
集群发现过程的工作原理	146
查看监控集群列表	147
添加集群	147
编辑集群	149
删除集群	150
重新发现集群	151
监控 VMware 虚拟基础架构	151
不支持的内容	153
查看并添加 vCenter Server	154
移除 vCenter Server	155
监控虚拟机	156
查看灾难恢复设置中的虚拟基础架构	157

预配和管理工作负载	159
工作负载概述	160
性能服务级别	165
管理存储效率策略	170
管理和监控MetroCluster配置	172
切换和切回期间的卷行为	172
通过 FC 配置的MetroCluster的集群连接状态定义	174
MetroCluster over FC 的数据镜像状态定义	175
监控MetroCluster配置	176
监控MetroCluster复制	178
管理配额	179
什么是配额限制	179
查看用户和用户组配额	179
创建规则以生成电子邮件地址	180
为用户和用户组配额创建电子邮件通知格式	180
编辑用户和组配额电子邮件地址	181
详细了解配额	181
配额对话框的说明	182
故障排除	185
向 Unified Manager 数据库目录添加磁盘空间	185
修改性能统计收集间隔	188
更改 Unified Manager 保留事件和性能数据的时间长度	189
未知的身份验证错误	190
未找到用户	190
使用其他身份验证服务添加 LDAP 的问题	190
Windows 系统上的NetApp可管理性 SDK 日志轮换问题	191
管理事件和警报	192
管理活动	192
什么是 Active IQ 平台事件	192
什么是事件管理系统事件	192
收到事件时会发生什么情况	197
查看活动和活动详情	198
查看未分配的事件	199
确认并解决事件	199
将事件分配给特定用户	200
禁用不需要的事件	201
使用 Unified Manager 自动修复功能解决问题	201
启用和禁用Active IQ事件报告	202
上传新的Active IQ规则文件	203
如何生成 Active IQ 平台事件	203
解决Active IQ平台事件	204

配置事件保留设置	205
Unified Manager 维护窗口是什么	205
管理主机系统资源事件	207
了解更多活动信息	208
事件和严重性类型列表	212
事件窗口和对话框说明	263
管理警报	274
什么是警报	274
警报电子邮件中包含哪些信息	275
添加警报	275
添加性能事件警报	278
测试警报	278
启用和禁用已解决和已过时事件的警报	279
排除灾难恢复目标卷生成警报	279
查看警报	280
编辑警报	280
删除警报	281
警报窗口和对话框的描述	281
管理脚本	287
脚本如何与警报结合使用	287
添加脚本	288
删除脚本	289
测试脚本执行	289
支持的 Unified Manager CLI 命令	290
脚本窗口和对话框的描述	295
监控和管理集群性能	297
Active IQ Unified Manager性能监控简介	297
Unified Manager 性能监控功能	297
用于管理存储系统性能的 Unified Manager 界面	298
集群配置和性能数据收集活动	298
什么是数据连续性收集周期	299
时间戳在收集的数据和事件中意味着什么	300
在 Unified Manager GUI 中导航性能工作流程	300
登录用户界面	300
图形界面和导航路径	301
搜索存储对象	306
过滤库存页面内容	307
从仪表板监控集群性能	308
了解仪表板上的性能面板	309
性能横幅消息和说明	309
修改性能统计收集间隔	310

使用工作负载分析器排除工作负载故障	310
工作负载分析器显示哪些数据	311
我什么时候应该使用工作负载分析器	312
使用工作负载分析器	312
从性能集群登录页面监控集群性能	313
了解性能集群登陆页面	313
性能集群登陆页面	314
使用“性能清单”页面监控性能	317
查看所有存储对象的性能清单页面	318
优化绩效清单页面内容	323
了解 Unified Manager 将数据分层到云的建议	325
使用性能资源管理器页面监视性能	326
了解根对象	326
应用过滤来减少网格中相关对象的列表	326
指定相关对象的时间范围	326
定义用于比较图表的相关对象列表	328
了解计数器图表	329
性能计数器图表的类型	329
选择要显示的性能图表	331
展开计数器图表窗格	332
将计数器图表焦点更改为较短的时间段	332
在事件时间线中查看事件详细信息	333
计数器图表缩放视图	333
按集群组件查看卷延迟	335
按协议查看 SVM IOPS 流量	336
查看卷和 LUN 延迟图表以验证性能保证	336
查看所有 SAN 阵列集群的性能	337
根据仅驻留在本地节点上的工作负载查看节点 IOPS	337
对象登陆页面的组件	338
使用 QoS 策略组信息管理性能	343
存储 QoS 如何控制工作负载吞吐量	343
查看所有集群上可用的所有 QoS 策略组	344
查看同一 QoS 策略组中的卷或 LUN	344
查看应用于特定卷或 LUN 的 QoS 策略组设置	345
查看性能图表以比较同一 QoS 策略组中的卷或 LUN	345
不同类型的 QoS 策略如何在吞吐量图表中显示	346
在性能资源管理器中查看工作负载 QoS 最小和最大设置	347
使用性能容量和可用 IOPS 信息管理性能	348
所用性能容量	348
性能容量使用值的含义	349
可用的 IOPS 是什么	350

查看节点和聚合性能容量使用值	351
查看节点并聚合可用 IOPS 值	352
查看性能容量计数器图表以识别问题	353
性能容量使用性能阈值条件	354
使用性能容量使用计数器来管理性能	355
了解并使用节点故障转移规划页面	355
使用节点故障转移计划页面确定纠正措施	355
节点故障转移计划页面的组件	356
将阈值策略与节点故障转移计划页面结合使用	357
使用性能容量使用明细图表进行故障转移规划	357
收集数据并监控工作负载性能	359
Unified Manager 监控的工作负载类型	359
工作负载性能测量值	360
预期的表现范围是多少	361
延迟预测如何用于性能分析	362
Unified Manager 如何使用工作负载延迟来识别性能问题	363
集群操作如何影响工作负载延迟	363
MetroCluster配置的性能监控	364
了解性能事件和警报	365
性能事件源	365
性能事件严重性类型	366
Unified Manager 检测到的配置更改	366
系统定义的性能阈值策略的类型	367
性能事件分析和通知	369
Unified Manager 如何确定事件对性能的影响	371
集群组件及其争用的原因	371
性能事件中涉及的工作负载的角色	373
管理绩效阈值	373
用户定义的性能阈值策略如何工作	374
当违反绩效阈值策略时会发生什么	375
可以使用阈值跟踪哪些性能计数器	375
哪些对象和计数器可以组合使用阈值策略	377
创建用户定义的性能阈值策略	378
为存储对象分配性能阈值策略	379
查看性能阈值策略	380
编辑用户定义的性能阈值策略	380
从存储对象中删除性能阈值策略	381
当性能阈值策略改变时会发生什么	381
当对象移动时性能阈值策略会发生什么变化	382
分析性能事件	383
显示有关性能事件的信息	383

根据用户定义的性能阈值分析事件	383
根据系统定义的性能阈值分析事件	384
根据动态性能阈值分析事件	389
解决性能事件	395
确认延迟在预期范围内	395
审查配置更改对工作负载性能的影响	396
从客户端提高工作负载性能的选项	396
检查客户端或网络问题	396
验证 QoS 策略组中的其他卷是否具有异常高的活动	396
移动逻辑接口 (LIF)	397
在不太繁忙的时间运行存储效率操作	397
添加磁盘并重新分配数据	398
在节点上启用闪存如何提高工作负载性能	398
在存储聚合上启用 Flash Pool 可以如何提高工作负载性能	399
MetroCluster配置健康检查	399
MetroCluster配置验证	399
将工作负载移至不同的聚合	400
将工作负载移至其他节点	401
将工作负载移动到不同节点上的聚合	402
将工作负载移至不同 HA 对中的节点	404
将工作负载移至不同 HA 对中的另一个节点	405
使用 QoS 策略设置来优先处理此节点上的工作	407
删除非活动卷和 LUN	407
添加磁盘并执行聚合布局重建	408
在 Unified Manager 服务器和外部数据提供商之间建立连接	408
可以发送到外部服务器的性能数据	408
设置 Graphite 以从 Unified Manager 接收性能数据	409
配置从 Unified Manager 服务器到外部数据提供商的连接	410
监视和管理集群健康状况	413
Active IQ Unified Manager健康监控简介	413
物理和逻辑容量	413
容量测量单位	413
Unified Manager 运行状况监控功能	414
用于管理存储系统健康状况的 Unified Manager 界面	415
管理和监控集群和集群对象健康状况	415
了解集群监控	415
查看集群列表及详情	417
检查MetroCluster配置中集群的运行状况	417
查看所有 SAN 阵列集群的健康和容量状态	419
查看节点列表及详情	420
生成合同续签的硬件清单报告	420

查看存储虚拟机列表和详细信息	421
查看汇总列表和详细信息	421
查看FabricPool容量信息	422
查看存储池详细信息	423
查看卷列表和详细信息	424
查看有关 NFS 共享的详细信息	424
查看有关 SMB/CIFS 共享的详细信息	425
查看 Snapshot 副本列表	426
删除 Snapshot 副本	426
计算 Snapshot 副本的可回收空间	427
集群对象窗口和对话框说明	428
常见的 Unified Manager 运行状况工作流程和任务	428
监控和排除数据可用性故障	429
解决容量问题	435
管理健康阈值	436
管理集群安全目标	440
管理备份和恢复操作	450
管理脚本	464
管理和监控群组	466
使用注释确定存储对象事件的优先级	474
通过 Web UI 和维护控制台发送支持包	482
与多个工作流程相关的任务和消息	489
保护和恢复数据	541
创建、监控和排除保护关系故障	541
SnapMirror保护类型	541
在 Unified Manager 中设置保护关系	542
执行保护关系故障转移和故障回复	544
解决保护作业失败	548
解决滞后问题	551
管理和监控保护关系	552
查看卷保护状态	552
查看卷保护关系	554
监控一致性组关系中的 LUN	555
从“Health: All Volumes”视图创建SnapVault保护关系	555
从卷/运行状况详细信息页面创建SnapVault保护关系	556
从“Health: All Volumes”视图创建SnapMirror保护关系	557
从卷/运行状况详细信息页面创建SnapMirror保护关系	558
创建具有版本灵活复制的SnapMirror关系	559
使用备份选项创建具有版本灵活复制的SnapMirror关系	560
配置目标效率设置	561
创建SnapMirror和SnapVault计划	562

创建级联或扇出关系，以扩展现有保护关系的保护	562
从卷关系页面编辑保护关系	563
从卷/健康详情页面编辑保护关系	563
创建SnapMirror策略以最大程度提高传输效率	564
创建SnapVault策略以最大程度提高传输效率	564
从卷关系页面中止活动数据保护传输	565
从卷/健康详情页面中止活动数据保护传输	565
从卷关系页面停止保护关系	566
从卷/健康详情页面暂停保护关系	567
从卷关系页面断开SnapMirror关系	568
从卷关系页面中删除保护关系	568
从卷关系页面恢复静止关系上的计划传输	568
从卷/健康详情页面恢复已暂停关系的预定传输	569
从卷关系页面初始化或更新保护关系	570
从卷/健康详情页面初始化或更新保护关系	570
从卷关系页面重新同步保护关系	571
从“卷关系”页面反向保护关系	572
使用卷和卷/健康详情页面恢复数据	573
什么是资源池	574
创建资源池	574
编辑资源池	575
查看资源池清单	575
添加资源池成员	575
从资源池中移除聚合	576
删除资源池	577
监控存储虚拟机灾难恢复保护关系	577
了解存储虚拟机关联	579
支持存储服务的 SVM 和资源池要求	581
什么是作业	581
监控作业	581
查看职位详情	582
中止作业	582
重试失败的保护作业	582
保护关系窗口和对话框说明	583
生成自定义报告	623
统一管理器报告	623
生成报告的接入点	623
了解报告	625
了解视图和报告关系	625
报告类型	626
报告限制	627

使用报告	628
报告工作流程	628
报告快速入门	628
搜索计划报告	631
自定义报告	632
下载报告	635
计划报告	635
安排报告	635
管理报告时间表	637
自定义报告示例	639
自定义集群存储报告	640
自定义聚合容量报告	642
自定义卷容量报告	644
自定义 Qtree 容量报告	647
自定义 NFS 共享报告	648
自定义存储虚拟机报告	649
自定义数量关系报告	650
自定义卷性能报告	654
Microsoft Excel 报告示例	654
创建报告以显示聚合容量表和图表	655
创建报告以显示总计与可用容量图表	657
创建报告以查看可用卷容量图表	661
创建报告以查看具有最多可用 IOPS 的聚合	663
使用 REST API 管理存储	665
开始使用Active IQ Unified Manager REST API	665
此内容的受众	665
Active IQ Unified Manager API 访问和类别	665
Active IQ Unified Manager中提供的 REST 服务	666
Active IQ Unified Manager中的 API 版本	667
ONTAP中的存储资源	667
Active IQ Unified Manager中的 REST API 访问和身份验证	668
身份验证	671
Active IQ Unified Manager中使用的 HTTP 状态代码	671
使用Active IQ Unified Manager API 的建议	672
故障排除日志	672
Job对象异步进程	673
你好 API 服务器	674
Unified Manager REST API	678
使用 API 管理数据中心内的存储对象	678
通过代理访问访问ONTAP API	682
使用 API 执行管理任务	685

使用 API 管理用户	686
使用 API 查看性能指标	686
查看作业和系统详细信息	694
使用 API 管理事件和警报	695
使用 API 管理工作负载	697
存储管理的常见 API 工作流程	705
了解工作流中使用的 API 调用	705
使用 API 确定聚合中的空间问题	705
使用事件 API 确定存储对象中的问题	707
使用网关 API 对ONTAP卷进行故障排除	708
用于工作负载管理的 API 工作流	711
法律声明	736
版权	736
商标	736
专利	736
隐私政策	736
开源	736

Active IQ Unified Manager文档

发行说明

提供Active IQ Unified Manager 9.16 的新功能、限制和已知问题的摘要。

欲了解更多信息，请参阅 "[Active IQ Unified Manager发行说明](#)"。

开始使用

VMware 安装快速入门说明

您可以下载`.tar`包含根证书的文件`README`文件，以及`OVA`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，请参阅["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`.tar`包含根证书的文件`README`文件，以及`OVA`文件。
2. 将文件保存到 vSphere Client 可以访问的本地目录或网络目录。
3. 在下载的目录中`.tar`文件，输入`tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz`命令。+ 必需的`OVA`文件、根证书和`README`文件解压到目标目录。

验证完整性

您可以验证`OVA`按照提供的步骤`README`文件。

安装 Unified Manager

1. 在 vSphere Client 中，单击“文件”>“部署 OVF 模板”。
2. 找到 OVA 文件并使用向导在 ESXi 服务器上部署虚拟设备。
3. 在“评论详情”页面的“发布者”部分中，消息 Entrust Code Signing - OVCS2 (Trusted certificate) 确认下载的完整性`OVA`文件。对于消息`Entrust Code Signing - OVCS2 (Invalid certificate)`，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，根据要执行的安装类型填充所需的字段：
 - 对于静态配置，请在所有字段中输入所需的信息。不需要添加“辅助 DNS”字段的信息。
 - 对于使用 IPv4 的 DHCP，请勿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。不要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”选项卡可查看初始启动过程。

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。

Linux 安装的快速入门说明

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 版本，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”基础环境进行安装
- RAM：12 GB，CPU：总计 9572 MHz
- 可用磁盘空间：100 GB 磁盘空间 `/opt/netapp/data`` 目录，根分区中 50 GB。对于单独安装 `/opt`` 和 `/var/log`` 目录，确保 `/opt`` 有 15 GB，`/var/log`` 有 16 GB，并且 `/tmp`` 有 10 GB 的可用空间。

有关详细的系统要求以及在安全站点安装产品的信息，请参阅["安装 Unified Manager 的要求"](#)以及["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

运行以下命令验证安装程序包的完整性：

- 跑步 ``openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>`` 使用代码签名证书中的公钥创建文件。
- 跑步 ``openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip`` 验证安装程序包上的签名。

验证存储库配置

配置 Red Hat Enterprise Linux 存储库的过程是特定于站点的。您可以使用 ``pre_install_check.sh`` 安装包中包含的脚本来验证您的操作系统的配置。如果您的系统已连接到互联网，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` 实用程序来安装软件 and 任何相关软件。由于 Red Hat Enterprise Linux 的映像各不相同，因此安装的软件包取决于映像中存在的软件。这 `yum` 实用程序确定安装所依赖的软件包。如果您需要有关依赖软件包的更多信息，请参阅["Linux 软件和安装要求"](#)。

要安装 Unified Manager，请以 root 用户身份或使用以下命令运行 `sudo`，从安装文件解压的目录中：

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

或

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

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 `README` 有关端口 443 限制的更多信息，请参阅软件附带的文件。

Windows 安装快速入门说明

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

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：100 GB 磁盘空间用于安装目录，50 GB 磁盘空间用于 MySQL 数据目录

有关详细的系统要求，请参阅["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 会根据需要安装其他第三方软件包。有关依赖软件包的更多信息，请参阅["Windows 软件和安装要求"](#)。

1. 使用默认本地管理员帐户登录 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 根密码。
5. 按照其余提示完成安装。
6. 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

Active IQ Unified Manager简介

Active IQ Unified Manager（以前称为OnCommand Unified Manager）使您能够从单一界面监控和管理ONTAP存储系统的运行状况和性能。您可以在 Linux 服务器、Windows 服务器上部署 Unified Manager，也可以将其作为虚拟设备部署在 VMware 主机上。

完成安装并添加要管理的集群后，Unified Manager 将提供一个图形界面，显示受监控存储系统的容量、可用性、保护和性能状态。

相关信息

["NetApp 互操作性表工具"](#)

Unified Manager 服务器的功能

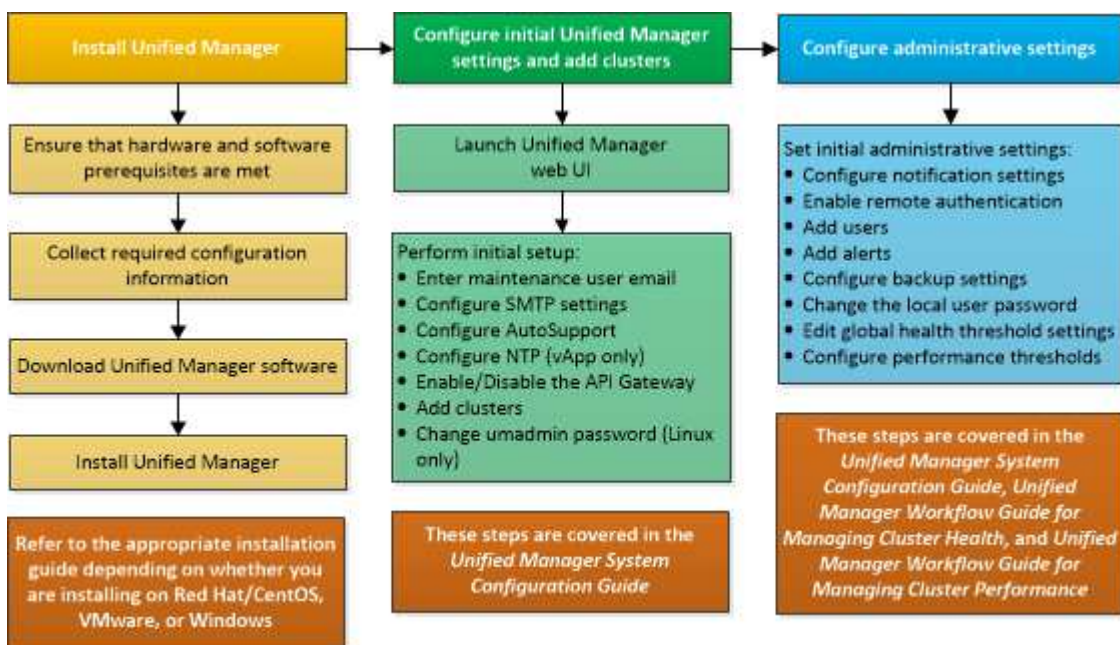
Unified Manager 服务器基础架构由数据收集单元、数据库和应用程序服务器组成。它提供发现、监控、基于角色的访问控制 (RBAC)、审计和日志记录等基础设施服务。

Unified Manager 收集集群信息，将数据存储在数据库中，并分析数据以查看是否存在任何集群问题。

安装顺序概述

安装工作流程描述了您在使用 Unified Manager 之前必须执行的任务。

这些部分描述了下面工作流程中显示的每个项目。



安装 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。如果您需要对 Unified Manager 服务器应用任何安全措施，则应该对安装 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 服务器的更多详细信息，请参阅知识库文章。

["适用于集群模式Data ONTAP的Active IQ Unified Manager的安全措施的可支持性"](#)

相关信息

有关详细信息，请参阅 ["NetApp 互操作性表工具"](#)

虚拟基础设施和硬件系统要求

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。

下表显示了内存、CPU 和磁盘空间资源的推荐值。这些值已经过限定，因此 Unified Manager 满足可接受的性能水平。

硬件配置	推荐设置
RAM	12 GB（最低要求 8 GB）
处理器	4 个 CPU
CPU 循环容量	总计 9572 MHz（最低要求 9572 MHz）
可用磁盘空间	• 5 GB（精简配置） • 152 GB（厚置备）

Unified Manager 可以安装在具有少量内存的系统上，但建议使用 12 GB RAM，以确保有足够的内存来实现最佳性能，并且随着配置的增长，系统可以容纳额外的集群和存储对象。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，膨胀）。

此外，在安装第二个 Unified Manager 实例之前，单个 Unified Manager 实例可以监控的节点数量是有限制的。有关详细信息，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。由于整体主机利用率而竞争不可用的 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 备份和恢复功能，请分配额外的容量，以便“数据”目录或磁盘有 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 主机系统外部至少具有 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以能够成功的方式进行配置 `ping` 主机本身的主机名。如果是 IPv6 配置，您应该验证 `ping6` 主机名是否成功，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。如果您在部署期间为网络配置了静态 IP 地址，那么您就为网络主机指定了一个名称。如果您使用 DHCP 配置网络，则应该从 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。

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 12 (bookworm)。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，请参阅 VMware 文档。

支持以下版本的 vSphere：

- VMware vCenter Server 7.0 和 8.0

请参阅互操作性矩阵以获取受支持的 ESXi 版本的完整和最新列表。

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

为了确保虚拟设备正常运行，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错误。

安装要求

支持 Unified Manager 虚拟设备的 VMware High Availability。

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

如果由于资源不足导致使用启用高可用性的环境进行部署失败，则可能需要通过禁用虚拟机重启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补丁会在 VMware vSphere 系统上自动安装或升级。由于 Unified Manager 安装和升级过程控制这些组件，因此您不应尝试独立安装或升级任何第三方组件。

支持的浏览器

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

互操作性矩阵列出了受支持的浏览器版本。

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

对于所有浏览器，禁用弹出窗口阻止程序可确保软件功能正常显示。

如果您计划配置 Unified Manager 进行 SAML 身份验证，以便身份提供商 (IdP) 可以对用户进行身份验证，那么您还应该检查 IdP 支持的浏览器列表。

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。

与 Unified Manager 服务器的连接

在典型安装中，连接到 Unified Manager Web UI 时无需指定端口号，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	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	用于安全访问 Unified Manager Web UI 或进行 API 调用；API 调用只能使用 HTTPS 进行。
维护控制台	SSH/SFTP	22	用于访问维护控制台和检索支持包。
Linux 命令行	SSH/SFTP	22	用于访问 Red Hat Enterprise Linux 命令行并检索支持包。

接口	协议	端口	描述
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。
休息	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	通过 TCP 的 WebSocket	56080	用于在此端口上侦听从ONTAP（云代理）接收的消息。
AMQP QPID 代理	通过 TCP 的 WebSocket	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 仅限于本地主机。这不会影响任何升级方案，因为之前的配置会保留。可以修改此配置，并且可以使用 `Control access to MySQL port 3306` 维护控制台上的选项。有关信息，请参阅["附加菜单选项"](#)。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，请参阅["维护控制台菜单"](#)。

来自 Unified Manager 服务器的连接

您应该配置防火墙以打开端口，以便 Unified Manager 服务器与托管存储系统、服务器和其他组件之间进行通信。如果端口未打开，则通信失败。

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

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	描述
存储系统	HTTPS	443/TCP	用于监控和管理存储系统。  如果您使用此端口或任何其他端口连接到 VMware vCenter Server 或 ESXi 服务器，请确保该端口可用并且可以在安全站点连接。
存储系统	NDMP	10000/TCP	用于某些快照恢复操作。
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 陷阱发送器
SNMPv1 或 SNMPv3	162/UDP	用于发送警报通知 SNMP 陷阱。	外部数据提供服务器
TCP	2003	用于将性能数据发送到外部数据提供商，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

完成工作表

在安装和配置 Unified Manager 之前，您应该准备好有关您的环境的具体信息。您可以在

工作表中记录该信息。

Unified Manager 安装信息

安装 Unified Manager 所需的详细信息。

部署软件的系统	你的价值
ESXi 服务器 IP 地址	
主机完全限定域名	
主机 IP 地址	
网络掩码	
网关 IP 地址	
主 DNS 地址	
辅助 DNS 地址	
搜索域名	
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。根据您的配置，某些值是可选的。

设置	你的价值
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）

设置	你的价值
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	
认证服务器基础可分辨名称	
身份提供商 (IdP) URL	
身份提供者 (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。

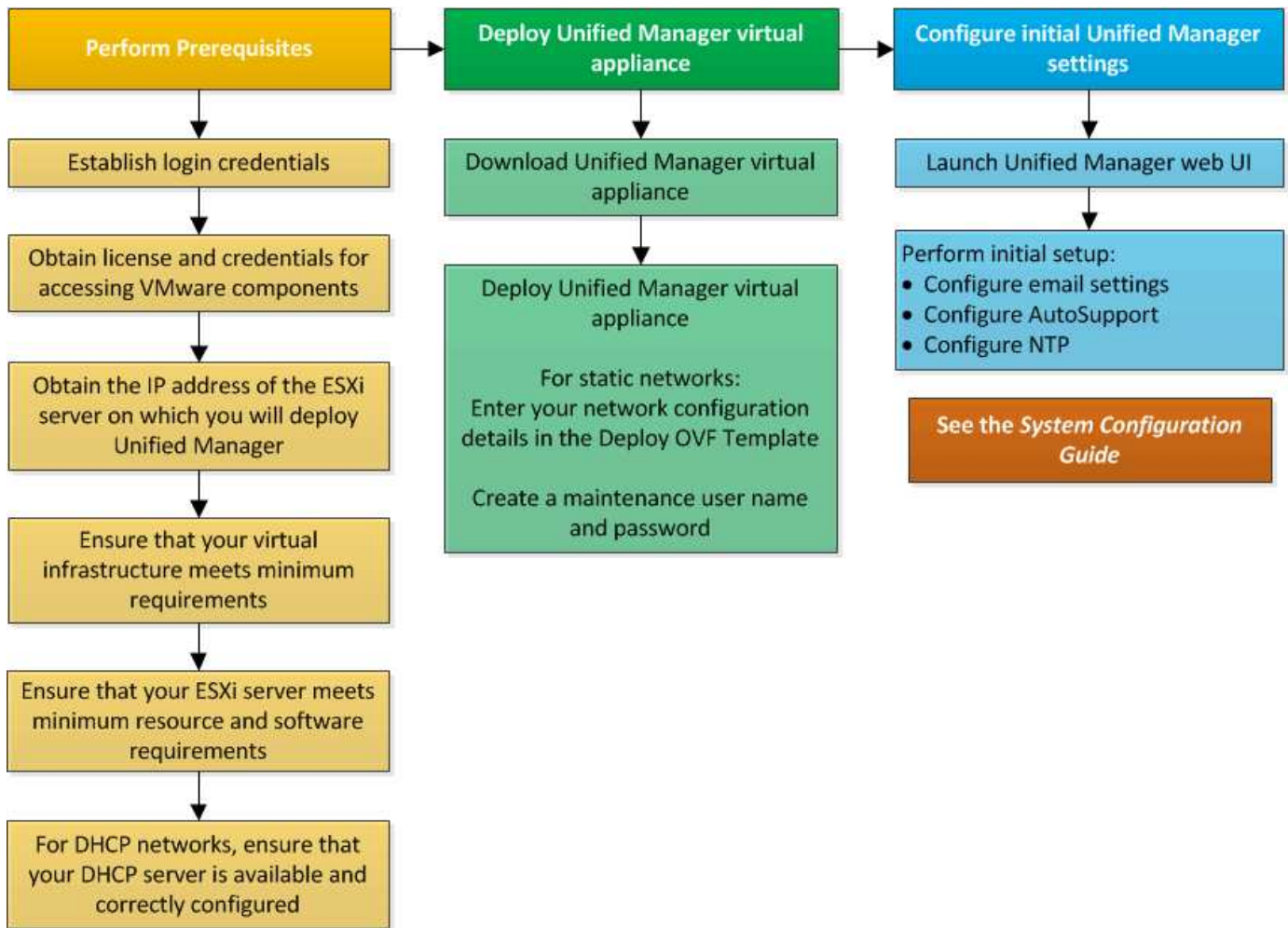
N 的簇 1	你的价值
主机名或集群管理 IP 地址	
ONTAP 管理员用户名  必须为管理员分配“admin”角色。	
ONTAP 管理员密码	
协议	HTTPS

安装、升级和删除 Unified Manager 软件

在 VMware vSphere 系统上，您可以安装 Unified Manager、升级到较新版本的软件或删除 Unified Manager 虚拟设备 (vApp)。

部署过程概述

部署工作流程描述了您在使用 Unified Manager 之前必须执行的任务。



部署 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

- 您应该验证并完成部署的系统要求。

看“[系统要求](#)”。

- 确保您拥有以下信息：
 - NetApp支持站点的登录凭据
 - 用于访问 VMware vCenter Server 和 vSphere Web Client 的凭据
 - 您要部署 Unified Manager 虚拟设备的 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 作为虚拟设备部署在 VMware ESXi 服务器上。

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 已被 Open VM Tools 取代 (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. 按照以下步骤操作“[下载 Unified Manager](#)”。
2. 此外，请按照“[部署 Unified Manager 虚拟设备](#)”。

下载 Unified Manager 安装文件

从 NetApp 支持站点下载 Unified Manager 安装文件，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 `.tar` 包含根证书的文件 `README` 文件，以及 `OVA` 包含为虚拟设备配置的 Unified Manager 软件的文件。

步骤

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

["NetApp 支持站点"](#)

2. 选择所需版本的 Unified Manager 并接受最终用户许可协议 (EULA)。
3. 下载并保存 `.tar` 将 VMware vSphere 安装文件复制到 vSphere Client 可以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. 导航到您下载的目录 `.tar` 文件并在终端窗口中输入以下命令以展开 Unified Manager 包：

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

所需的 `OVA` 文件、根证书和 `README` Unified Manager 的文件解压缩到目标目录。

6. 验证完整性 `OVA` 按照提供的步骤 `README` 文件。

部署 Unified Manager 虚拟设备

下载安装文件后，您可以将 Unified Manager 部署为虚拟设备。使用 vSphere Web Client

在 ESXi 服务器上部署虚拟设备。部署虚拟设备时，会创建一个虚拟机。

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。

看["虚拟基础架构要求"](#)。

看["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。DHCP 是默认配置的。

如果使用静态网络配置，请确保 IP 地址在同一子网中不重复，并且已配置适当的 DNS 服务器条目。

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
- 您要部署 Unified Manager 虚拟设备的 ESXi 服务器的 IP 地址
- 有关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
 - 搜索域名

从 Unified Manager 9.8 开始，VMware Tools 已被 Open VM Tools 取代 (*open-vm-tools*)。您无需在安装过程中安装 VMware Tools，因为 *open-vm-tools* 包含在 Unified Manager 安装包中。

部署虚拟设备时，会生成用于 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受信任的证书的浏览器警告。

支持 Unified Manager 虚拟设备的 VMware High Availability。

步骤

1. 在 vSphere Client 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“审核详情”页面上：

- 验证发布者部分的详细信息。消息 **Entrust Code Signing - OVCS2 (Trusted certificate)** 确认下载的完整性 *OVA* 文件。+ 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”框，并在使用 DHCP 和 IPv6 寻址时将所有其他字段留空。
- 如果您想使用静态网络配置，您可以填写此页面上的字段，这些设置在部署期间应用。确保 IP 地址对于部署它的主机是唯一的、尚未被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，右键单击虚拟机，然后选择 **启动** 来启动虚拟机。



如果由于资源不足导致开机操作失败，请添加资源，然后重试安装。

4. 单击“控制台”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和城市或地区。

显示的所有日期信息均使用为 Unified Manager 配置的时区，而不管托管设备上的时区设置如何。如果您的存储系统和管理服务器配置了相同的 NTP 服务器，则它们指的是相同的时间点，即使它们看起来不同。例如，如果您使用与管理服务器配置不同时区的设备创建 Snapshot 副本，则时间戳就是管理服务器时间。

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，则应确保其配置正确。 如果您使用启用 DHCP 的网络，FQDN 和 DNS 服务器条目将自动提供给虚拟设备。如果 DHCP 未正确配置 DNS，则会自动分配主机名“UnifiedManager”并将其与安全证书关联。如果您尚未设置启用 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. 在提示符下，输入维护用户名，然后单击 **Enter**。

维护用户名应以 az 的字母开头，后跟 -、az 或 0-9 的任意组合。

8. 在提示符下，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 来执行 Unified Manager 的初始设置，如[“配置 Active IQ Unified Manager”](#)。

升级 Unified Manager

您只能将Active IQ Unified Manager从版本 9.13 或 9.14 升级到版本 9.16。

在升级过程中，Unified Manager 不可用。在升级 Unified Manager 之前，您应该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新版本的软件可用，则必须断开这两种产品的连接，然后在执行升级后建立新的 Workflow Automation 连接。如果您只对其中一个产品进行升级，则应在升级后登录工作流自动化并验证它是否仍在从 Unified Manager 获取数据。

步骤

1. 按照以下步骤操作"[下载 Unified Manager ISO 映像](#)"。
2. 此外，请按照"[升级 Unified Manager](#)"。

Unified Manager 版本支持的升级路径

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 都可以执行就地升级到更高版本。Unified Manager 升级仅限于 N-2 型号，这意味着升级只能在所有平台上的下 2 个版本内进行。例如，您只能从 Unified Manager 9.13 和 9.14 升级到 Unified Manager 9.16。

如果您运行的版本早于支持的版本，则需要先将 Unified Manager 实例升级到支持的版本之一，然后再升级到当前版本。

例如，如果您安装的版本是 Unified Manager 9.9，并且您想要升级到 Unified Manager 9.14，则请遵循一系列升级操作。

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 → 9.16

有关升级路径矩阵的更多信息，请参阅 "[知识库 \(KB\) 文章](#)"。

下载 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. 下载 `.iso` 升级映像，并将其保存到 vSphere Client 可以访问的本地目录或网络目录中。
4. 验证校验和以确保软件已正确下载。

升级 Unified Manager 虚拟设备

您可以将 Active IQ Unified Manager 虚拟设备从版本 9.13 或 9.14 升级到 9.16。

开始之前

确保以下事项：

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

看["虚拟基础架构要求"](#)。

看["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)。
- 在升级过程中，系统可能会提示您确认是否要保留以前的默认设置（将性能数据保留 13 个月）或将其更改为 6 个月。确认后，历史绩效数据将在 6 个月后清除。
- 您有以下信息：
 - 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 维护用户的凭证

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

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

步骤

1. 在 vSphere Client 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，请导航至 **Summary > Commands > Shut Down Guest**。
4. 创建 Unified Manager VM 的备份副本（例如快照或克隆）以创建应用程序一致的备份。
5. 从 vSphere Client 启动 Unified Manager VM。
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“控制台”选项卡。
10. 登录到 Unified Manager 维护控制台。
11. 在主菜单中，选择*升级*。

显示一条消息，指出 Unified Manager 在升级过程中不可用，升级完成后将恢复。

12. 类型 `y` 继续。

将显示一条警告，提醒您备份虚拟设备所在的虚拟机。

13. 类型 `y` 继续。

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

14. 按任意键继续。

您将自动退出维护控制台。

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

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

重新启动 Unified Manager 虚拟机

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

开始之前

- 虚拟设备应已启动。
- 您应该以维护用户身份登录到 Unified Manager 维护控制台。

您也可以使用 VMware 重启客户机 选项从 vSphere 重启虚拟机。参考 ["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. 从您的浏览器启动 Unified Manager Web UI，然后登录。

删除 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

- 您应该拥有访问 VMware vCenter Server 和 vSphere Web Client 的凭据。
- 应关闭 Unified Manager 服务器与工作流自动化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. 使用 Unified Manager 维护控制台验证 Unified Manager 服务器是否没有与外部数据提供商的活动连接。
2. 在 vSphere Client 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

Active IQ Unified Manager（以前称为OnCommand Unified Manager）使您能够从单一界面监控和管理ONTAP存储系统的运行状况和性能。您可以在 Linux 服务器、Windows 服务器上部署 Unified Manager，也可以将其作为虚拟设备 (vApp) 部署在 VMware 主机上。

完成安装并添加要管理的集群后，Unified Manager 将提供一个图形界面，显示受监控存储系统的容量、可用性、保护和性能状态。

相关信息

["NetApp 互操作性表工具"](#)

Unified Manager 服务器的功能

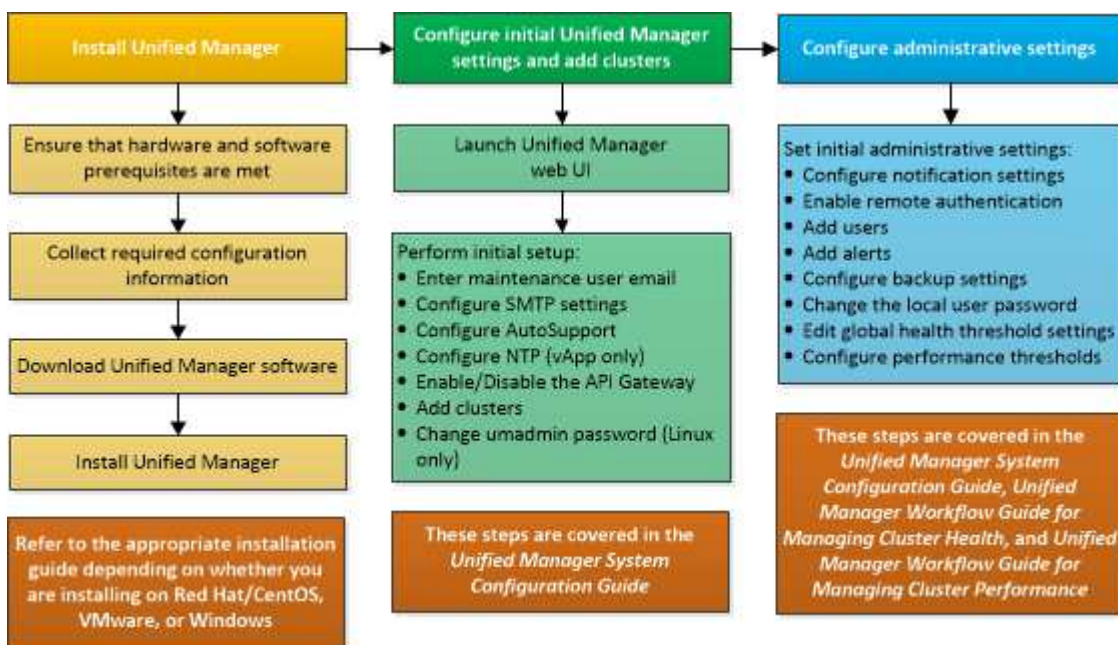
Unified Manager 服务器基础架构由数据收集单元、数据库和应用程序服务器组成。它提供发现、监控、基于角色的访问控制 (RBAC)、审计和日志记录等基础设施服务。

Unified Manager 收集集群信息，将数据存储在数据库中，并分析数据以查看是否存在任何集群问题。

安装顺序概述

安装工作流程描述了您在使用 Unified Manager 之前必须执行的任务。

这些部分描述了下面工作流程中显示的每个项目。



安装 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。如果您需要对 Unified Manager 服务器应用任何安全措施，则应该对安装 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 服务器的更多详细信息，请参阅知识库文章。

["适用于集群模式Data ONTAP的Active IQ Unified Manager的安全措施的可支持性"](#)

相关信息

["NetApp 互操作性表工具"](#)

虚拟基础设施和硬件系统要求

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。

下表显示了内存、CPU 和磁盘空间资源的推荐值。这些值已经过限定，因此 Unified Manager 满足可接受的性能水平。

硬件配置	推荐设置
RAM	12 GB（最低要求 8 GB）
处理器	4 个 CPU
CPU 循环容量	总计 9572 MHz（最低要求 9572 MHz）
可用磁盘空间	<div>150GB，容量分配如下：</div> <div> • 分配给根分区 50 GB • 分配给 <code>/opt/netapp/data`</code> 目录，安装在 LVM 驱动器上或安装在目标系统上的单独本地磁盘上</li></ul></div> <div><div></div><div>对于单独安装 <code>/opt`</code> 和 <code>/var/log`</code> 目录，确保 <code>/opt`</code> 有 15 GB 并且 <code>/var/log`</code> 有 16 GB 的可用空间。这 <code>/tmp`</code> 目录应至少有 10 GB 的可用空间。</div></div>

Unified Manager 可以安装在具有少量内存的系统上，但建议使用 12 GB RAM，以确保有足够的内存来实现最佳性能，并且随着配置的增长，系统可以容纳额外的集群和存储对象。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，膨胀）。

此外，在安装第二个 Unified Manager 实例之前，单个 Unified Manager 实例可以监控的节点数量是有限制的。

有关更多信息，请参阅《最佳实践指南》。

"技术报告 4621: 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。由于整体主机利用率而竞争不可用的 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 备份和恢复功能，请分配额外的容量，以便“数据”目录或磁盘有 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 主机系统外部至少具有 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以能够成功的方式进行配置 `ping` 主机本身的主机名。如果是 IPv6 配置，您应该验证 `ping6` 主机名是否成功，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。如果您在部署期间为网络配置了静态 IP 地址，那么您就为网络主机指定了一个名称。如果您使用 DHCP 配置网络，则应该从 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。

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。

操作系统软件

Linux 系统必须安装以下版本的操作系统及支持软件：

- Red Hat Enterprise Linux 8.x 和 9.4 版本，基于 x86_64 架构。

请参阅互操作性矩阵以获取受支持的 Red Hat Enterprise Linux 版本的完整和最新列表。

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

该服务器应专用于运行 Unified Manager。服务器上不应安装任何其他应用程序。由于公司规定，您的 Linux 系统上可能安装了像 Qualys 这样的漏洞扫描程序。您应该在安装 Unified Manager 之前禁用漏洞扫描程序，以防止安装失败。



漏洞扫描程序（例如 Qualys）在内部扫描虚拟机 (VM)（其中 Unified Manager 和漏洞扫描程序安装在同一 VM 上）或外部扫描虚拟机（其中 Unified Manager 和漏洞扫描程序安装在两个不同的服务器上，并且漏洞扫描程序扫描安装了 Unified Manager 的 VM）时可能会导致 CPU 使用率过高。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 VM 中禁用漏洞扫描程序。如果无法禁用扫描仪，则在非工作时间扫描虚拟机，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 26.1.3 与 Unified Manager 捆绑并配置。

以下第三方软件包是必需的，但不包含在 Unified Manager 中。这些软件包由 `yum` 安装程序，前提是您已按照以下部分所述配置了存储库。

- MySQL 社区版 8.4.4 版（来自 MySQL 存储库）
- OpenJDK 版本 11.0.25（来自 Red Hat Extra Enterprise Linux Server 存储库）
- Python 3.9.x（来自 Red Hat Extra Enterprise Linux Server 存储库）
- p7zip 版本 16.02 或更高版本（来自 Red Hat Extra Packages for Enterprise Linux 存储库）



在升级任何第三方软件之前，您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

Linux 系统上的 Unified Manager 安装可由 root 用户或非 root 用户使用 `sudo` 命令。

此外，默认 Unified Manager 安装在 sudoers 文件中包括 umadmin 用户（默认维护用户）和 jboss 用户 (ocum_sudoers 和 `ocie\_sudoers) 在 `/etc/sudoers.d/` 目录。如果您因为安全策略或安全监控工具而从环境中删除此内容，则必须将其添加回来。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

下面列出了在您的系统上安装 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，或在异地（在云中）部署的系统可能需要额外的步骤，并且 Unified Manager 可能无法在这样的部署中正常运行。

- 您必须按照 Red Hat 最佳实践安装 Red Hat Enterprise Linux，并且应该选择以下默认选项，这需要选择“带有 GUI 的服务器”基础环境。
- 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。
- 对于 `yum` 安装程序在 Red Hat Enterprise Linux 存储库中查找相关软件，您必须在 Red Hat Enterprise Linux 安装期间或之后使用有效的 Red Hat 订阅注册系统。

有关 Red Hat 订阅管理器的信息，请参阅 Red Hat 文档。

- 您必须启用 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。

如果您的系统上未配置 EPEL 存储库，则必须手动下载并配置存储库。

看["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。

如果您的系统上未配置 MySQL 存储库，则必须手动下载并配置存储库。

看["手动配置 MySQL 存储库"](#)。

- 您必须在 Unified Manager 主机上仅安装一个版本的 Java；否则，系统可能无法确定要使用哪个版本。看 ["在 Active IQ Unified Manager 主机上更新 Java 后，服务将无法启动"](#)。

如果您的系统无法访问互联网，并且存储库没有从连接互联网的系统镜像到未连接的系统，则您应该按照安装说明确定系统的外部软件依赖项。然后，您可以将所需的软件下载到已连接互联网的系统，并将`.rpm`文件到您计划安装 Unified Manager 的系统。要下载工件和包，您必须使用`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适当的 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 而设计，并符合 Red Hat 最佳实践（目录布局、权限等）。其他位置的软件可能不遵循这些准则，这可能会导致 Unified Manager 安装失败，或者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
```

您必须使用“带有 GUI 的服务器”基础环境安装 Red Hat Enterprise Linux。它提供了 Unified Manager 安装说明所使用的命令。其他基础环境可能需要您安装其他命令来验证或完成安装。如果`firewall-cmd`在您的系统上不可用，您必须通过运行以下命令来安装它：

```
# sudo yum install firewalld
```

运行命令之前请联系您的 IT 部门，了解您的安全策略是否需要不同的程序。



Red Hat 系统上应禁用 THP（透明大页面）。启用后，在某些情况下，当某些进程消耗过多内存并终止时，它可能会导致 Unified Manager 关闭。

支持的浏览器

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

互操作性矩阵列出了受支持的浏览器版本。

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

对于所有浏览器，禁用弹出窗口阻止程序可确保软件功能正常显示。

如果您计划配置 Unified Manager 进行 SAML 身份验证，以便身份提供商 (IdP) 可以对用户进行身份验证，那么您还应该检查 IdP 支持的浏览器列表。

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。

与 Unified Manager 服务器的连接

在典型安装中，连接到 Unified Manager Web UI 时无需指定端口号，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	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	用于安全访问 Unified Manager Web UI 或进行 API 调用；API 调用只能使用 HTTPS 进行。
维护控制台	SSH/SFTP	22	用于访问维护控制台和检索支持包。
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。

接口	协议	端口	描述
休息	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	通过 TCP 的 WebSocket	56080	用于在此端口上侦听从ONTAP（云代理）接收的消息。
AMQP QPID 代理	通过 TCP 的 WebSocket	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。这不会影响任何升级方案，因为之前的配置会保留。可以修改此配置，并且可以使用 `Control access to MySQL port 3306` 维护控制台上的选项。有关信息，请参阅["附加菜单选项"](#)。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，请参阅["维护控制台菜单"](#)。

来自 Unified Manager 服务器的连接

您应该配置防火墙以打开端口，以便 Unified Manager 服务器与托管存储系统、服务器和其他组件之间进行通信。如果端口未打开，则通信失败。

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

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	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	用于某些快照恢复操作。

目标	协议	端口	描述
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 陷阱发送器
SNMPv1 或 SNMPv3	162/UDP	用于发送警报通知 SNMP 陷阱。	外部数据提供服务器
TCP	2003	用于将性能数据发送到外部数据提供商，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

完成工作表

在安装和配置 Unified Manager 之前，您应该准备好有关您的环境的具体信息。您可以在工作表中记录该信息。

Unified Manager 安装信息

安装 Unified Manager 所需的详细信息。

部署软件的系统	你的价值
主机完全限定域名	
主机 IP 地址	
网络掩码	
网关 IP 地址	
主 DNS 地址	

部署软件的系统	你的价值
辅助 DNS 地址	
搜索域名	
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。根据您的配置，某些值是可选的。

设置	你的价值
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	
认证服务器基础可分辨名称	
身份提供商 (IdP) URL	
身份提供者 (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。

N 的簇 1	你的价值
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

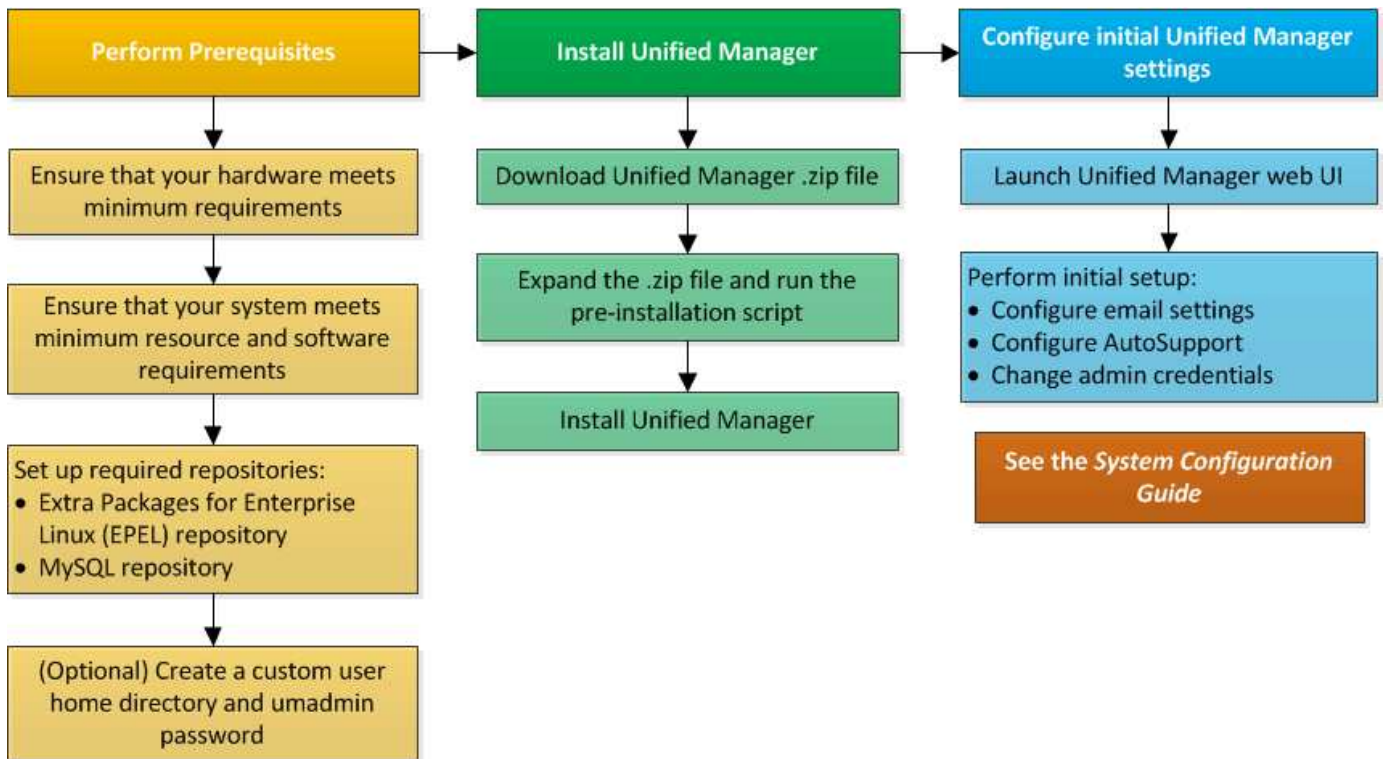
安装、升级和删除 Unified Manager 软件

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 服务器可以在物理机上运行，也可以在 VMware ESXi、Microsoft Hyper-V 或 Citrix XenServer 上运行的虚拟机上运行。

安装过程概述

安装工作流程描述了您在使用 Unified Manager 之前必须执行的任务。



设置所需的软件存储库

系统必须能够访问某些存储库，以便安装程序可以访问和安装所有必需的软件依赖项。

手动配置 EPEL 存储库

如果您安装 Unified Manager 的系统无法访问 Extra Packages for Enterprise Linux (EPEL) 存储库，则必须手动下载并配置存储库才能成功安装。

EPEL 存储库提供对必须在您的系统上安装的所需第三方实用程序的访问。您可以使用 EPEL 存储库在 Red Hat Enterprise Linux 系统上安装 Unified Manager。

步骤

1. 下载用于安装的 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 包的内部存储库，例如，`javapackages-filesystem-<version>.module.rpm`，确保模块化包的元数据也可在同一个存储库中使用。

手动配置 MySQL 存储库

如果您安装 Unified Manager 的系统无法访问 MySQL 社区版存储库，则必须手动下载并配置存储库才能成功安装。

MySQL 存储库提供对必须安装在您的系统上的所需 MySQL 软件的访问。



如果系统没有互联网连接，此任务可能会失败。如果您安装 Unified Manager 的系统无法访问互联网，请参阅 MySQL 文档。

步骤

1. 下载适合您的安装的 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-11-openjdk、p7zip 以及 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
```

如果您收到有关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 MySQL repo 文件并禁用 gpgcheck 通过标记 `gpgcheck=0`。

NFS 和 CIFS 共享上的 SELinux 要求

如果您计划安装 `/opt/netapp`` 或者 `/opt/netapp/data`` 在 NAS 或 SAN 设备上，并且启用了 SELinux，您需要注意一些事项。

如果您计划安装 `/opt/netapp`` 或者 `/opt/netapp/data`` 从根文件系统以外的任何地方，并且您的环境中启用了 SELinux，您应该为已挂载的目录设置正确的上下文。对于您环境中的适用场景，请按照以下步骤设置并确认正确的 SELinux 上下文。

配置 SELinux 上下文 `/opt/netapp/data`` 已安装

如果您已安装 `/opt/netapp/data`` 在您的系统中，SELinux 设置为 ``Enforcing`，确保 SELinux 上下文类型为 `/opt/netapp/data`` 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
```

示例输出：

```
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`。您应该将此上下文更改为 `mysqld_db_t`。

2. 执行以下步骤，根据您安装的方式设置上下文 `/opt/netapp/data`。

- a. 运行以下命令将上下文设置为 `mysqld_db_t`：

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

- b. 如果您已配置 `/opt/netapp/data`` 在 ``/etc/fstab`，你应该编辑 ``/etc/fstab`` 文件。对于 ``/opt/netapp/data`` mount 选项，添加 MySQL 标签为：

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

- c. 卸载并重新安装 `/opt/netapp/data/`` 用于启用上下文。

- d. 如果您有直接 NFS 挂载，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. 验证上下文是否设置正确：

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

示例输出：

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

配置 SELinux 上下文 `/opt/netapp` 已安装，并且 `/opt/netapp/data/` 也单独安装

在这种情况下，首先，你应该设置上下文 `/opt/netapp/data/` 如上一节所述。在设置正确的上下文之后 `/opt/netapp/data/`，确保父目录 `/opt/netapp` 没有将 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
```

示例输出：

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

在此输出中，上下文是 `file_t` 应该改变。以下命令将上下文设置为 `usr_t`。您可以将上下文设置为除 `file_t` 根据您的安全要求。

2. 根据您的安装的方式执行以下步骤来设置上下文 `/opt/netapp`。

- a. 运行以下命令来设置上下文：

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

1. 如果您已配置 `/opt/netapp` 在 `/etc/fstab`，你应该编辑 `/etc/fstab` 文件。对于 `/opt/netapp` mount 选项，添加 MySQL 标签为：

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

2. 卸载，然后重新安装 `/opt/netapp` 用于启用上下文。
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. 验证上下文是否设置正确：

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

示例输出

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

配置 SELinux 上下文 `/opt/netapp` 已安装，并且 `/opt/netapp/data/` 不单独安装

如果您已安装 `/opt/netapp` 在您的系统中，SELinux 设置为 `Enforcing`，确保 SELinux 上下文类型为 `/opt/netapp` 设置为 `mysql_d_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
```

示例输出：

```
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`。您应该将此上下文更改为 `mysql_d_t`。

2. 执行以下步骤，根据您安装的方式设置上下文 `/opt/netapp`。

- a. 运行以下命令将上下文设置为 `mysql_d_t`：

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

- b. 如果您已配置 `/opt/netapp` 在 `/etc/fstab`，编辑 `/etc/fstab` 文件。对于 `/opt/netapp/`mount` 选项，添加 MySQL 标签为：
``context=system_u:object_r:mysql_d_t:s0`

- c. 卸载，然后重新安装 `/opt/netapp/` 用于启用上下文。

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

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

3. 验证上下文是否设置正确：

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

示例输出：

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

在 Linux 系统上安装 Unified Manager

重要的是，您要了解下载和安装 Unified Manager 的步骤顺序会根据您的安装场景而有所不同。

在安装之前创建自定义用户主目录和 **umadmin** 密码

您可以在安装 Unified Manager 之前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灵活地覆盖 Unified Manager 安装默认设置。

开始之前

- 系统必须满足["硬件系统要求"](#)。
- 您必须能够以 root 用户身份登录 Red Hat Enterprise Linux 系统。

默认 Unified Manager 安装执行以下任务：

- 使用以下命令创建 umadmin 用户 `/home/umadmin` 作为主目录。
- 为 umadmin 用户分配默认密码“admin”。

由于某些安装环境限制访问 `/home`，安装失败。您必须在不同位置创建主目录。此外，某些网站可能有关于密码复杂性的规则，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您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。

如果在安装之前定义了这些信息，安装脚本就会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 安装在 `sudoers` 文件中包括 umadmin 用户(`ocum_sudoers` 和 `ocie_sudoers`) 在 `/etc/sudoers.d/` 目录。如果您因为安全策略或某些安全监控工具而从您的环境中删除了此内容，则必须将其添加回来。您需要保留 `sudoers` 配置，因为某些 Unified Manager 操作需要这些 `sudo` 权限。

您环境中的安全策略不得限制 Unified Manager 维护用户的 `sudo` 权限。如果权限受到限制，某些 Unified Manager 操作可能会失败。验证安装成功后以 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，且不会出现任何错误。

步骤

1. 以 root 用户身份登录服务器。
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 Unified Manager

您必须下载 Unified Manager `.zip` 文件从 NetApp 支持站点安装 Unified Manager。

开始之前

您必须拥有 NetApp 支持站点的登录凭据。

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

步骤

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

["NetApp 支持站点"](#)

2. 选择所需版本的 Unified Manager 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，并保存 `.zip` 文件复制到目标系统上的目录。



- 确保为您的 Red Hat Enterprise Linux 系统下载了正确版本的安装程序文件。根据您是否安装了 Red Hat Enterprise Linux 8 或 9，确保下载适当版本的 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. 验证下载软件的完整性校验和。
5. 如果您已经下载了代码签名证书和数字签名，您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：
 - 此命令使用代码签名证书中的公钥创建一个文件：

```
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
```

类似于以下的消息 `Verified Ok` 确认安装程序文件可以安全使用。

安装 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

- 您要安装 Unified Manager 的系统必须满足系统和软件要求。

看["硬件系统要求"](#)。

看["Linux 软件 and 安装要求"](#)。

- 您必须已下载 Unified Manager `.zip` 文件从NetApp支持站点复制到目标系统。
- 您应该已经验证了下载的 `.zip` 文件。
- 您必须拥有受支持的 Web 浏览器。
- 您的终端仿真软件必须启用回滚功能。

Red Hat Enterprise Linux 系统可能安装了所有必需的支持软件（Java、MySQL、附加实用程序）的必需版本，可能只安装了部分必需的软件，或者可能是新安装的系统，没有安装任何必需的软件。

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	验证软件和版本的命令
OpenJDK 版本 11.0.25	<code>java -version</code>
MySQL 8.4.4 社区版	<code>`rpm -qa</code>
<code>grep -i mysql`</code>	<code>p7zip 16.02</code>
<code>`rpm -qa</code>	<code>grep p7zip`</code>

3. 如果安装的MySQL版本低于MySQL 8.4.4社区版，请输入以下命令进行卸载：

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

如果收到依赖性错误，则必须添加 `--nodeps`` 卸载组件的选项。

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

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

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

5. 验证目录中是否有以下模块：

```
ls *.rpm
```

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

6. 运行预安装脚本以确保没有系统配置设置或任何可能与 Unified Manager 安装冲突的已安装软件：

```
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，则必须在安装 Unified Manager 之前修复这些问题。

对于 Red Hat Enterprise Linux 8 系统，如果您有带有 JDK 11 的内部存储库 - OpenJDK、p7zip 和 AppStream 存储库提供的其他软件包，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
```

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，您才必须执行步骤 7。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，请转到步骤 8。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
```

“安装：”部分中的项目是当前目录中可用的软件包，“安装依赖项：”部分中的项目是系统中缺少的软件包。

- b. 在可以访问互联网的系統上，下载缺少的软件包：

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



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

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

- a. 将缺失的软件包从互联网连接的系統复制到您的安装系統。

8. 以 root 用户身份，或使用 sudo，运行以下命令安装软件：

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

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

如果安装失败并出现 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
```



不要尝试使用其他命令进行安装（例如 `rpm -ivh`）。在 Red Hat Enterprise Linux 系统上成功安装 Unified Manager 要求所有 Unified Manager 文件和相关文件都按照特定顺序安装到由 `yum install netapp-um<version>.x86\_64.rpm` 命令。

9. 忽略安装消息后立即显示的电子邮件通知。

该电子邮件通知 root 用户初始 cron 作业失败，但这对安装没有不利影响。

10. 安装消息完成后，向后滚动消息，直到看到系统显示 Unified Manager Web UI 的 IP 地址或 URL、维护用户名 (umadmin) 和默认密码的消息。

该消息类似于以下内容：

```
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. 如果您在安装 Unified Manager 之前创建了具有自定义主目录的 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，如中所述["配置Active IQ Unified Manager"](#)。必须更改 umadmin 用户的默认密码。

### Unified Manager 安装期间创建的用户

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

- **umadmin**

用于首次登录 Unified Manager。该用户被分配了“应用程序管理员”用户角色，并配置为“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。该用户由 MySQL 第三方实用程序创建。

除了这些用户之外，Unified Manager 还创建了相应的组：maintenance、jboss 和 mysql。维护和 jboss 组由 Unified Manager 创建，而 mysql 组由第三方实用程序创建。



如果您在安装 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。



## 更改 JBoss 密码

您可以重置安装期间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。

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

### 步骤

1. 以 root 用户身份登录系统。
2. 按所示顺序输入以下命令来停止 Unified Manager 服务：

```
systemctl stop ocieau
```

```
systemctl stop ocie
```

不要停止相关的 MySQL 软件。

3. 输入以下命令开始密码更改过程：

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

4. 出现提示时，输入新的 JBoss 密码，然后再次输入以进行确认。

请注意，密码应介于 8 到 16 个字符之间，并且必须至少包含一个数字、一个大写字母和一个小写字母，以及至少一个以下特殊字符：

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

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

```
systemctl start ocie
```

```
systemctl start ocieau
```

6. 所有服务启动后，您可以登录 Unified Manager UI。

## 在 Red Hat Enterprise Linux 上升级 Union Manager

当有新版本可用时，您可以升级 Unified Manager。

当 NetApp 提供 Unified Manager 软件的补丁版本时，其安装过程与新版本相同。

如果 Unified Manager 与 OnCommand Workflow Automation 实例配对，并且这两种产品都有新版本的软件可用，则必须断开这两种产品的连接，然后在执行升级后建立新的 Workflow Automation 连接。如果您只对其中一个产品进行升级，则应在升级后登录工作流自动化并验证它是否仍在从 Unified Manager 获取数据。

## Unified Manager 版本支持的升级路径

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 都可以执行就地升级到更高版本。Unified Manager 升级仅限于 N-2 型号，这意味着升级只能在所有平台上的下 2 个版本内进行。例如，您只能从 Unified Manager 9.13 和 9.14 升级到 Unified Manager 9.16。

如果您运行的版本早于支持的版本，则需要先将 Unified Manager 实例升级到支持的版本之一，然后再升级到当前版本。

例如，如果您安装的版本是 Unified Manager 9.9，并且您想要升级到 Unified Manager 9.14，则请遵循一系列升级操作。

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 → 9.16

有关升级路径矩阵的更多信息，请参阅 ["知识库 \(KB\) 文章"](#)。

## 升级 Unified Manager

您可以通过在 Linux 平台上下载并运行安装文件从 Unified Manager 9.13 或 9.14 升级到 9.16。

开始之前

- 要升级 Unified Manager 的系统必须满足系统和软件要求。

看["硬件系统要求"](#)。

看["Linux 软件 and 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。

看["在 Linux 上升级 JRE"](#)。

- 为避免数据丢失，您必须创建 Unified Manager 数据库的备份，以防升级期间出现问题。NetApp 建议您将备份文件从 `/opt/netapp/data` 目录到外部位置。
- 升级过程中，系统可能会提示您确认是否要保留之前的默认设置（即保留性能数据 13 个月）或将其更改为 6 个月。确认后，历史绩效数据将在 6 个月后清除。
- 您应该已经完成所有正在运行的操作，因为 Unified Manager 在升级过程中不可用。
- MySQL 社区版会在 Unified Manager 升级期间自动升级。如果您系统上安装的 MySQL 版本早于 8.4.4，则 Unified Manager 升级过程会自动将 MySQL 升级到 8.4.4。

步骤

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

看["下载适用于 Linux 的 Unified Manager"](#)。

3. 导航到目标目录并展开 Unified Manager 包：

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

Unified Manager 所需的 RPM 模块已解压缩到目标目录。

4. 验证目录中是否有以下模块：

```
ls *.rpm
```

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

5. 运行预安装脚本以确保没有系统配置设置或任何可能与升级冲突的已安装软件：

```
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，您必须修复这些问题并继续升级。

如果检测到任何缺失的包，请执行["丢失包裹时需要执行的额外步骤"](#)。如果没有丢失任何包，请继续下一步。

6. 使用以下脚本升级 Unified Manager：

```
upgrade.sh
```

该脚本自动执行 RPM 模块，升级必要的支持软件 and 在其上运行的 Unified Manager 模块。此外，升级脚本还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相冲突。如果脚本发现任何问题，则必须在升级 Unified Manager 之前修复这些问题。如果您在升级 Unified Manager 之前安装了软件包（例如 *net-snmp*），则 MySQL 依赖项可能会在升级过程中卸载该软件包。您需要再次手动安装该包才能继续使用它。

7. 升级完成后，向后滚动消息，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。

该消息类似于以下内容：

```
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，然后使用您之前设置的相同维护用户名 (umadmin) 和密码登录。

丢失包裹时需要执行的额外步骤

如果在升级过程中检测到您的站点缺少任何软件包，或者您的系统未连接到互联网，或者您没有使用 Red Hat Enterprise Linux 存储库，请执行以下步骤来确定是否缺少任何所需的软件包并下载这些软件包。



这些步骤需要在主程序的步骤\_5\_之后执行。此过程将升级 Unified Manager，您无需运行任何其他升级步骤。

1. 查看可用和不可用包的列表：

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

“安装：”部分中的项目是当前目录中可用的软件包，“安装依赖项：”部分中的项目是系统中缺少的软件包。

2. 在具有互联网访问权限的其他系统上，运行以下命令来下载缺少的软件包。

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

软件包下载到指定的目录中 --downloadaddr=。

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

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

3. 将下载的软件包复制到安装系统上解压 Unified Manager 包的目录。
4. 将目录更改为该目录并运行以下命令来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，然后使用您之前设置的相同维护用户名 (umadmin) 和密码登录。

将主机操作系统从 **Red Hat Enterprise Linux 7.x** 升级到 **8.x**

如果您之前在 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，则必须遵循本主题中列出的步骤之一。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 的备份，然后将备份还原到 Red Hat Enterprise Linux 8.x 系统上。请注意，Red Hat Enterprise Linux 支持的版本是从 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，您正在将 Unified Manager 还原到新的 8.x 服务器上，而在另一种情况下，您正在在同一服务器上执行还原操作。

由于此任务要求您在 Red Hat Enterprise Linux 7.x 系统上创建 Unified Manager 的备份，因此您应该仅在准备完成整个升级过程时才创建备份，以便 Unified Manager 在最短的时间内处于离线状态。在 Red Hat Enterprise Linux 7.x 系统关闭期间和新 Red Hat Enterprise Linux 8.x 启动之前的一段时间内，Unified Manager UI 中收集的数据会出现差距。

看["管理备份和恢复操作"](#)如果您需要查看备份和恢复过程的详细说明。

如果您有一个备用系统，可以在其中安装 Red Hat Enterprise Linux 8.x 软件，请按照以下步骤操作，以便在 Red Hat Enterprise Linux 7.x 系统仍然可用时可以在该系统上执行 Unified Manager 还原。

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

看["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。

看["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。备份文件在恢复过程中填充此信息。

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，然后复制备份文件（.7z 文件）和数据库存储库目录的内容（/database-dumps-repo 子目录）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，复制备份文件（.7z 文件）从外部位置到 /opt/netapp/data/ocum-backup/ 以及数据库存储库文件 /database-dumps-repo 下的子目录 /ocum-backup 目录。
6. 输入以下命令从备份文件恢复 Unified Manager 数据库：

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

7. 在您的 Web 浏览器中输入 IP 地址或 URL 以启动 Unified Manager Web UI，然后登录系统。

一旦您验证系统正常运行，您就可以从 Red Hat Enterprise Linux 7.x 系统中删除 Unified Manager。

在同一服务器上升级主机操作系统

如果您没有可以安装 Red Hat Enterprise Linux 8.x 软件的备用系统，请按照以下步骤操作。

1. 从 Web UI 中的管理菜单，创建 Unified Manager 备份，然后复制备份文件（.7z 文件）和数据库存储库目录的内容（/database-dumps-repo 子目录）复制到外部位置。
2. 从系统中删除 Red Hat Enterprise Linux 7.x 映像并彻底擦除系统。
3. 在同一系统上安装和配置 Red Hat Enterprise Linux 8.x 软件。

看["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。

看["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。备份文件在恢复过程中填充此信息。

5. 复制备份文件（.7z 文件）从外部位置到 `/opt/netapp/data/ocum-backup/` 以及数据库存储库文件 `/database-dumps-repo/` 下的子目录 `/ocum-backup/` 目录。
6. 输入以下命令从备份文件恢复 Unified Manager 数据库：

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

7. 在您的 Web 浏览器中输入 IP 地址或 URL 以启动 Unified Manager Web UI，然后登录系统。

## 安装 Unified Manager 后升级第三方产品

当 Unified Manager 已安装在 Linux 系统上时，您可以升级第三方产品，例如 JRE。

开发这些第三方产品的公司会定期报告安全漏洞。您可以按照自己的时间表升级到该软件的较新版本。

### 在 Linux 上升级 OpenJDK

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

#### 开始之前

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

您可以在发行系列中更新 OpenJDK 版本。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 Unified Manager 主机。
2. 将适当版本的 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 Unified Manager

更改配置后，您可能需要重新启动 Unified Manager。

### 开始之前

您必须具有安装了 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 Unified Manager

您可以使用单个命令从 Red Hat Enterprise Linux 主机停止并卸载 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)。使用以下命令将 SELinux 运行时模式更改为“Permissive” `setenforce 0` 命令。
- 在删除该软件之前，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。防火墙规则不会被自动删除。

### 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
```

此步骤将删除所有相关的 NetApp RPM 软件包。它不会删除必备的软件模块，例如 Java、MySQL 和 p7zip。

3. \*可选：\*如果适用，请删除支持软件模块，例如 Java、MySQL 和 p7zip：

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

此操作完成后，软件将被删除。所有数据来自 `/opt/netapp/data` 目录被移动到 `/opt/netapp/data/BACKUP` 卸载后的文件夹。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。

## 删除自定义 **umadmin** 用户和维护组

如果您在安装 Unified Manager 之前创建了自定义主目录来定义您自己的 umadmin 用户和维护帐户，则应在卸载 Unified Manager 后删除这些项目。

标准 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 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

Active IQ Unified Manager（以前称为OnCommand Unified Manager）使您能够从单一界面监控和管理ONTAP存储系统的运行状况和性能。您可以在 Linux 服务器、Windows 服务器上部署 Unified Manager，也可以将其作为虚拟设备部署在 VMware 主机上。

完成安装并添加要管理的集群后，Unified Manager 将提供一个图形界面，显示受监控存储系统的容量、可用性、保护和性能状态。

相关信息

["NetApp 互操作性表工具"](#)

## Unified Manager 服务器的功能

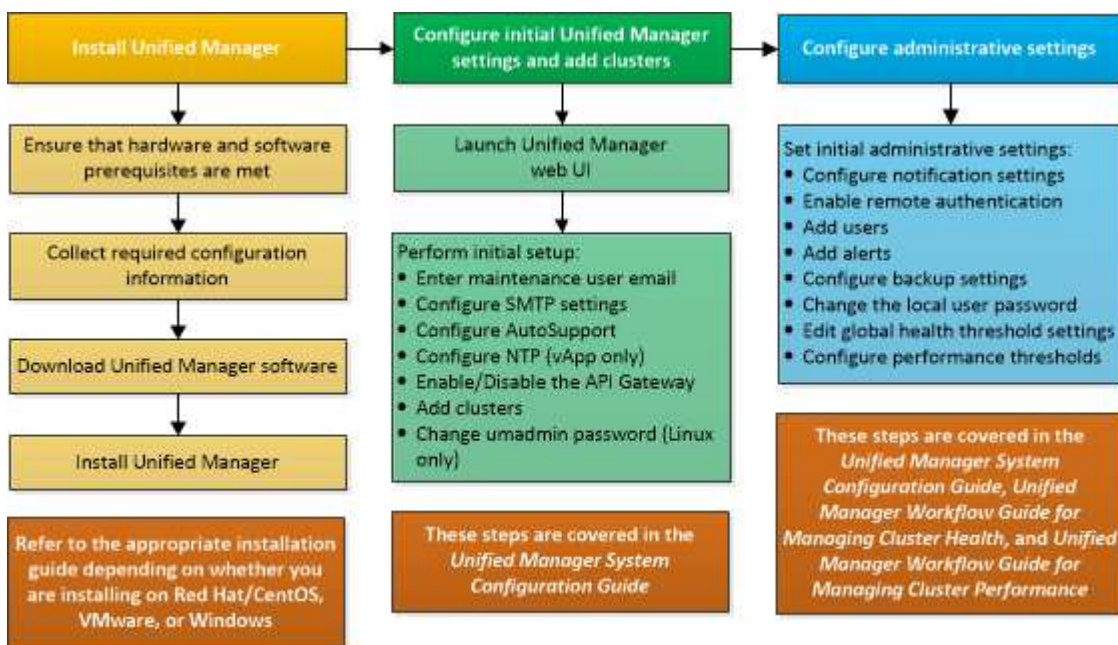
Unified Manager 服务器基础架构由数据收集单元、数据库和应用程序服务器组成。它提供发现、监控、基于角色的访问控制 (RBAC)、审计和日志记录等基础设施服务。

Unified Manager 收集集群信息，将数据存储在数据库中，并分析数据以查看是否存在任何集群问题。

## 安装顺序概述

安装工作流程描述了您在使用 Unified Manager 之前必须执行的任务。

这些部分描述了下面工作流程中显示的每个项目。



# 安装 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。如果您需要对 Unified Manager 服务器应用任何安全措施，则应该对安装 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 服务器的更多详细信息，请参阅知识库文章。

["适用于集群模式Data ONTAP的Active IQ Unified Manager的安全措施的可支持性"](#)

相关信息

["NetApp 互操作性表工具"](#)

## 虚拟基础设施和硬件系统要求

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。

下表显示了内存、CPU 和磁盘空间资源的推荐值。这些值已经过限定，因此 Unified Manager 满足可接受的性能水平。

| 硬件配置     | 推荐设置                                                                                                                |
|----------|---------------------------------------------------------------------------------------------------------------------|
| RAM      | 12 GB（最低要求 8 GB）                                                                                                    |
| 处理器      | 4 个 CPU                                                                                                             |
| CPU 循环容量 | 总计 9572 MHz（最低要求 9572 MHz）                                                                                          |
| 可用磁盘空间   | 150GB，容量分配如下： <ul style="list-style-type: none"><li>• 100 GB 磁盘空间用于安装目录</li><li>• 50 GB 磁盘空间用于 MySQL 数据目录</li></ul> |

Unified Manager 可以安装在具有少量内存的系统上，但建议使用 12 GB RAM，以确保有足够的内存来实现最佳性能，并且随着配置的增长，系统可以容纳额外的集群和存储对象。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，膨胀）。

此外，在安装第二个 Unified Manager 实例之前，单个 Unified Manager 实例可以监控的节点数量是有限制的。有关更多信息，请参阅《最佳实践指南》。

["技术报告 4621：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。由于整体主机利用率而竞争不可用的 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 备份和恢复功能，请分配额外的容量，以便“数据”目录或磁盘有 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 主机系统外部至少具有 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以能够成功的方式进行配置 `ping` 主机本身的主机名。如果是 IPv6 配置，您应该验证 `ping6` 主机名是否成功，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。如果您在部署期间为网络配置了静态 IP 地址，那么您就为网络主机指定了一个名称。如果您使用 DHCP 配置网络，则应该从 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。

## Windows 软件和安装要求

为了在 Windows 上成功安装 Unified Manager，您应该确保安装 Unified Manager 的系统满足软件要求。

### 操作系统软件

您可以在以下 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

请参阅互操作性矩阵以获取受支持 Windows 版本的完整和最新列表。

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



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

该服务器应专用于运行 Unified Manager。服务器上不应安装任何其他应用程序。由于公司规定，您的 Windows 系统上可能安装了活动的防病毒软件。您应该在安装 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。如果您的系统上未安装这些第三方软件包，Unified Manager 会在安装过程中安装它们。

- 适用于 Visual Studio 2015 版本 14.26.28720.3 的 Microsoft Visual C++ 可再发行组件包
- MySQL 社区版 8.4.4
- Python 3.12.4
- OpenJDK 版本 11.0.25
- 7-zip 23.01 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 开始不再支持 Oracle Java。

如果已预先安装 MySQL，则应确保：

- 它使用默认端口。
- 未安装示例数据库。
- 服务名称是“MYSQL84”。

Unified Manager 部署在 WildFly Web 服务器上。WildFly 26.1.3 与 Unified Manager 捆绑并配置。



在升级任何第三方软件之前，您应该关闭正在运行的 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。
- 这 `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。
- 您要安装 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。
- 您应该禁用 Microsoft IIS 全球网络发布服务并确保端口 80 和 443 是空闲的。
- 您应该确保在安装过程中禁用“Windows Installer RDS 兼容性”的远程桌面会话主机设置。
- UDP 端口 514 应该是空闲的，并且不应被任何其他服务使用。
- 在安装 Unified Manager 之前，您应该禁用系统上的所有防病毒软件。安装完成后，请确保手动将以下路径从防病毒扫描中排除：
  - 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`

## 支持的浏览器

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

互操作性矩阵列出了受支持的浏览器版本。

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

对于所有浏览器，禁用弹出窗口阻止程序可确保软件功能正常显示。

如果您计划配置 Unified Manager 进行 SAML 身份验证，以便身份提供商 (IdP) 可以对用户进行身份验证，那么您还应该检查 IdP 支持的浏览器列表。

## 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。

### 与 Unified Manager 服务器的连接

在典型安装中，连接到 Unified Manager Web UI 时无需指定端口号，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  | 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 | 用于安全访问 Unified Manager Web UI 或进行 API 调用；API 调用只能使用 HTTPS 进行。 |
| 维护控制台                              | SSH/SFTP | 22  | 用于访问维护控制台和检索支持包。                                              |
| 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    | 描述                                                                               |
|--------------|--------------------|-------|----------------------------------------------------------------------------------|
| 休息           | 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 | 通过 TCP 的 WebSocket | 56080 | 用于在此端口上侦听从ONTAP（云代理）接收的消息。                                                       |
| AMQP QPID 代理 | 通过 TCP 的 WebSocket | 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端口 MySQL 3306 的访问。这不会影响任何升级方案，因为之前的配置会保留。可以修改此配置，并且可以使用 `Control access to MySQL port 3306` 维护控制台上的选项。有关信息，请参阅["附加菜单选项"](#)。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，请参阅["配置Active IQ Unified Manager"](#)。

## 来自 Unified Manager 服务器的连接

您应该配置防火墙以打开端口，以便 Unified Manager 服务器与托管存储系统、服务器和其他组件之间进行通信。如果端口未打开，则通信失败。

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

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        | 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 | 用于某些快照恢复操作。  |

| 目标                 | 协议      | 端口                                                        | 描述                                |
|--------------------|---------|-----------------------------------------------------------|-----------------------------------|
| 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 陷阱发送器                        |
| SNMPv1 或 SNMPv3    | 162/UDP | 用于发送警报通知 SNMP 陷阱。                                         | 外部数据提供服务器                         |
| TCP                | 2003    | 用于将性能数据发送到外部数据提供商，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                      |
| 通过 TCP 的 WebSocket | 56080   | 用于在此端口上侦听从ONTAP（云代理）接收的消息。                                | AMQP QPID 代理                      |
| 通过 TCP 的 WebSocket | 56443   | 用于在此端口上侦听从ONTAP（云代理）接收的消息。通过此端口的通信支持 TLS 或 SSL 提供的加密。     | 系统日志                              |

## 完成工作表

在安装和配置 Unified Manager 之前，您应该准备好有关您的环境的具体信息。您可以在工作表中记录该信息。

### Unified Manager 安装信息

安装 Unified Manager 所需的详细信息。

| 部署软件的系统   | 你的价值 |
|-----------|------|
| 主机完全限定域名  |      |
| 主机 IP 地址  |      |
| 网络掩码      |      |
| 网关 IP 地址  |      |
| 主 DNS 地址  |      |
| 辅助 DNS 地址 |      |
| 搜索域名      |      |
| 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。根据您的配置，某些值是可选的。

| 设置                                   | 你的价值    |
|--------------------------------------|---------|
| 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       |         |



| 设置                | 你的价值 |
|-------------------|------|
| 认证服务器基础可分辨名称      |      |
| 身份提供商 (IdP) URL   |      |
| 身份提供者 (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。

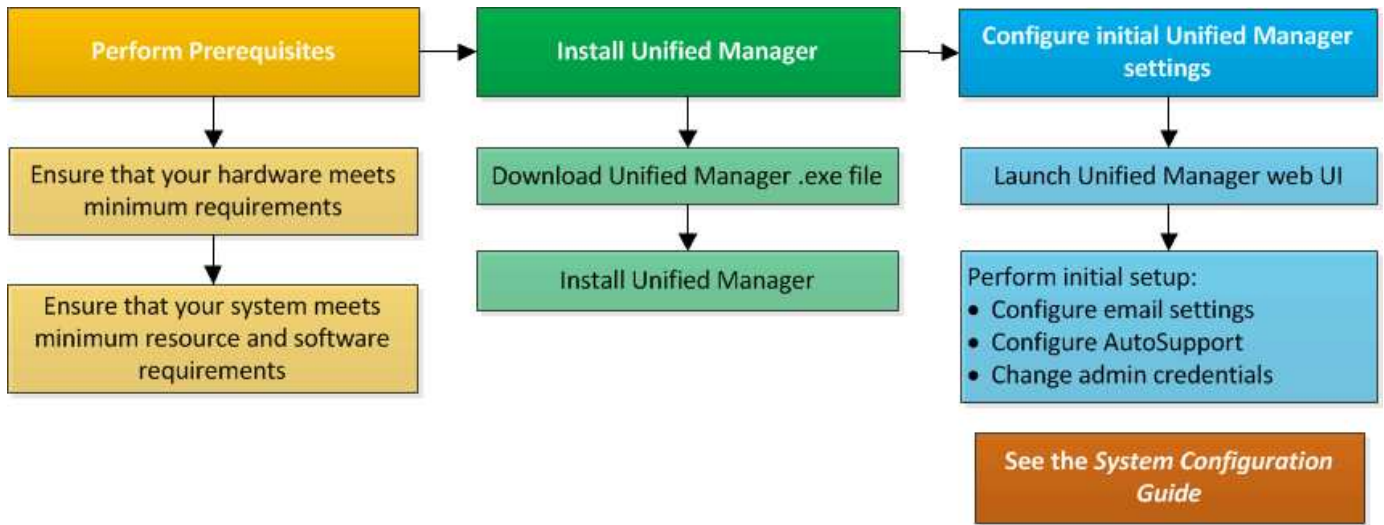
| N 的簇 1                                                                                                                | 你的价值  |
|-----------------------------------------------------------------------------------------------------------------------|-------|
| 主机名或集群管理 IP 地址                                                                                                        |       |
| ONTAP 管理员用户名<br> 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

您可以安装 Unified Manager、升级到较新版本或删除 Unified Manager 应用程序。

### 安装过程概述

安装工作流程描述了您在使用 Unified Manager 之前必须执行的任务。



## 在 Windows 上安装 Unified Manager

了解在 Windows 上下载和安装 Unified Manager 的步骤顺序非常重要。

### 安装 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。

看["硬件系统要求"](#)。

看["Windows 软件和安装要求"](#)。



从 Unified Manager 9.5 开始，OpenJDK 在安装包中提供并自动安装。从 Unified Manager 9.5 开始不再支持 Oracle Java。

- 您应该具有 Windows 管理员权限。确保您的用户名不以感叹号"!"开头!". Installation of Unified Manager might fail if the user name of user running the installation begins with "!"。
- 除ASA r2 系统外，所有集群均受支持。
- 您应该有一个受支持的 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 根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 Windows。
2. 登录NetApp支持站点，然后导航到 Unified Manager 的下载页面：

## "NetApp 支持站点"

3. 选择所需版本的 Unified Manager 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，请解压 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列出它们。如果系统中未安装所需的第三方软件包，Unified Manager 会在安装过程中安装它们。

7. 单击“下一步”。
8. 输入用户名和密码来创建维护用户。
9. 在数据库连接向导中，输入 MySQL 根密码。
10. 单击“更改”为 Unified Manager 安装目录和 MySQL 数据目录指定新位置。

如果您不更改安装目录，Unified Manager 将安装在默认安装目录中。

11. 单击“下一步”。
12. 在“准备安装 Shield”向导中，单击“安装”。
13. 安装完成后，单击\*完成\*。
14. 如果您的 Windows 系统上安装了活动的防病毒软件，请在安装完成后手动将以下路径从防病毒扫描中排除：
  - Unified Manager 数据目录
  - Unified Manager 安装目录
  - MySQL 数据目录

安装过程中会创建多个目录：

- 安装目录

这是您在安装期间指定的 Unified Manager 的根目录。例子：C:\Program Files\NetApp\

- MySQL 数据目录

这是存储 MySQL 数据库的目录，您在安装期间指定。例子：

C:\ProgramData\MySQL\MySQLServerData\

- Java 目录

这是 OpenJDK 的安装目录。例子：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、支持包、备份和所有其他附加数据。例子：

C:\ProgramData\NetApp\OnCommandAppData\

您可以访问 Web UI 来执行 Unified Manager 的初始设置，如["配置Active IQ Unified Manager"](#)。

执行 **Unified Manager** 的无人值守安装

您可以使用命令行界面安装 Unified Manager，无需用户干预。通过键值对的方式传递参数即可完成无人值守安装。

步骤

- 1. 使用默认本地管理员帐户登录 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 如果预装了第三方软件包 | <div>ActiveIQUnifiedManager-x.y.exe</div> <div>/V"MYSQL_PASSWORD=mysql_password</div> <div>INSTALLDIR="Installation directory\"</div> <div>MYSQL_DATA_DIR="MySQL data</div> <div>directory\"</div> <div>MAINTENANCE_PASSWORD=maintenance_passw</div> <div>ord</div> <div>MAINTENANCE_USERNAME=maintenance_usern</div> <div>ame /qn /l*v CompletePathForLogFile"</div> <div>例子：</div> <div>ActiveIQUnifiedManager.exe /s</div> <div>/v"MYSQL_PASSWORD=netapp21!</div> <div>INSTALLDIR="C:\Program Files\NetApp\"</div> <div>MYSQL_DATA_DIR="C:\ProgramData\MySQL\</div> <div>MySQLServer\" MAINTENANCE_PASSWORD=*</div> <div>MAINTENANCE_USERNAME=admin /qn /l*v</div> <div>C:\install.log"</div> |

| 选项          | AutoSupport                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 如果未安装第三方软件包 | <pre>ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR="Installation directory\" MYSQL_DATA_DIR="MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_passw ord MAINTENANCE_USERNAME=maintenance_usern ame /qr /l*v CompletePathForLogFile"  例子:  ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR="C:\Program Files\NetApp\" MYSQL_DATA_DIR="C:\ProgramData\MYSQL\ MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qr /l*v C:\install.log"</pre> |

这`/qr`该选项可启用安静模式并减少用户界面。将显示一个基本用户界面，其中显示安装进度。系统不会提示您输入。如果未预安装 JRE、MySQL 和 7zip 等第三方软件包，则应使用`/qr`选项。如果出现以下情况，安装将失败`/qn`该选项用于未安装第三方软件包的服务器上。

这`/qn`选项启用没有用户界面的安静模式。安装期间不显示任何用户界面或详细信息。您不应该使用`/qn`当未安装第三方软件包时的选项。

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

https://IP address

更改 JBoss 密码

您可以重置安装期间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

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

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

步骤

1. 以管理员用户身份登录 Unified Manager 主机。

2. 使用 Windows 服务控制台停止以下 Unified Manager 服务：

- NetApp Active IQ收购服务 (Ocie-au)
- NetApp Active IQ管理服务器服务 (Oncommandsvc)

3. 启动 `password.bat` 脚本开始密码更改过程：

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

4. 出现提示时，输入 MySQL 根用户密码。

5. 出现提示时，输入新的 JBoss 用户密码，然后再次输入以进行确认。

请注意，密码应介于 8 到 16 个字符之间，并且必须至少包含一个数字、一个大写字母和一个小写字母，以及至少一个以下特殊字符：

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

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收购服务 (Ocie-au)

7. 所有服务启动后，您可以登录 Unified Manager UI。

## Unified Manager 版本支持的升级路径

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 都可以执行就地升级到更高版本。Unified Manager 升级仅限于 N-2 型号，这意味着升级只能在所有平台上的下 2 个版本内进行。例如，您只能从 Unified Manager 9.13 和 9.14 升级到 Unified Manager 9.16。

如果您运行的版本早于支持的版本，则需要先将 Unified Manager 实例升级到支持的版本之一，然后再升级到当前版本。

例如，如果您安装的版本是 Unified Manager 9.9，并且您想要升级到 Unified Manager 9.14，则请遵循一系列升级操作。

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 → 9.16

有关升级路径矩阵的更多信息，请参阅 ["知识库 \(KB\) 文章"](#)。

## 升级 Unified Manager

您可以通过在 Windows 平台上下载并运行安装文件将 Unified Manager 9.13 或 9.14 升级到 9.16。

## 开始之前

- 要升级 Unified Manager 的系统应满足系统和软件要求。

看["硬件系统要求"](#)。

看["Windows 软件和安装要求"](#)。



从 Unified Manager 9.5 开始，OpenJDK 在安装包中提供并自动安装。从 Unified Manager 9.5 开始不再支持 Oracle Java。



在开始升级之前，请确保您的系统上安装了 Microsoft .NET 4.5.2 或更高版本。

- MySQL 社区版会在 Unified Manager 升级期间自动升级。如果您系统上安装的 MySQL 版本早于 8.4.4，则 Unified Manager 升级过程会自动将 MySQL 升级到 8.4.4。您不能运行早期版本的 MySQL 到 8.4.4 的独立升级。
- 除 ASA r2 系统外，所有集群均受支持。
- 您应该具有 Windows 管理员权限。确保您的用户名不以感叹号"!"开头!"。 Installation of Unified Manager might fail if the user name of user running the installation begins with "!"。
- 您应该拥有有效的凭据才能登录NetApp支持站点。
- 为避免数据丢失，您应该创建 Unified Manager 机器的备份，以防升级期间出现问题。
- 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。

- 升级过程中，系统可能会提示您确认是否要保留之前的默认设置（即保留性能数据 13 个月）或将其更改为 6 个月。确认后，6个月后的历史绩效数据将被清除。
- 升级之前，您应该关闭 *<InstallDir>\JDK* 和 *MySQL Data Directory* 中所有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，Unified Manager 升级可能会失败。在升级 Unified Manager 之前，您应该禁用系统上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，您应该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新版本的软件可用，则必须断开这两种产品的连接，然后在执行升级后建立新的 Workflow Automation 连接。如果您只对其中一个产品进行升级，则应在升级后登录工作流自动化并验证它是否仍在从 Unified Manager 获取数据。

## 步骤

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

["NetApp 支持站点"](#)。

2. 选择所需版本的 Unified Manager 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，请解压 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 会提示您以下消息：

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. 输入安装时设置的MySQL84 root密码，然后单击\*下一步\*。
6. 在受支持的 Web 浏览器的新窗口中启动 Web UI 并登录以使用升级版的 Unified Manager。
7. 如果您的 Windows 系统上安装了活动的防病毒软件，请确保在升级完成后手动将以下路径从防病毒扫描中排除：
  - 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

当安装在 Windows 系统上时，您可以在 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会定期报告安全漏洞。您可以按照自己的时间表升级到该软件的较新版本。

### 升级 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，以获取安全漏洞的修复。

#### 开始之前

您必须拥有安装 Unified Manager 的系统的 Windows 管理员权限。

您可以在发行系列中更新 OpenJDK 版本。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. 以管理员用户身份登录 Unified Manager 主机。
2. 从 OpenJDK 站点下载适当版本的 OpenJDK（64 位）到目标系统。

例如，下载 jdk-11.0.18\_windows-x64\_bin.zip from <https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html>。





下载该文件需要 Oracle 帐户。如果您没有 Oracle 帐户，请转至["Oracle 帐户登录"](#)页面来创建一个。

3. 使用 Windows 服务控制台停止以下 Unified Manager 服务：
  - NetApp Active IQ收购服务 (Ocie-au)
  - NetApp Active IQ管理服务器服务 (Oncommandsvc)
4. 展开 `zip` 文件。
5. 从结果中复制目录和文件 `jdk` 目录`（例如，``jdk-11.0.18`` 到安装 Java 的位置。例子：  
``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收购服务 (Ocie-au)

## 卸载第三方产品

升级 Unified Manager 后，您可以卸载第三方产品，例如 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 3.12 之外的任何版本的 Python。确保保留 Python 版本 3.12。

### 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\*。

## 重新启动 Unified Manager

更改配置后，您可能需要重新启动 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 Windows。
2. 停止 Unified Manager 服务：

| 从...            | 按以下顺序停止服务...                                                                   |
|-----------------|--------------------------------------------------------------------------------|
| 命令行             | a. <code>sc stop ocie-au</code><br>b. <code>sc stop Oncommandsvc</code>        |
| Microsoft 服务管理器 | a. NetApp Active IQ收购服务 (Ocie-au)<br>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. <code>sc start Oncommandsvc</code><br>b. <code>sc start ocie-au</code>      |
| Microsoft 服务管理器 | a. NetApp Active IQ管理服务器服务 (Oncommandsvc)<br>b. NetApp Active IQ收购服务 (Ocie-au) |

## 卸载 Unified Manager

您可以使用程序和功能向导来卸载 Unified Manager，或者从命令行界面执行无人值守卸载。

### 开始之前

- 您必须具有 Windows 管理员权限。
- 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。防火墙规则不会被自动删除。

### 步骤

#### 1. 通过选择以下选项之一来卸载 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 Windows 命令行。
  - ii. 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
```

如果服务器上启用了用户帐户控制 (UAC)，并且您以域用户身份登录，则必须使用命令行卸载方法。

Unified Manager 已从您的系统中卸载。

2. 卸载在 Unified Manager 卸载期间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

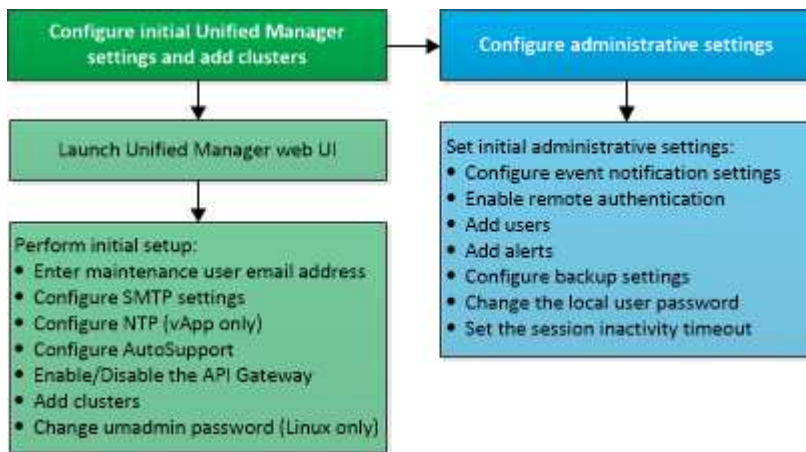
## 配置Active IQ Unified Manager

安装Active IQ Unified Manager（以前称为OnCommand Unified Manager）后，您必须完成初始设置（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。

本手册中描述的一些步骤是完成 Unified Manager 实例的初始设置所必需的。其他程序是推荐的配置设置，这些设置有助于在新实例上进行设置，或者在您开始定期监控ONTAP系统之前了解这些设置。

### 配置序列概述

配置工作流程描述了您在使用 Unified Manager 之前必须执行的任务。



### 访问 Unified Manager Web UI

安装 Unified Manager 后，您可以访问 Web UI 来设置 Unified Manager，以便开始监控您的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，浏览器可能会显示警告，表明该证书不受信任。您可以承认风险并继续访问，或者安装证书颁发机构 (CA) 签名的数字证书进行服务器身份验证。

#### 步骤

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

链接格式如下：`https://URL`。

2. 使用您的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，您将被锁定在系统之外，并且需要联系您的系统管理员。这仅适用于本地用户。

## 执行 **Unified Manager Web UI** 的初始设置

要使用 Unified Manager，您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 服务器主机以及添加ONTAP集群。

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
- 使用安装期间创建的维护用户名和密码（Linux 安装的 umadmin 用户）登录

仅当您首次访问 Web UI 时才会出现Active IQ Unified ManagerGetting Started 页面。以下页面来自 VMware 上的安装。

☰

Active IQ Unified Manager

All ▾

Search All Storage Objects and Actions 🔍

## Getting Started

1

2

3

4

5

EmailAutoSupportAPI GatewayAdd ONTAP ClustersFinish

### Notifications

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

### Maintenance User Email

Emailmgo@eng.netapp.com

### SMTP Server

Host Name or IP Addressemail.eng.netapp.com

Port25

User Nameadmin

Password

☐ Use STARTTLS ⓘ☐ Use SSL ⓘ

Continue

如果您稍后想要更改这些选项中的任何一个，您可以从 Unified Manager 左侧导航窗格中的常规选项中选择您的选择。请注意，NTP 设置仅适用于 VMware 安装，并且可以稍后使用 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）。然后点击“继续”。



如果您选择了“使用 STARTTLS”或“使用 SSL”选项，则单击“继续”按钮后将显示证书页面。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 同意并继续 以启用从 Unified Manager 到 NetAppActive IQ 的AutoSupport消息发送。

如果您需要指定代理来提供互联网访问以发送AutoSupport内容，或者您想要禁用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. 在设置 API 网关页面中，选择是否要使用 API 网关功能，该功能允许 Unified Manager 管理您计划使用 ONTAP REST API 监控的 ONTAP 集群。然后点击“继续”。

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 的更多信息，请参阅["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，您必须拥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“统一管理器仪表板”页面。

## 添加集群

您可以将集群添加到 Active IQ Unified Manager，以便监控该集群。其中包括可通过获取集群的运行状况、容量、性能和配置等信息来发现并解决可能出现的任何问题。

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 Unified Manager 用于连接集群的 FQDN 或短名称。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，并将应用程序访问权限设置为 *ontapi*、*console* 和 *http*。

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

**SSL (HTTPS) 证书：**此证书归 Unified Manager 所有。全新安装 Unified Manager 时会生成默认的自签名 SSL (HTTPS) 证书。NetApp 建议您将其升级为 CA 签名证书以获得更好的安全性。如果服务器证书过期，您应该重新生成它并重新启动 Unified Manager，以便服务合并新证书。有关重新生成 SSL 证书的更多信息，请参阅["生成 HTTPS 安全证书"](#)。

**EMS 证书：**此证书归 Unified Manager 所有。它用于对从 ONTAP 接收的 EMS 通知进行身份验证。

**用于相互 TLS 通信的证书：**在 Unified Manager 和 ONTAP 之间的相互 TLS 通信期间使用。根据 ONTAP 版本，为集群启用基于证书的身份验证。如果运行 ONTAP 版本的集群低于 9.5，则不会启用基于证书的身份验证。

如果您正在更新旧版本的 Unified Manager，则不会自动为集群启用基于证书的身份验证。但是，您可以通过修改和保存集群详细信息来启用它。如果证书过期，您应该重新生成它以包含新证书。有关查看和重新生成证书的更多信息，请参阅["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，默认情况下不启用基于证书的身份验证。如果您使用 Unified Manager CLI 添加集群，则需要使用 Unified Manager UI 编辑该集群。你可以看到["支持的 Unified Manager CLI 命令"](#)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，并且您从服务器备份 Unified Manager 并将其还原到主机名或 IP 地址已更改的另一个 Unified Manager 服务器，则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，请参阅["编辑集群"](#)。

+

集群证书：此证书归ONTAP拥有。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证书。有关证书生成的信息，请参阅知识库 (KB) 文章 ["如何在系统管理器用户界面中续订ONTAP自签名证书"](#)。

- Unified Manager 服务器上必须有足够的空间。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，您必须添加本地集群和远程集群，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. 在添加集群对话框中，指定所需的值，例如集群的主机名或 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. 在授权主机对话框中，单击“查看证书”，查看集群的证书信息。
6. 单击“是”。

保存集群详细信息后，您可以看到集群的 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的每个 API 调用的证书。

发现新集群的所有对象后，Unified Manager 开始收集前 15 天的历史性能数据。这些统计信息将通过数据连续性收集功能进行收集。添加集群后，此功能会立即为您提供两周以上的集群性能信息。数据连续性收集周期完成后，将收集实时集群性能数据，默认情况下每五分钟收集一次。



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。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范围的差距。





如果您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不同步，以及 Unified Manager HTTPS 证书的开始日期是否晚于集群上的日期。您必须通过 NTP 或类似服务确保时钟同步。

## 相关信息

["安装 CA 签名并返回的 HTTPS 证书"](#)

## 配置 Unified Manager 以发送警报通知

您可以配置 Unified Manager 来发送有关您环境中的事件的警报通知。在发送通知之前，您必须配置其他几个 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，您应该考虑配置您的环境以根据收到的事件触发警报并生成通知电子邮件或 SNMP 陷阱。

### 步骤

#### 1. ["配置事件通知设置"](#)。

如果您希望在您的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。如果您想使用 SNMP 陷阱，您可以选择该选项并提供必要的信息。

#### 2. ["启用远程身份验证"](#)。

如果您希望远程 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内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的角色。创建警报时，您会指定一个用户来接收警报通知。

#### 5. ["添加警报"](#)。

添加了用于发送通知的电子邮件地址、添加了用于接收通知的用户、配置了网络设置以及配置了环境所需的 SMTP 和 SNMP 选项后，您就可以分配警报了。

## 配置事件通知设置

您可以配置 Unified Manager 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，并且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

电子邮件地址出现在已发送警报通知的“发件人”字段中。如果电子邮件因任何原因无法送达，该电子邮件地址也将用作无法送达邮件的收件人。

- SMTP 服务器主机名以及访问该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、社区和其他所需的 SNMP 配置值

要指定多个陷阱目标，请用逗号分隔每个主机。在这种情况下，列表中所有主机的所有其他 SNMP 设置（例如版本和出站陷阱端口）必须相同。

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。

笔记：

- 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成功送达。
  - 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）来代替主机名。
3. 单击“保存”。
  4. 如果您选择了“使用 STARTTLS”或“使用 SSL”选项，则单击“保存”按钮后将显示证书页面。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\*查看证书详情\*按钮来查看证书详情。如果现有证书已过期，请取消选中 使用 **STARTTLS** 或 使用 **SSL** 框，保存通知设置，然后再次选中 使用 **STARTTLS** 或 使用 **SSL** 框以查看新证书。

#### 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 服务器必须直接与身份验证服务器连接。您必须禁用任何本地 LDAP 客户端，例如 SSSD（系统安全服务守护进程）或 NSLCD（名称服务 LDAP 缓存守护进程）。

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。

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



用于验证用户身份的证书必须符合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...”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 | <ul style="list-style-type: none"><li>• 认证服务器管理员名称采用以下格式之一：<ul style="list-style-type: none"><li>◦ domainname\username</li><li>◦ username@domainname</li><li>◦ Bind Distinguished Name（使用适当的 LDAP 符号）</li></ul></li><li>• 管理员密码</li><li>• 基本可分辨名称（使用适当的 LDAP 符号）</li></ul> |
| 打开 LDAP          | <ul style="list-style-type: none"><li>• 绑定可分辨名称（以适当的 LDAP 符号表示）</li><li>• 绑定密码</li><li>• 基本可分辨名称</li></ul>                                                                                                                                                                 |

如果 Active Directory 用户的身份验证花费很长时间或超时，则身份验证服务器可能需要很长时间才能响应。禁用 Unified Manager 中对嵌套组的支持可能会减少身份验证时间。

如果您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“保存”。

禁用嵌套组的远程身份验证

如果您启用了远程身份验证，则可以禁用嵌套组身份验证，以便只有个人用户（而不是组成员）可以远程向 Unified Manager 进行身份验证。当您想要提高 Active Directory 身份验证响应时间时，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 Unified Manager 中对嵌套组的支持可能会减少身份验证时间。如果嵌套组支持被禁用，并且如果将远程组添加到 Unified Manager，则各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“保存”。

设置身份验证服务

身份验证服务可在身份验证服务器中对远程用户或远程组进行身份验证，然后才允许他们访问 Unified Manager。您可以使用预定义的身份验证服务（例如 Active Directory 或 OpenLDAP）或通过配置您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. 选择以下身份验证服务之一：

| 如果您选择...         | 操作                                                                                                                                           |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Active Directory | <div>a. 输入管理员名称和密码。</div> <div>b. 指定身份验证服务器的基本可分辨名称。</div> <div>例如，如果认证服务器的域名是+ou@domain.com+，那么基本可分辨名称就是*cn=ou,dc=domain,dc=com*。</div>     |
| OpenLDAP         | <div>a. 输入绑定可分辨名称和绑定密码。</div> <div>b. 指定身份验证服务器的基本可分辨名称。</div> <div>例如，如果认证服务器的域名是+ou@domain.com+，那么基本可分辨名称就是*cn=ou,dc=domain,dc=com*。</div> |

| 如果您选择... | 操作                                                                                                                                                                                             |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 其他       | <p>a. 输入绑定可分辨名称和绑定密码。</p> <p>b. 指定身份验证服务器的基本可分辨名称。</p> <p>例如，如果认证服务器的域名是+ou@domain.com+，那么基本可分辨名称就是*cn=ou,dc=domain,dc=com*。</p> <p>c. 指定认证服务器支持的LDAP协议版本。</p> <p>d. 输入用户名、组成员身份、用户组和成员属性。</p> |



如果要修改身份验证服务，则必须删除任何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“保存”。

## 添加身份验证服务器

您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内的远程用户可以访问 Unified Manager。

### 开始之前

- 必须提供以下信息：
  - 认证服务器的主机名或IP地址
  - 认证服务器的端口号
- 您必须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。

如果您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），那么您还可以添加合作伙伴身份验证服务器。当其中一个身份验证服务器无法访问时，这使得管理服务器能够与合作伙伴进行通信。

### 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：



## 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. 在测试用户对话框中，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\*测试\*。

如果您正在验证远程组，则不得输入密码。

## 添加警报

您可以配置警报，以便在生成特定事件时通知您。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。您可以指定接收通知的频率并将脚本与警报关联。

## 开始之前

- 您必须配置通知设置，例如用户电子邮件地址、SMTP 服务器和 SNMP 陷阱主机，以便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 and 事件，以及要通知的用户的用户名或电子邮件地址。
- 如果您希望根据事件执行脚本，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\*，然后输入警报的名称和描述。
4. 单击“资源”，然后选择要包含在警报中或从警报中排除的资源。

您可以通过在\*名称包含\*字段中指定文本字符串来设置过滤器，以选择一组资源。根据您的指定的文本字符串，可用资源列表仅显示符合过滤规则的资源。您指定的文本字符串区分大小写。

如果资源同时符合您指定的包含规则和排除规则，则排除规则优先于包含规则，并且不会针对与排除的资源相关的事件生成警报。

5. 单击“事件”，然后根据事件名称或事件严重性类型选择要触发警报的事件。



要选择多个事件，请在选择时按住 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，并分配在生成警报时执行的脚本。



如果您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，如果您从“用户”页面修改了所选用户的电子邮件地址，则所选用户的修改后的电子邮件地址不会更新。

您还可以选择通过 SNMP 陷阱通知用户。

## 7. 单击“保存”。

### 添加警报的示例

此示例显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，并排除名称包含“xyz”的所有卷
- 事件：包括所有重大健康事件
- 操作：包括“sample@domain.com”和“Test”脚本，并且每 15 分钟通知一次用户

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**”，显示名称中包含“abc”的卷。
  - b. 选择 **+ [All Volumes whose name contains 'abc'] +** 从可用资源区域，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. 从匹配事件区域选择“所有关键事件”，并将其移动到选定事件区域。
5. 单击“操作”，然后在“警报这些用户”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。

您可以配置警报以在指定时间内重复向收件人发送通知。您应该确定事件通知对于警报生效的时间。

7. 在选择要执行的脚本菜单中，选择\*测试\*脚本。
8. 单击“保存”。

## 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。

维护用户和远程用户的密码不能使用以下步骤进行更改。要更改远程用户密码，请与密码管理员联系。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. 从顶部菜单栏中，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“保存”。

如果 Unified Manager 是在高可用性配置中进行配置的，则必须在设置的第二个节点上更改密码。这两个实例必须使用相同的密码。

设置会话不活动超时

您可以指定 Unified Manager 的不活动超时值，以便会话在一定时间不活动后自动终止。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。

此设置会影响所有已登录的用户会话。



如果您启用了安全断言标记语言 (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来指定不活动超时：

| 目的                 | 操作                                                 |
|--------------------|----------------------------------------------------|
| 没有设置超时，这样会话就不会自动关闭 | 在“不活动超时”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“不活动超时”面板中，将滑块按钮向右移动（打开），以分钟为单位指定不活动超时值，然后单击“应用”。 |

通过 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，以便会话在一定时间后自动终止。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）。这意味着您的会话会在 72 小时后自动结束，即使您已登录并正在使用 Unified Manager。

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已登录的用户会话。

步骤

- 1. 通过输入 ``um cli login`` 命令。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>`` 命令修改会话超时值。

## 更改 Unified Manager 主机名

在某些时候，您可能想要更改已安装 Unified Manager 的系统的主机名。例如，您可能希望重命名主机，以便更轻松按类型、工作组或受监控的集群识别 Unified Manager 服务器。

更改主机名所需的步骤有所不同，具体取决于 Unified Manager 是在 VMware ESXi 服务器、Red Hat Linux 服务器还是 Microsoft Windows 服务器上运行。

### 更改 Unified Manager 虚拟设备主机名

首次部署 Unified Manager 虚拟设备时，会为网络主机分配一个名称。您可以在部署后更改主机名。如果更改主机名，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，或者分配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。如果您在部署期间为网络配置了静态 IP 地址，那么您将为网络主机指定一个名称。如果您使用 DHCP 配置网络，则主机名应从 DNS 中获取。如果 DHCP 或 DNS 配置不正确，则会自动分配主机名“Unified Manager”并将其与安全证书关联。

无论主机名如何分配，如果您更改主机名，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。

如果您使用服务器的 IP 地址而不是主机名访问 Web UI，则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。

如果您在 Unified Manager 中更改主机名，则必须在 OnCommand Workflow Automation (WFA) 中手动更新主机名。主机名不会在 WFA 中自动更新。

直到 Unified Manager 虚拟机重新启动后，新证书才会生效。

#### 步骤

##### 1. 生成 HTTPS 安全证书

如果您想使用新的主机名访问 Unified Manager Web UI，则必须重新生成 HTTPS 证书以将其与新的主机名关联。

##### 2. 重新启动 Unified Manager 虚拟机

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

#### 生成 HTTPS 安全证书

首次安装 Active IQ Unified Manager 时，会安装默认 HTTPS 证书。您可以生成一个新的 HTTPS 安全证书来替换现有的证书。

#### 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，如果您想要更好的可分辨名称 (DN) 值，或者您想要更大的密钥大小，或者更长的有效期，或者当前证书已过期。

如果您无权访问 Unified Manager Web UI，则可以使用维护控制台重新生成具有相同值的 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。如果您使用 `Reset Server Certificate` 选项，则会创建一个有效期为 397 天的新 HTTPS 证书。该证书将具有大小为 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”。

系统弹出“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   | <div><div>单击“更新当前证书属性”选项。</div><div><p>如果您不输入新值，则通用名称和备用名称字段将使用现有证书中的值。“通用名称”应设置为主机的 FQDN。其他字段不需要值，但您可以输入值，例如，如果您希望在证书中填充这些值，则输入 EMAIL、COMPANY、DEPARTMENT、City、State 和 Country 的值。您还可以从可用的密钥大小（密钥算法为“RSA”）和有效期中进行选择。</p><div><div></div><div><ul style="list-style-type: none"><li>• 密钥大小的允许值为 2048，3072 和 4096。</li><li>• 有效期最短1天，最长36500天。</li></ul><p>尽管允许有效期为 36500 天，但建议您使用不超过 397 天或 13 个月的有效期。因为如果您选择的有效期超过 397 天，并计划导出此证书的 CSR 并由知名 CA 进行签名，则 CA 返回给您的签名证书的有效期将减少到 397 天。</p><ul style="list-style-type: none"><li>• 如果您想从证书中的备用名称字段中删除本地识别信息，可以选中“排除本地识别信息（例如 localhost）”复选框。选中此复选框后，只有您在字段中输入的内容才会在备用名称字段中使用。当留空时，生成的证书将根本没有备用名称字段。</li></ul></div></div></div></div> |

4. 单击“是”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 Unified Manager 虚拟机

您可以从 Unified Manager 的维护控制台重新启动虚拟机。生成新的安全证书后或虚拟机出现问题时必须重新启动。

开始之前

虚拟设备已启动。

您以维护用户身份登录到维护控制台。

您还可以使用“重新启动客户机”选项从 vSphere 重新启动虚拟机。有关详细信息，请参阅 VMware 文档。

步骤

1. 访问维护控制台。
2. 选择\*系统配置\*>\*重新启动虚拟机\*。

#### 在 Linux 系统上更改 Unified Manager 主机名

在某些时候，您可能想要更改已安装 Unified Manager 的 Red Hat Enterprise Linux 机器的主机名。例如，您可能希望重命名主机，以便在列出 Linux 机器时更轻松按类型、工作组或受监控的集群组识别 Unified Manager 服务器。

开始之前

您必须具有安装 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。如果您在部署期间为网络配置了静态 IP 地址，那么您将为网络主机指定一个名称。如果您使用 DHCP 配置网络，则主机名应从 DNS 服务器中获取。

无论主机名如何分配，如果您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。

如果您使用服务器的 IP 地址而不是主机名访问 Web UI，则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。直到 Linux 机器重新启动后，新证书才会生效。

如果您在 Unified Manager 中更改主机名，则必须在 OnCommand Workflow Automation (WFA) 中手动更新主机名。主机名不会在 WFA 中自动更新。

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 更改主机名 `hostnamectl` 命令：

```
hostnamectl set-hostname new_FQDN
```

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

#### 4. 为服务器重新生成HTTPS证书：

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

#### 5. 重启网络服务：

```
systemctl restart NetworkManager.service
```

#### 6. 服务重启后，验证新的主机名是否能ping通自己：

```
ping new_hostname
```

```
ping nuhost
```

此命令应返回先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，输入以下命令重新启动 Unified Manager：

```
systemctl start mysqld ocie ocieau
```

## 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系统管理器中创建工作负载并附加 QoS 策略，但使用 Unified Manager 应用时，您可以配置和管理 Unified Manager 实例正在监控的所有集群中的工作负载。

您必须具有应用程序管理员角色。

此选项默认启用，但如果您不想使用 Unified Manager 配置和管理工作负载，则可以禁用它。

启用后，此选项会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“常见任务”>“配置”获取        |
| 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 获取 |
| 创建性能存储效率策略的页面            | 可从“设置”>“策略”>“存储效率”访问   |
| 描述当前工作负载性能和工作负载 IOPS 的面板 | 可从仪表板获取                |

有关这些页面和此功能的更多信息，请参阅产品中的在线帮助。

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来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，将滑块按钮向左移动。 |
| 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 Unified Manager 备份

您可以通过在主机系统和维护控制台上执行的一组配置步骤来配置 Unified Manager 上的备份功能。

有关配置步骤的信息，请参阅[“管理备份和恢复操作”](#)。

## 管理功能设置

通过“功能设置”页面，您可以启用和禁用Active IQ Unified Manager中的特定功能。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、根据不活动时间超时 Web UI 会话以及禁用接收Active IQ平台事件。



只有具有应用程序管理员角色的用户才能使用“功能设置”页面。

有关脚本上传的信息，请参阅[“启用和禁用脚本上传”](#)。

### 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\*选择激活或停用此功能。激活此功能后，可以使用以下页面进行操作和监控：

- 配置（存储工作负载配置）
- 政策 > 性能服务水平
- 政策 > 存储效率
- 集群设置页面上按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来创建性能服务级别和存储效率策略，并配置存储工作负载。您还可以监控符合指定性能服务级别的存储工作负载以及不符合规定的存储工作负载。工作负载性能和工作负载 IOPS 面板还使您能够根据数据中心内集群所配置的存储工作负载来评估集群的总容量、可用容量和已用容量及性能 (IOPS)。

激活此功能后，您可以运行 Unified Manager REST API 来从 菜单栏 > 帮助按钮 > **API 文档** > 存储提供商 类别执行其中一些功能。或者，您可以输入主机名或 IP 地址以及访问 REST API 页面的 URL，格式为 `https://<hostname>/docs/api/`

有关 API 的更多信息，请参阅["Active IQ Unified Manager REST API 入门"](#)。

## 启用 API 网关

API 网关功能允许 Active IQ Unified Manager 作为单一控制平面，您可以从中管理多个 ONTAP 集群，而无需单独登录它们。

您可以从首次登录 Unified Manager 时出现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，并且并非所有 ONTAP REST API 的功能都可以通过使用 Unified Manager REST API 来实现。但是，如果您有特定的业务需求，需要访问 ONTAP API 来管理未向 Unified Manager 公开的特定功能，则可以启用 API 网关功能并执行 ONTAP API。网关充当代理，通过维护与 ONTAP API 相同的格式的标头和正文请求来传输 API 请求。您可以使用 Unified Manager 凭据并执行特定的 API 来访问和管理 ONTAP 集群，而无需传递单独的集群凭据。Unified Manager 作为单一管理点，在由 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，您可以输入主机名或 IP 地址以及 URL 来访问 REST API 页面，格式如下 `https://<hostname>/docs/api/`

有关 API 的更多信息，请参阅["Active IQ Unified Manager REST API 入门"](#)。

## 指定不活动超时

您可以指定 Active IQ Unified Manager 的不活动超时值。在指定时间不活动后，应用程序将自动注销。默认情况下，此选项处于启用状态。

您可以从 \*常规\* > 功能设置 > 不活动超时 \*停用此功能或修改时间。一旦激活此功能，您应该在 \***LOGOUT AFTER**\* 字段中指定不活动的时间限制（以分钟为单位），之后系统将自动注销。默认值为 4320 分钟（72 小时）。



如果您启用了安全断言标记语言 (SAML) 身份验证，则此选项不可用。

## 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控的存储系统生成的AutoSupport消息运行一组规则而创建的。这些事件与其他 Unified Manager 事件不同，它们识别与系统配置、布线、最佳实践和可用性相关问题相关的事件或风险。

您可以从 常规 > 功能设置 > 活动**Active IQ**门户事件\*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\*存储管理 > 事件设置 > \*上传规则\*手动上传规则。

此功能默认启用。禁用此功能将阻止在 Unified Manager 上发现或显示Active IQ事件。禁用此功能后，启用此功能可允许 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。

## 启用和禁用安全设置以实现合规性

通过使用“功能设置”页面的“安全仪表板”面板上的“自定义”按钮，您可以启用或禁用 Unified Manager 上的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，相应的列将显示在集群清单页面的\*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。



只有具有管理员角色的用户才能编辑这些设置。

您的ONTAP集群、存储虚拟机和卷的安全标准将根据["NetApp ONTAP 9 安全强化指南"](#)。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状态。还会生成安全事件并针对存在安全违规的集群和存储虚拟机启用管理操作。

### 自定义安全设置

要根据您的ONTAP环境自定义合规性监控设置，请按照以下步骤操作：

#### 步骤

1. 单击\*常规>功能设置>安全仪表板>自定义\*。出现“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存储虚拟机屏幕上的默认安全视图、报告和计划报告。如果您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 报告可能有错误。

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，请参阅["集群合规性类别"](#)。
3. 要启用或禁用存储虚拟机的自定义设置，请在“存储虚拟机”下选择所需的常规设置。有关自定义存储虚拟机合规性的选项的信息，请参阅["存储虚拟机合规性类别"](#)。

### 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，您可以启用 Unified Manager 警报来向默认ONTAP管理员用户发出警报。



## 启用和禁用脚本上传

默认情况下，将脚本上传到 Unified Manager 并运行它们的功能是启用的。如果贵组织出于安全原因不想允许此类活动，则可以禁用此功能。

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来禁用或启用脚本：

| 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。 |

## 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，谁被允许访问系统以及登录和注销期间的使用条款和条件。

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

您可以使用维护控制台配置网络设置、配置和管理安装了 Unified Manager 的系统，以及执行其他维护任务以帮助预防 and 排除可能出现的问题。

### 维护控制台提供哪些功能

Unified Manager 维护控制台使您能够维护 Unified Manager 系统上的设置并进行任何必要的更改以防止问题发生。

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

- 排除虚拟设备的任何问题，尤其是在 Unified Manager Web 界面不可用的情况下
- 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商以发送性能统计数据

- 更改性能数据收集内部
- 从以前备份的版本恢复 Unified Manager 数据库和配置设置。

维护用户执行的操作

维护用户是在 Red Hat Enterprise Linux 系统上安装 Unified Manager 期间创建的。维护用户名是“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他们分配角色。

维护用户或 umadmin 用户也可以访问 Unified Manager 维护控制台。

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，并且您只能在技术支持的指导下使用它。

诊断用户可以在技术支持的指导下执行操作系统级命令，以进行故障排除。

访问维护控制台

如果 Unified Manager 用户界面未运行，或者您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，维护控制台将注销您。



在 VMware 上安装时，如果您已经通过 VMware 控制台以维护用户身份登录，则无法同时使用安全外壳登录。

步骤

1. 按照以下步骤访问维护控制台：

| 在此操作系统上... | 请按照以下步骤操作...                                                                                                                                                             |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VMware     | <div>a. 使用安全外壳连接到 Unified Manager 虚拟设备的 IP 地址或完全限定域名。</div> <div>b. 使用您的维护用户名和密码登录维护控制台。</div>                                                                           |
| Linux      | <div>a. 使用安全外壳连接到 Unified Manager 系统的 IP 地址或完全限定域名。</div> <div>b. 使用维护用户 (umadmin) 名称和密码登录到此系统。</div> <div>c. 输入命令 <code>`maintenance_console`</code> 然后按 Enter 键。</div> |

| 在此操作系统上... | 请按照以下步骤操作...                                                                                                                                                                                  |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows    | <ul style="list-style-type: none"> <li>a. 使用管理员凭据登录 Unified Manager 系统。</li> <li>b. 以 Windows 管理员身份启动 PowerShell。</li> <li>c. 输入命令 <code>`maintenance_console`</code> 然后按 Enter 键。</li> </ul> |

显示 Unified Manager 维护控制台菜单。

## 使用 vSphere VM 控制台访问维护控制台

如果 Unified Manager 用户界面未运行，或者您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。
- 必须打开虚拟设备才能访问维护控制台。

步骤

1. 在 vSphere Client 中，找到 Unified Manager 虚拟设备。
2. 单击“控制台”选项卡。
3. 单击控制台窗口内部即可登录。
4. 使用您的用户名和密码登录维护控制台。

15 分钟不活动后，维护控制台将注销您。

## 维护控制台菜单

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

根据安装 Unified Manager 的操作系统，维护控制台包含以下菜单：

- 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. 外部数据提供者
  - d. 备份还原
  - e. 性能轮询间隔配置

- f. 禁用 SAML 身份验证
- g. 查看/更改应用程序端口
- h. 调试日志配置
- i. 控制对 MySQL 端口 3306 的访问
- j. 退出

您从列表中选择数字来访问特定的菜单选项。例如，对于备份和恢复，您选择\_4\_。

## 网络配置菜单

网络配置菜单使您能够管理网络设置。当 Unified Manager 用户界面不可用时，您应该使用此菜单。



如果 Unified Manager 安装在 Red Hat Enterprise Linux 或 Microsoft Windows 上，则此菜单不可用。

有以下菜单选项可供选择。

- 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。如果您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

使您能够更改解析主机名时要搜索的域名。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

使您能够添加或删除静态网络路由。您必须选择“提交更改”才能使更改生效。

- 添加路线

使您能够添加静态路由。

- 删除路线

使您能够删除静态路由。

- 后退

带您返回\*主菜单\*。

- 出口

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。您必须选择“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。您必须选择此选项才能实施所做的任何更改，否则更改不会发生。

- **Ping 主机**

对目标主机执行 ping 操作以确认 IP 地址更改或 DNS 配置。

- 恢复默认设置

将所有设置重置为出厂默认设置。您必须选择“提交更改”才能使更改生效。

- 后退

带您返回\*主菜单\*。

- 出口

退出维护控制台。

## “System Configuration”菜单

系统配置菜单提供各种选项，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。



当 Unified Manager 安装在 Linux 或 Microsoft Windows 系统上时，此菜单中只有“从 Unified Manager 备份还原”选项可用。

有以下菜单选项可供选择：

- 显示服务器状态

显示当前服务器状态。状态选项包括“正在运行”和“未运行”。

如果服务器没有运行，您可能需要联系技术支持。

- 重启虚拟机

重新启动虚拟机，停止所有服务。重启后，虚拟机和服务重新启动。

- 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<登录用户>的用户密码

更改当前登录用户的密码，该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 地址或完全限定域名 (FQDN)。

- 更改 **NTP** 服务

在 `ntp` 和 `systemd-timesyncd` 服务。

- 从统一管理器备份恢复

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

更改安装虚拟设备的主机的名称。

- 后退

退出系统配置菜单并返回主菜单。

- 出口

退出维护控制台菜单。

## 支持和诊断菜单

通过“支持和诊断”菜单，您可以生成支持包，然后将其发送给技术支持以获得故障排除帮助。

有以下菜单选项可用：

- 生成轻量级支持包

使您能够生成仅包含 30 天的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

使您能够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，您还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 服务器内部的详细数据以及AutoSupport消息或轻量级支持包中通常不包含的详细级别日志。

## 附加菜单选项

以下菜单选项使您能够在 Unified Manager 服务器上执行各种管理任务。

有以下菜单选项可供选择：

- 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，以便身份提供商 (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 配置问题阻止用户访问 Unified Manager GUI 时，通常使用此控制台选项。

- 外部数据提供者

提供将 Unified Manager 连接到外部数据提供商的选项。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。将显示以下选项：

- 显示服务器配置——显示外部数据提供商的当前连接和配置设置。
- 添加/修改服务器连接——使您能够为外部数据提供商输入新的连接设置，或更改现有设置。
- 修改服务器配置——使您能够为外部数据提供商输入新的配置设置，或更改现有设置。
- 删除服务器连接——删除与外部数据提供商的连接。

删除连接后，Unified Manager 将失去与外部服务器的连接。

- 备份恢复

有关信息，请参阅以下主题["管理备份和恢复操作"](#)。

- 性能轮询间隔配置

提供一个选项来配置 Unified Manager 从集群收集性能统计数据的频率。默认收集间隔为5分钟。

如果您发现大型集群的收集没有按时完成，则可以将此间隔更改为 10 或 15 分钟。

- 查看/更改应用程序端口

如果出于安全考虑，提供一个选项来更改 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。

- 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了该端口，那么您也可以使该端口对远程主机可用。或者，当为所有主机启用时，您可以将此端口的访问限制为仅限本地主机。如果之前在远程主机上启用了访问，则在升级场景中将保留该配置。切换端口可见性后，您应该检查 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。

- 出口

退出维护控制台菜单。

## 在 **Windows** 上更改维护用户密码

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 登录页面上，单击“忘记密码”。

将显示一个页面，提示您输入要重置其密码的用户的姓名。

2. 输入用户名并单击\*提交\*。

一封包含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. 点击电子邮件中的\*重置密码链接\*并定义新密码。

4. 返回 Web UI 并使用新密码登录 Unified Manager。

## 在 **Linux** 系统上更改 **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。如果需要，您可以随时再次更改密码。



## 开始之前

- Unified Manager 必须安装在 Red Hat Enterprise Linux Linux 系统上。
- 您必须拥有安装了 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
```

系统提示您输入 umadmin 用户的新密码。

## 更改 Unified Manager 用于 HTTP 和 HTTPS 协议的端口

如果出于安全考虑，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

您必须拥有授权登录 Unified Manager 服务器维护控制台的用户 ID 和密码。



使用 Mozilla Firefox 或 Google Chrome 浏览器时，某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，请先检查您的浏览器。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寻求解决方案。

更改端口后，Unified Manager 实例会自动重新启动，因此请确保这是一个短时间关闭系统的好时机。

1. 使用 SSH 以维护用户身份登录 Unified Manager 主机。

将显示 Unified Manager 维护控制台提示。

2. 键入标有 查看/更改应用程序端口 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 HTTP 和 HTTPS 端口的新端口号，然后按 Enter。

将端口号留空将为协议分配默认端口。

系统会提示您是否要立即更改端口并重新启动 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。

完成此更改后，用户必须在 URL 中包含新的端口号才能访问 Unified Manager Web UI，例如 + <https://host.company.com:1234>+或 [https://\[2001:db8:0:1\]:2123](https://[2001:db8:0:1]:2123)。

## 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。

虚拟设备必须已打开电源。



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 > 重新启动操作系统。

重启后，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. 选择新的网络接口并按 **Enter**。

选择 **eth1** 并按 **Enter**。

5. 输入 **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，系统将提示您输入网络设置。

进入网络设置后，自动返回\*网络配置\*菜单。

7. 选择\*提交更改\*。

您必须提交更改才能添加网络接口。

## 向 Unified Manager 数据库目录添加磁盘空间

Unified Manager 数据库目录包含从 ONTAP 系统收集的所有健康和性能数据。某些情况下可能需要您增加数据库目录的大小。

例如，如果 Unified Manager 从大量集群（每个集群都有许多节点）收集数据，则数据库目录可能会已满。当数据库目录已满 90% 时，您将收到警告事件；当数据库目录已满 95% 时，您将收到严重事件。



当目录达到 95% 满度后，将不再从集群收集其他数据。

根据 Unified Manager 是在 VMware ESXi 服务器、Red Hat 服务器还是 Microsoft Windows 服务器上运行，向数据目录添加容量所需的步骤会有所不同。

### 为 Linux 主机的数据目录添加空间

如果您分配的磁盘空间不足 `/opt/netapp/data` 目录以支持 Unified Manager，当您最初设置 Linux 主机然后安装 Unified Manager 时，您可以在安装后通过增加 `/opt/netapp/data`

## 目录。

### 开始之前

您必须具有安装了 Unified Manager 的 Red Hat Enterprise Linux 机器的 root 用户访问权限。

我们建议您在增加数据目录的大小之前备份 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 服务和相关的 MySQL 软件：

```
systemctl stop ocieau ocie mysqld
```

3. 创建临时备份文件夹（例如， /backup-data ）具有足够的磁盘空间来包含当前 `/opt/netapp/data` 目录。
4. 复制现有 `/opt/netapp/data` 目录到备份数据目录：

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

5. 如果启用了 SE Linux：

- a. 获取现有文件夹的 SE Linux 类型 `/opt/netapp/data` 文件夹：

```
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：

- a. `cd /opt/netapp/data`
- b. `rm -rf *`

7. 扩大规模 `/opt/netapp/data` 通过 LVM 命令或添加额外的磁盘将目录大小增加到至少 150 GB。



如果您已经创建 `/opt/netapp/data` 从磁盘，那么您不应该尝试安装 `/opt/netapp/data` 作为 NFS 或 CIFS 共享。因为在这种情况下，如果您尝试扩展磁盘空间，一些 LVM 命令，例如 `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）保持不变：

```
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`，以便这个无关的文件将来不会导致数据库错误。

11. 将备份数据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，按照所示顺序启动 `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
```

为 **VMware** 虚拟机数据盘添加空间

如果需要增加 Unified Manager 数据库的数据磁盘空间量，您可以在安装后使用 Unified Manager 维护控制台增加磁盘空间来增加容量。

开始之前

- 您必须具有 vSphere Client 的访问权限。
- 虚拟机一定不能有本地存储的快照。
- 您必须拥有维护用户凭证。

我们建议您在增加虚拟磁盘的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，然后向数据添加更多磁盘容量 disk 3。有关详细信息，请参阅 VMware 文档。

在极少数情况下，Unified Manager 部署使用“硬盘 2”作为数据磁盘，而不是“硬盘 3”。如果您的部署中出现这种情况，请增加较大磁盘的空间。数据磁盘的空间总是比其他磁盘大。

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. 单击控制台窗口，然后使用您的用户名和密码登录维护控制台。
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。

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，您可以向安装 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. 按照与您想要使用的方法相对应的步骤来添加更多空间：

| 选项                                         | 描述                                                  |
|--------------------------------------------|-----------------------------------------------------|
| 在物理服务器上，向安装 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：<br><a href="#">"扩展基本卷"</a>   |
| 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：<br><a href="#">"添加硬盘驱动器"</a> |
| 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：<br><a href="#">"增加磁盘分区的大小"</a>  |

## 管理用户访问

您可以创建角色并分配功能来控制用户对 Active IQ Unified Manager 的访问。您可以识别具有访问 Unified Manager 中选定对象所需权限的用户。只有拥有这些角色和功能的用户才能管理 Unified Manager 中的对象。

## 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，以便身份提供商 (IdP) 对访问图形界面的用户进行身份验证，请确保这些用户被定义为“远程”用户。

启用 SAML 身份验证时，“本地”或“维护”类型的用户无法访问 UI。

如果您从 Windows Active Directory 添加一个组，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。如果您从 OpenLDAP 或其他身份验证服务添加一个组，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，然后输入所需的信息。

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“添加”。

## 创建数据库用户

要支持工作流自动化和 Unified Manager 之间的连接，或访问数据库视图，您必须首先在 Unified Manager Web UI 中创建具有集成模式或报告模式角色的数据库用户。

### 开始之前

您必须具有应用程序管理员角色。

数据库用户提供与工作流自动化的集成以及对特定于报告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，也无法执行 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. 输入数据库用户的名称和密码。
5. 在\*角色\*下拉列表中，选择适当的角色。

| 如果您是...                     | 选择此角色 |
|-----------------------------|-------|
| 将 Union Manager 与工作流自动化连接起来 | 集成架构  |
| 访问报告和其他数据库视图                | 报告架构  |

6. 单击“添加”。

## 编辑用户设置

您可以编辑每个用户指定的用户设置，例如电子邮件地址和角色。例如，您可能想要更改存储操作员用户的角色，并为该用户分配存储管理员权限。

开始之前

您必须具有应用程序管理员角色。

修改分配给用户的角色时，发生以下任一操作时都会应用更改：

- 用户注销并重新登录 Unified Manager。
- 会话超时已达到 24 小时。

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，编辑为用户指定的适当设置。
4. 单击“保存”。

## 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，您必须重新分配已分配给远程组用户的事件。

如果您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。

## 什么是 RBAC

RBAC（基于角色的访问控制）可以控制谁有权访问Active IQ Unified Manager服务器中的各种功能和资源。

### 基于角色的访问控制的作用

基于角色的访问控制 (RBAC) 使管理员能够通过定义角色来管理用户组。如果您需要限制选定管理员对特定功能的访问，则必须为他们设置管理员帐户。如果您想限制管理员可以查看的信息和可以执行的操作，您必须将角色应用到您创建的管理员帐户。

管理服务器使用RBAC进行用户登录和角色权限。如果您没有更改管理服务器的管理用户访问的默认设置，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，您必须使用应用程序管理员帐户访问权限登录。

### 用户类型的定义

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。当 Unified Manager 安装在 Red Hat Enterprise Linux 系统上时，维护用户的用户名为“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授予的角色执行功能。

- 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。该帐户的名称应与身份验证服务器上存储的组的名称相匹配。远程组内的所有用户都可以使用其各自的用户凭据访问 Unified Manager UI。



远程组可以根据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，但无法访问 Unified Manager Web 界面或维护控制台，也无法执行 API 调用。

## 用户角色的定义

维护用户或应用程序管理员为每个用户分配一个角色。每个角色都包含一定的权限。您可以在 Unified Manager 中执行的活动范围取决于您被分配的角色以及该角色包含的权限。

Unified Manager 包括以下预定义用户角色：

- 操作员

查看存储系统信息和 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、解决事件并添加注释。

- 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。此角色可以管理用户、安全证书、数据库访问和管理选项，包括身份验证、SMTP、网络 and AutoSupport。



当 Unified Manager 安装在 Linux 系统上时，具有应用程序管理员角色的初始用户将自动被命名为“umadmin”。

- 集成模式

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

此角色允许直接从 Unified Manager 数据库对报告和其他数据库视图进行只读访问。可以查看的数据库包括：

- netapp\_model\_view
- netapp\_performance
- ocum

- ocum\_report
- ocum\_report\_birt
- opm
- scalemonitor

## Unified Manager 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                 |     |       | •       |      |      |

| 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 |
|-------------------------|-----|-------|---------|------|------|
| 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 |     |       |         | •    |      |
| 安排和保存报告                 |     | •     | •       |      |      |
| 从管理操作中执行“修复”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

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商 (IdP) 进行身份验证。

请注意，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的用户。

### 身份提供者要求

当配置 Unified Manager 使用身份提供商 (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。

您必须将 Unified Manager URI 和元数据输入到 IdP 服务器中。您可以从 Unified Manager SAML 身份验证页面复制此信息。Unified Manager 被视为安全断言标记语言 (SAML) 标准中的服务提供者 (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

#### 经过验证的身份提供者

- 口令
- Active Directory 联合身份验证服务 (ADFS)

#### ADFS 配置要求

- 您必须按照以下顺序定义三个声明规则，Unified Manager 需要这些规则来解析此依赖方信任条目的 ADFS SAML 响应。

| 声明规则       | 值                                  |
|------------|------------------------------------|
| SAM 帐户名称   | 姓名 ID                              |
| SAM 帐户名称   | urn:oid:0.9.2342.19200300.100.1.1  |
| 令牌组——非限定名称 | 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”，否则用户在退出 Unified Manager 时可能会收到错误。按照下面的步骤进行操作：
  - 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“表单身份验证”而不是默认的“Windows 身份验证”。
- 在某些情况下，当 Unified Manager 安全证书由 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：
  - 按照链接中的说明，禁用 ADFS 服务器上与链式 CA 证书关联的信赖方的吊销检查：

["禁用每个依赖方信任的撤销检查"](#)

- 让 CA 服务器驻留在 ADFS 服务器内以签署 Unified Manager 服务器证书请求。

#### 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。

## 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 之前先通过安全身份提供商 (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是否成功。
- 您必须至少创建一个具有应用程序管理员角色的远程用户或远程组。
- 身份提供商 (IdP) 必须受 Unified Manager 支持，并且必须进行配置。
- 您必须拥有 IdP URL 和元数据。
- 您必须有权访问 IdP 服务器。

从 Unified Manager 启用 SAML 身份验证后，用户无法访问图形用户界面，直到使用 Unified Manager 服务器主机信息配置 IdP。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。

显示配置 IdP 连接所需的字段。

3. 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。

如果可以从 Unified Manager 服务器直接访问 IdP 服务器，则可以在输入 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。

您现在可以使用此信息配置 IdP 服务器。

5. 单击“保存”。

将显示一个消息框，确认您是否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。

下次授权的远程用户尝试访问 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。



当使用 ADFS 作为身份提供者时，Unified Manager GUI 不遵守 ADFS 超时，并将继续工作，直到达到 Unified Manager 会话超时。您可以通过单击 常规 > 功能设置 > 不活动超时 来更改 GUI 会话超时。

## 更改用于 **SAML** 身份验证的身份提供者

您可以更改 Unified Manager 用于对远程用户进行身份验证的身份提供商 (IdP)。

#### 开始之前

- 您必须拥有 IdP URL 和元数据。
- 您必须有权访问 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. 输入新的 IdP URI 以及将 Unified Manager 服务器连接到 IdP 所需的 IdP 元数据。

如果可以直接从 Unified Manager 服务器访问 IdP，则可以在输入 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”。

将显示一个消息框来确认您是否要更改配置。

5. 单击“确定”。

访问新的 IdP 并输入 Unified Manager 服务器 URI 和元数据以完成配置。

下次授权的远程用户尝试访问 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。

## 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 安全证书的任何更改都要求您更新 SAML 身份验证配置设置。如果您重命名主机系统、为主机系统分配新的 IP 地址或手动更改系统的安全证书，则证书会更新。

更改安全证书并重新启动 Unified Manager 服务器后，SAML 身份验证将不起作用，用户将无法访问 Unified Manager 图形界面。您必须更新 IdP 服务器和 Unified Manager 服务器上的 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\*选项的号码。

将显示一条消息，确认您要禁用 SAML 身份验证并重新启动 Unified Manager。

3. 使用更新后的 FQDN 或 IP 地址启动 Unified Manager 用户界面，将更新后的服务器证书接受到浏览器中，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“保存”。

将显示一个消息框，确认您是否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. 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。

| 身份提供者 | 配置步骤                                                                                                                                                                                                                                      |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ADFS  | <ol style="list-style-type: none"> <li>删除 ADFS 管理 GUI 中现有的依赖方信任条目。</li> <li>使用 `saml_sp_metadata.xml` 来自更新的 Unified Manager 服务器。</li> <li>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。</li> <li>重新启动 ADFS Windows 服务。</li> </ol> |
| 口令    | <ol style="list-style-type: none"> <li>将 Unified Manager 服务器的新 FQDN 更新到 `attribute-filter.xml` 和 `relying-party.xml` 文件。</li> <li>重新启动 Apache Tomcat Web 服务器并等待端口 8005 上线。</li> </ol>                                                     |

9. 登录 Unified Manager 并通过您的 IdP 验证 SAML 身份验证是否按预期工作。

## 禁用 SAML 身份验证

当您想要在远程用户登录 Unified Manager Web UI 之前停止通过安全身份提供商 (IdP) 对其进行身份验证时，可以禁用 SAML 身份验证。当禁用 SAML 身份验证时，配置的目录服务提供商（例如 Active Directory 或 LDAP）将执行登录身份验证。

禁用 SAML 身份验证后，除了配置的远程用户之外，本地用户和维护用户也将能够访问图形用户界面。

如果您无法访问图形用户界面，您还可以使用 Unified Manager 维护控制台禁用 SAML 身份验证。



禁用 SAML 身份验证后，Unified Manager 会自动重新启动。

### 步骤

1. 在左侧导航窗格中，单击“常规”>“**SAML 身份验证**”。
2. 取消选中\*启用 SAML 身份验证\*复选框。
3. 单击“保存”。

将显示一个消息框，确认您是否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 登录页面输入其凭据。

访问您的 IdP 并删除 Unified Manager 服务器 URI 和元数据。

## 从维护控制台禁用 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。如

果配置错误或无法访问 IdP，则可能会发生这种情况。

开始之前

您必须以维护用户身份访问维护控制台。

当禁用 SAML 身份验证时，配置的目录服务提供商（例如 Active Directory 或 LDAP）将执行登录身份验证。除了配置的远程用户之外，本地用户和维护用户也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，Unified Manager 会自动重新启动。

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\*选项的号码。

将显示一条消息，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。

## SAML 身份验证页面

您可以使用 SAML 身份验证页面配置 Unified Manager，以便通过安全身份提供商 (IdP) 使用 SAML 对远程用户进行身份验证，然后他们才能登录 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 身份验证复选框以使用安全身份提供者启用身份验证。

### • IdP URI

从 Unified Manager 服务器访问 IdP 的 URI。下面列出了示例 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”按钮来填充此字段。

- **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**

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

您可以在 Unified Manager 服务器上使用 LDAP 或 Active Directory 启用身份验证，并将其配置为与您的服务器协同工作以对远程用户进行身份验证。

要启用远程身份验证、设置身份验证服务和添加身份验证服务器，请参阅上一节“配置 Unified Manager 以发送警报通知”。

### 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“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“保存”。

### 删除身份验证服务器

如果您想阻止 Unified Manager 服务器与身份验证服务器通信，您可以删除该身份验证服务器。例如，如果您想要更改管理服务器正在与之通信的身份验证服务器，您可以删除该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。

当您删除身份验证服务器时，该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. 选择一个或多个要删除的身份验证服务器，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。

通过 **Active Directory** 或 **OpenLDAP** 执行的身份验证

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通信，以便身份验证服务器内的用户可以访问 Unified Manager。

您可以使用以下预定义身份验证服务之一，也可以指定您自己的身份验证服务：

- 微软活动目录



您不能使用 Microsoft 轻量级目录服务。

- 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。管理服务器使用轻量级目录访问协议 (LDAP) 对配置的身份验证服务器内的远程用户进行身份验证。

对于在 Unified Manager 中创建的本地用户，管理服务器维护自己的用户名和密码数据库。管理服务器执行身份验证，并且不使用 Active Directory 或 OpenLDAP 进行身份验证。

审核日志记录

您可以使用审计日志检测审计日志是否已被泄露。用户执行的所有活动都受到监控并记录在审计日志中。审核针对Active IQ Unified Manager的所有用户界面和公开的 API 功能进行。

您可以使用\*审计日志：文件视图\*来查看和访问Active IQ Unified Manager中可用的所有审计日志文件。审计日志：文件视图中的文件根据其创建日期列出。此视图显示从安装或升级到系统中现在捕获的所有审计日志的信息。每当您在 Unified Manager 中执行操作时，信息都会更新并可在日志中获取。使用“文件完整性状态”属性捕获每个日志文件的状态，该属性受到主动监控以检测日志文件的篡改或删除。当系统中有审计日志时，审计日志可以具有以下状态之一：

| 状态  | 描述                   |
|-----|----------------------|
| 积极的 | 当前正在记录日志的文件。         |
| 正常  | 系统中处于非活动状态、压缩并存储的文件。 |

| 状态   | 描述                    |
|------|-----------------------|
| 被篡改  | 该文件已被手动编辑过的用户破坏。      |
| 手动删除 | 已被授权用户删除的文件。          |
| 滚动删除 | 根据滚动配置策略，由于滚动而被删除的文件。 |
| 意外删除 | 由于未知原因而被删除的文件。        |

审计日志页面包括以下命令按钮：

- 配置
- 删除
- 下载

使用 **DELETE** 按钮可以删除审计日志视图中列出的任何审计日志。您可以删除审计日志，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 列列出了原因以及执行删除操作的用户的姓名。



删除日志文件将导致文件从系统中删除，但数据库表中的条目不会被删除。

您可以使用审计日志部分中的 **DOWNLOAD** 按钮从Active IQ Unified Manager下载审计日志并导出审计日志文件。标记为“正常”或“篡改”的文件以压缩文件形式下载`.gzip`格式。

审计日志文件定期归档并保存到数据库以供参考。存档之前，审计日志经过数字签名以维护安全性和完整性。

生成完整的AutoSupport包时，支持包将包括存档和活动审计日志文件。但是，当生成轻量级支持包时，它仅包含活动审计日志。不包括存档的审计日志。

## 配置审计日志

您可以使用审计日志部分中的“配置”按钮来配置审计日志文件的滚动策略，并为审计日志启用远程日志记录。

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\*中的值。字段 **TOTAL AUDIT LOG SIZE** 中的值是系统中存在的审计日志数据的总大小。滚动策略由字段 **AUDIT LOG RETENTION DAYS**、**MAX FILE SIZE** 和 **TOTAL AUDIT LOG SIZE** 中的值决定。当审计日志备份的大小达到\*TOTAL AUDIT LOG SIZE\*中配置的值时，将删除第一个存档的文件。这意味着最旧的文件被删除。但文件条目仍然在数据库中可用，并被标记为“Rollover Delete”。**AUDIT LOG RETENTION DAYS** 值表示审计日志文件保留的天数。任何比此字段中设置的值更旧的文件都会被翻转。

## 步骤

1. 单击\*审计日志\*>>\*配置\*。
2. 在 **MAX FILE SIZE**、**TOTAL AUDIT LOG SIZE** 和 **AUDIT LOG RETENTION DAYS** 中输入值。

如果您想启用远程日志记录，那么您应该选择\*启用远程日志记录\*。 /// 2025-6-11, OTHERDOC-133

## 启用审计日志的远程记录

您可以在“配置审计日志”对话框中选中“启用远程日志记录”复选框来启用远程审计日志记录。您可以使用此功能将审计日志传输到远程 Syslog 服务器。这将使您能够在空间受限的情况下管理审计日志。

审计日志的远程记录提供了防篡改备份，以防 Active IQ Unified Manager 服务器上的审计日志文件被篡改。

### 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。

显示用于配置远程日志记录的附加字段。

2. 输入您要连接的远程服务器的 **HOSTNAME** 和 **PORT**。
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。

证书应上传至 .pem 格式。此证书应从目标 Syslog 服务器获取，并且不应过期。证书应包含所选的“主机名”作为 `SubjectAltName (SAN)` 属性。

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 **FORMAT** 和 **PROTOCOL** 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。

在保存审计日志配置之前，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，您可能需要创建客户端身份验证证书的哈希值。

示例：syslog-ng 需要使用以下命令创建证书的 <hash> openssl x509 -noout -hash -in cert.pem，然后您应该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。

您将被重定向到审计日志页面。



\*连接超时\*值会影响配置。如果配置响应的时间比定义值长，则可能由于连接错误导致配置失败。要建立成功的连接，请增加\*连接超时\*值，然后再次尝试配置。

## 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通信，以对尝试登录 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，您可以使用身份验证服务器启用远程身份验证。

- 认证服务

使您能够配置管理服务器以在目录服务提供商（例如 Active Directory、OpenLDAP）中对用户进行身份验证，或指定您自己的身份验证机制。仅当您启用了远程身份验证时，您才可以指定身份验证服务。

- 活动目录

- 管理员名称

- 指定认证服务器的管理员名称。

- 密码

- 指定访问认证服务器的密码。

- 基本可分辨名称

- 指定远程用户在认证服务器中的位置。例如，如果认证服务器的域名是+ou@domain.com+，那么基本可分辨名称就是\*cn=ou,dc=domain,dc=com\*。

- 禁用嵌套组查找

- 指定是否启用或禁用嵌套组查找选项。默认情况下此选项是禁用的。如果您使用 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

- 指定访问认证服务器的密码。

- 基本可分辨名称

- 指定远程用户在认证服务器中的位置。例如，如果认证服务器的域名是+ou@domain.com+，那么基本可分辨名称就是\*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。

- 其他的

- 绑定可分辨名称

- 指定绑定可分辨名称，该名称与基本可分辨名称一起使用，以在您配置的身份验证服务器中查找远程用户。

- 绑定密码

指定访问认证服务器的密码。

- 基本可分辨名称

指定远程用户在认证服务器中的位置。例如，如果认证服务器的域名是+ou@domain.com+，那么基本可分辨名称就是\*cn=ou,dc=domain,dc=com\*。

- 协议版本

指定您的身份验证服务器支持的轻量级目录访问协议 (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的属性名称，该属性包含要由管理服务器进行身份验证的用户登录名。

- 组成员资格属性

指定一个值，该值根据用户的身份验证服务器中指定的属性和值为远程用户分配管理服务器组成员身份。

- UGID

如果远程用户作为身份验证服务器中 GroupOfUniqueNames 对象的成员，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

指定是否启用或禁用嵌套组查找选项。默认情况下此选项是禁用的。如果您使用 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的各个成员的信息的属性名称。

- 用户对象类

指定远程认证服务器中用户的对象类。

- 组对象类

指定远程认证服务器中所有组的对象类。



您为 *\_Member\_*、*User Object Class* 和 *Group Object Class* 属性输入的值应与在 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验证远程用户的身份验证服务器。远程用户或组的凭据由身份验证服务器维护。

- 命令按钮

使您能够添加、编辑或删除身份验证服务器。

- 添加

使您能够添加身份验证服务器。

如果您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），那么您还可以添加合作伙伴身份验证服务器。当其中一个身份验证服务器无法访问时，这使得管理服务器能够与合作伙伴进行通信。

- 编辑

使您能够编辑选定身份验证服务器的设置。

- 删除

删除选定的认证服务器。

- 姓名或 IP 地址

显示用于在管理服务器上验证用户的验证服务器的主机名或 IP 地址。

- 港口

显示认证服务器的端口号。

- 测试认证

此按钮通过验证远程用户或组来验证您的身份验证服务器的配置。

测试时，如果仅指定用户名，管理服务器会在认证服务器中搜索远程用户，但不会对用户进行认证。如果您同时指定用户名和密码，管理服务器将搜索并验证远程用户。

如果远程身份验证被禁用，则您无法测试身份验证。

## 管理安全证书

您可以在 Unified Manager 服务器中配置 HTTPS，以通过安全连接监控和管理您的集群。

### 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到的证书进行比较，以确保浏览器与 Unified Manager 的加密连接不会被拦截。

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 的主题备用名称 (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多有关安全证书的详细信息，您可以在浏览器中查看连接证书。

## 下载 HTTPS 证书签名请求

您可以下载当前 HTTPS 安全证书的认证签名请求，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。

#### 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。

## 安装 CA 签名并返回的 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。

#### \*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
- 包含链中的所有证书，从 Unified Manager 服务器证书到根签名证书，包括任何存在的中间证书

您必须具有应用程序管理员角色。



如果创建 CSR 的证书有效期超过 397 天，则 CA 会在签署并返回证书之前将有效期缩短至 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...”找到要上传的文件。
4. 选择文件，然后单击\*安装\*来安装该文件。

有关信息，请参阅[“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-----
```

## 安装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，并使用外部工具（如 OpenSSL、BoringSSL、LetsEncrypt）生成。

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”。“常规”部分下的“HTTPS 证书”页面中提供了“安装 **HTTPS** 证书”选项。您上传的文件应采用以下输入格式。

1. 属于Active IQ Unified Manager主机的服务器的私钥
2. 与私钥匹配的服务器证书
3. 反向直到根的 CA 证书，用于签署上述证书

### 加载带有 **EC** 密钥对的证书的格式

允许的曲线是“prime256v1”和“secp384r1”。带有外部生成的 EC 对的证书样本：

```
-----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 密钥对允许的密钥大小为 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，您应该重新启动Active IQ Unified Manager实例以使更改生效。

### 上传外部生成的证书时进行检查

系统在上传使用外部工具生成的证书时执行检查。如果任何检查失败，则证书被拒绝。还包括对产品内 CSR 生成的证书和使用外部工具生成的证书的验证。

- 输入中的私钥根据输入中的主机证书进行验证。
- 主机证书中的通用名称 (CN) 与主机的主机 FQDN 进行检查。
- 主机证书的通用名称 (CN) 不能为空或空白，并且不能设置为localhost。
- 证书的有效起始日期不应为将来日期，且证书的有效到期日期不应为过去日期。
- 如果存在中级 CA 或 CA，则证书的有效开始日期不应在未来，有效到期日期不应在过去。



输入中的私钥不应该被加密。如果有任何私钥被加密，那么系统就会拒绝它们。

#### 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\[\"ActiveIQ Unified Manager 无法安装外部生成的证书\"\]](https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate[\)

## 证书管理的页面描述

您可以使用 HTTPS 证书页面查看当前的安全证书并生成新的 HTTPS 证书。

### HTTPS 证书页面

HTTPS 证书页面使您能够查看当前安全证书、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是安装期间生成的证书。

## 命令按钮

命令按钮使您能够执行以下操作：

- 下载 **HTTPS** 证书签名请求

下载当前安装的 HTTPS 证书的认证请求。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署并返回安全证书后上传并安装该证书。重新启动管理服务器后，新证书将生效。

- 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，新证书将生效。

## 重新生成 **HTTPS** 证书对话框

“重新生成 HTTPS 证书”对话框使您能够自定义安全信息，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”选择使您能够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。

- 状态

可选。公司所在的州或省/自治区/直辖市位置（非缩写）。

- 国家

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。

- 其他名称

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。

如果您想从证书中的备用名称字段中删除本地识别信息，请选中“排除本地识别信息（例如 localhost）”复选框。选中此复选框后，只有您在字段中输入的内容才会在备用名称字段中使用。当留空时，生成的证书将根本没有备用名称字段。

- 密钥大小（密钥算法：**RSA**）

密钥算法设置为RSA。您可以从以下密钥大小中选择一个：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。如果您从以前的版本升级，您可能会看到以前的证书有效性保持不变。

有关详细信息，请参阅 ["生成 HTTPS 证书"](#)。

# 监视和管理存储

## Active IQ Unified Manager简介

Active IQ Unified Manager（以前称为OnCommand Unified Manager）使您能够从单一界面监控和管理ONTAP存储系统的运行状况和性能。

Unified Manager 提供以下功能：

- 发现、监控和通知安装了ONTAP软件的系统。
- 仪表板显示环境的容量、安全性和性能健康状况。
- 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到活动增加影响的工作负载。
- 提供可执行的建议纠正措施来解决某些事件和事件，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（例如 LUN 或文件共享），并分配性能服务级别来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。

## Active IQ Unified Manager健康监控简介

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运行ONTAP软件的大量系统。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、管理保护功能以及捆绑诊断数据并将其发送给技术支持。

您可以使用 Unified Manager 来监控您的集群。当集群中出现问题时，Unified Manager 会通过事件通知您此类问题的详细信息。有些事件还会为您提供可以采取的补救措施来纠正问题。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 通过将存储对象与注释关联来管理环境中的存储对象。您可以创建自定义注释，并通过规则将集群、存储虚拟机 (SVM) 和卷与注释动态关联。

您还可以使用容量和运行状况图表中提供的信息来为各个集群对象规划集群对象的存储要求。

### 物理和逻辑容量

Unified Manager 利用用于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（例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）。逻辑空间是指理论上如何使用空间，不考虑重复数据删除或压缩的结果。“使用的逻辑空间”是使用的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）节省的空间。该测量值通常看起来大于物理使用容量，因为这没有反映数据压缩和物理空间的其他减少。因此，总逻辑容量可能高于配置的空间。

## 容量测量单位

Unified Manager 根据 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 ONTAP 的所有版本，吞吐量使用的单位仍然是每秒千字节 (Kbps)、每秒兆字节 (Mbps)、每秒千兆字节 (Gbps) 或每秒太字节 (Tbps) 等等。

| Unified Manager for ONTAP 9.10.0 及更早版本中显示的容量单位 | Unified Manager for ONTAP 9.10.1 中显示的容量单位 | 计算方式                        | 以字节为单位的值             |
|------------------------------------------------|-------------------------------------------|-----------------------------|----------------------|
| 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 |

## Active IQ Unified Manager 性能监控简介

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，您还可以指定某些性能计数器的最大值，以便在超过阈值时生成事件。Unified Manager 会向您发出有关这些性能事件的警报，以便您采取纠正措施，并使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 监控两种类型工作负载的性能：

- 用户定义的工作负载

这些工作负载包括您在集群中创建的 FlexVol 卷和 FlexGroup 卷。

- 系统定义的工作负载

这些工作负载由内部系统活动组成。

## 使用 Unified Manager REST API

Active IQ Unified Manager为您提供 REST API 来查看有关监控和管理存储环境的信息。此外，您还可以使用这些 API 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ONTAP管理的集群上执行ONTAP API。

有关 Unified Manager REST API 的信息，请参阅["Active IQ Unified Manager REST API 入门"](#)。

## Unified Manager 服务器的功能

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。它提供发现、监控、基于角色的访问控制 (RBAC)、审计和日志记录等基础设施服务。

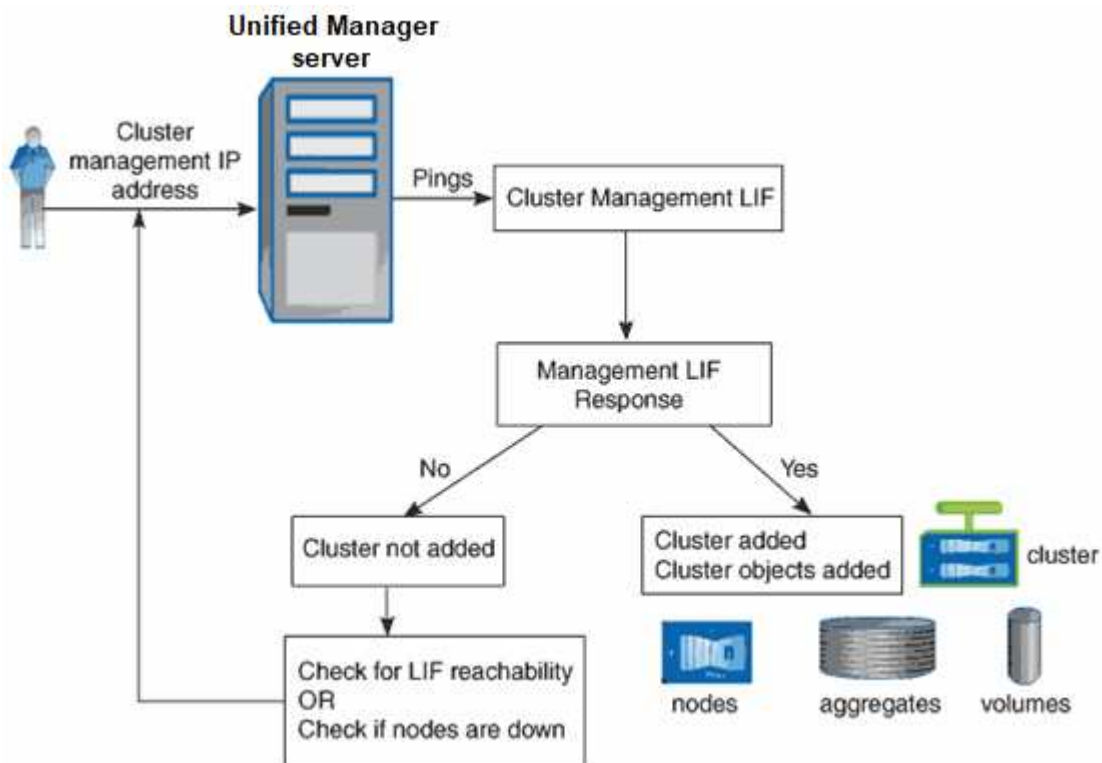
Unified Manager 收集集群信息，将数据存储在数据库中，并分析数据以查看是否存在任何集群问题。

发现过程如何运作

将集群添加到 Unified Manager 后，服务器会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。

默认监控间隔为 15 分钟：如果您已将集群添加到 Unified Manager 服务器，则需要 15 分钟才能在 Unified Manager UI 中显示集群详细信息。

下图说明了Active IQ Unified Manager中的发现过程：





# 了解用户界面

Unified Manager 用户界面主要由一个仪表板组成，该仪表板提供所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。

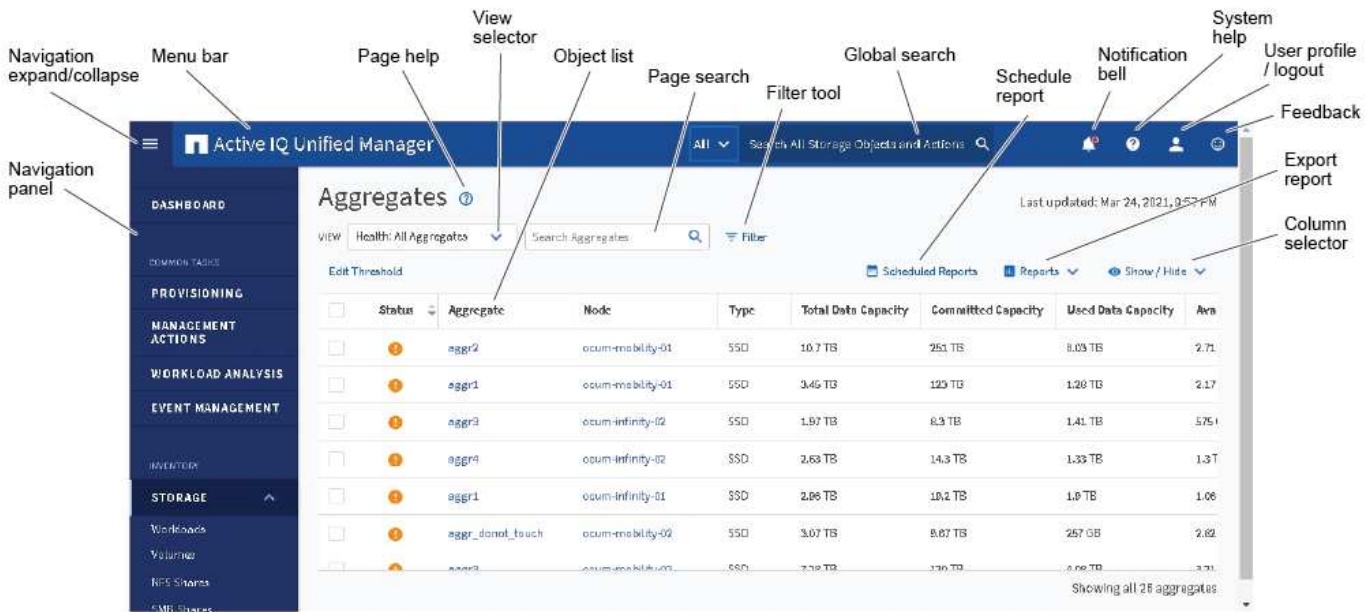
您可以选择首选视图并根据需要使用操作按钮。您的屏幕配置保存在工作区中，以便在启动 Unified Manager 时可以使用您需要的所有功能。但是，当您从一个视图导航到另一个视图，然后导航回来时，视图可能会不一样。

## 典型窗口布局

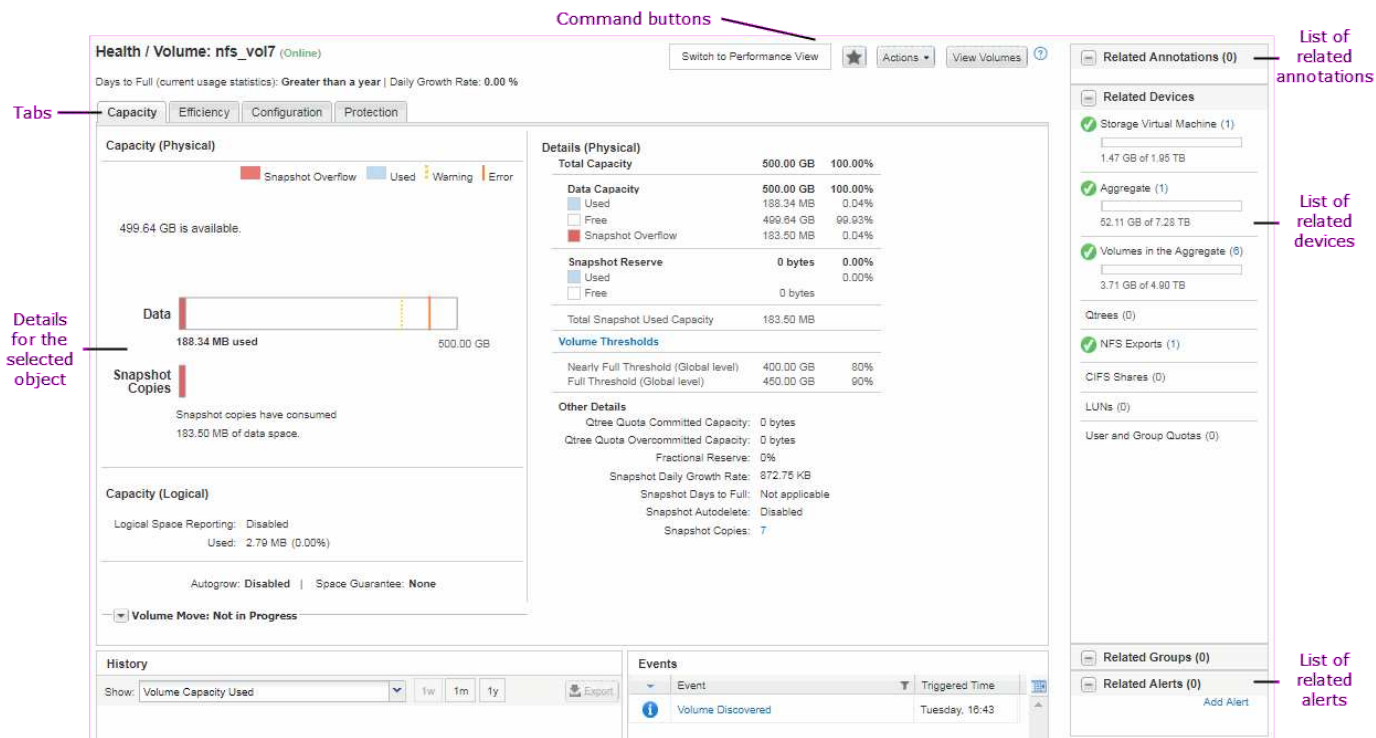
了解典型的窗口布局有助于您有效地导航和使用Active IQ Unified Manager 。大多数 Unified Manager 窗口类似于两种常规布局之一：对象列表或详细信息。建议的显示设置至少为 1280 x 1024 像素。

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



## 窗口布局自定义

Active IQ Unified Manager使您能够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，您可以控制哪些数据可查看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。单击列标题时，排序箭头 (▲ 和 ▼) 出现在该列中。

### • 过滤

您可以点击过滤器图标 ( ) 应用过滤器来定制存储和网络对象页面上的信息显示，以便只显示符合所提供条件的条目。您可以从“过滤器”窗格应用过滤器。

使用“过滤器”窗格，您可以根据所选的选项过滤大多数列。例如，在“健康状况：所有卷”视图中，您可以使用“过滤器”窗格，通过选择“状态下”下的相应过滤器选项来显示所有处于脱机状态的卷。

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”列中的过滤器来过滤大于 20.45 GB 的数据，则实际容量 20.454 GB 将显示为 20.45 GB。同样，如果过滤小于 20.45 GB 的数据，则实际容量 20.449 GB 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 %”列中的过滤器来过滤大于 20.45% 的数据，则实际容量 20.454% 将显示为 20.45%。同样的，如果过滤小于20.45%的数据，那么实际容量20.449%就会显示为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。一旦选择了适当的列，您就可以使用鼠标拖动它们来重新排序。

- 搜索中

您可以使用搜索框搜索某些对象属性，以帮助优化库存页面中的项目列表。例如，您可以输入“云”来优化卷清单页面中的卷列表，以查看其中包含单词“云”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的值 `(.csv)` 文件，`(.pdf)` 文档或 Microsoft Excel `(.xlsx)` 文件并使用导出的数据来构建报告。

## 使用 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。

每个选项卡和 Unified Manager 用户界面的菜单栏中均提供帮助。

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，请单击  \* > 菜单栏中的 帮助/文档。

您可以通过展开导航窗格中目录的任意部分来找到更详细的信息。

- 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。

## 为您最喜欢的帮助主题添加书签

在“帮助收藏夹”选项卡中，您可以为经常使用的帮助主题添加书签。帮助书签可让您快速访问您喜欢的主题。

### 步骤

1. 导航到您想要添加为收藏夹的帮助主题。
2. 单击“收藏夹”，然后单击“添加”。

## 搜索存储对象

要快速访问特定对象，您可以使用菜单栏顶部的“搜索所有存储对象”字段。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过滤它们。

### 开始之前

- 您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。
- 有效搜索必须至少包含三个字符。

当使用下拉菜单值“全部”时，全局搜索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 25 个搜索结果。

果。您可以从下拉菜单中选择特定的对象类型，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。

您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
- 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来导航到该对象的健康详细信息页面。如果某个对象没有直接的健康页面，则会显示其父对象的健康页面。例如，搜索特定 LUN 时，将显示该 LUN 所在的 SVM 详细信息页面。

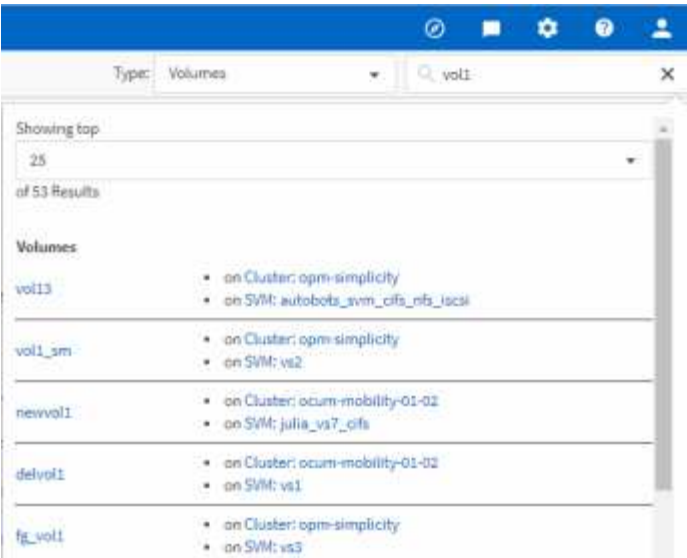


无法在全局搜索栏中搜索端口和 LIF。

#### 步骤

1. 从菜单中选择一种对象类型，以优化仅针对单一对象类型的搜索结果。
2. 在\*搜索所有存储对象\*字段中输入对象名称的至少三个字符。

在此示例中，下拉框选择了卷对象类型。在\*搜索所有存储对象\*字段中输入“vol1”将显示名称中包含这些字符的所有卷的列表。



### 将存储数据导出为报告

您可以以多种输出格式导出存储数据，然后使用导出的数据来构建报告。例如，如果有 10 个尚未解决的关键事件，您可以从事件管理库存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。

您可以将数据导出到`.csv`文件，`.xlsx`文件，或`.pdf`从\*存储\*和\*网络\*库存页面获取文档并使用导出的数据来构建报告。产品中还有其他位置仅`.csv`或者`.pdf`可以生成文件。

#### 步骤

1. 请执行以下操作之一：

| 如果您想导出...        | 操作                                                            |
|------------------|---------------------------------------------------------------|
| 存储对象清单详细信息       | 单击左侧导航菜单中的“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，或您创建的任何自定义视图。      |
| QoS 策略组详细信息      | 单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。                              |
| 活动详情             | 单击左侧导航菜单中的“事件管理”。                                             |
| 存储对象 Top 10 性能详情 | 单击“存储”>“集群”>“性能：所有集群”，然后选择一个集群并选择“最佳表现者”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** 以确认导出请求。

从“最佳表现者”选项卡中，您可以选择下载您正在查看的单个集群或数据中心中所有集群的统计报告。

文件已下载。

- 4. 在适当的应用程序中打开该文件。

相关信息

["运行状况/集群清单页面"](#)

["计划报告"](#)

过滤库存页面内容

您可以在 Unified Manager 中过滤库存页面数据，以便根据特定条件快速定位数据。您可以使用过滤功能来缩小 Unified Manager 页面的内容范围，以仅显示您感兴趣的结果。这是一种非常高效的方法，它可以仅显示您感兴趣的数据。

使用\*过滤\*根据您的喜好自定义网格视图。可用的过滤选项基于网格中查看的对象类型。如果当前应用了过滤器，则已应用的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参数。

| 参数      | 验证                               |
|---------|----------------------------------|
| 字符串（文本） | 运算符包括*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 <b>is</b> 和 <b>is not</b> 。 |

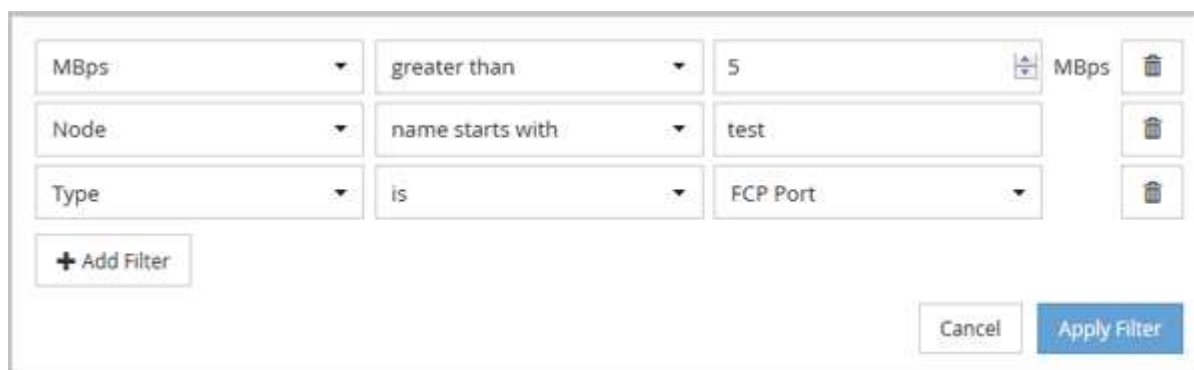
每个过滤器都需要列、运算符和值字段；可用的过滤器反映当前页面上可过滤的列。您最多可以应用四个过滤器。过滤结果基于组合过滤参数。过滤结果适用于过滤搜索中的所有页面，而不仅仅是当前显示的页面。

您可以使用过滤面板添加过滤器。

- 1. 在页面顶部，单击“过滤器”按钮。显示过滤面板。
- 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. 要添加另一个过滤器，请单击“+添加过滤器”。一个额外的筛选字段即会显示。使用上述步骤中所述的过程完成此筛选器。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”。过滤选项应用于网格，过滤器的数量显示在过滤器按钮的右侧。
- 7. 使用过滤面板通过单击要删除的过滤器右侧的垃圾桶图标来删除单个过滤器。
- 8. 要删除所有过滤器，请单击过滤面板底部的“重置”。

## 筛选示例

该图显示了带有三个过滤器的过滤面板。当您拥有的过滤器少于四个时，将显示“+添加过滤器”按钮。



The screenshot shows a filter panel with three rows of filters. Each row has a dropdown menu for the field, a dropdown for the operator, and a text input for the value. The first row is 'MBps' with operator 'greater than' and value '5'. The second row is 'Node' with operator 'name starts with' and value 'test'. The third row is 'Type' with operator 'is' and value 'FCP Port'. To the right of each filter is a trash icon. At the bottom left is a '+ Add Filter' button. At the bottom right are 'Cancel' and 'Apply Filter' buttons.

单击“应用过滤器”后，“过滤”面板将关闭，应用过滤器，并显示已应用的过滤器数量（  3 ）。

## 从通知铃查看活动事件

通知铃声（  ）提供了一种快速查看 Unified Manager 正在跟踪的最重要的活动事件的方法。

活动事件列表提供了一种查看所有集群上严重、错误、警告和升级事件总数的方法。此列表包括前 7 天的事件，但不包括信息事件。您可以单击链接来显示您最感兴趣的事件列表。

请注意，当集群不可访问时，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。规模监控问题（例如管理站空间或 RAM 不足）也会显示在此页面上。

### 步骤

1. 在菜单栏中，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 容量”或“4 性能”。

## 从仪表板监控和管理集群

信息板可提供有关受监控 ONTAP 系统当前运行状况的累积概览信息。仪表板提供“面板”，使您能够评估正在监控的集群的整体容量、性能和安全健康状况。

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        | 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，这些解决方案将显示在此面板中，并带有 修复 按钮。                                |
| 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    | 显示分配给每个定义的性能服务级别的符合和不符合的工作负载总数。                                                              |
| 安全性       | 显示合规或不合规的集群数量、合规或不合规的 SVM 数量以及加密或未加密的卷数量。                                                    |
| 保护        | 显示受 SVM-DR 关系保护的存储虚拟机的数量、受 SnapMirror 关系保护的卷的数量、受 Snapshot 保护的卷的数量以及受 MetroCluster 保护的集群的数量。 |
| 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。                                                      |

## 信息板页面

仪表板页面有“面板”，显示您正在监控的集群的高级容量、性能和安全健康状况。此页面还提供了一个管理操作面板，其中列出了 Unified Manager 可以采取的修复措施来解决某些事件。

此外，大多数面板还会显示相应类别的活动事件数量，以及过去 24 小时内增加的新事件数量。此信息有助于确定可能需要进一步分析的集群，以便解决相应事件。单击事件将显示热门事件，并提供指向事件管理库存页面的链接，该页面经过筛选可显示该类别中的活动事件。

在仪表板顶部，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，然后深入查看各个集群以查看相关详细信息。



下面列出的一些面板将根据您的配置出现在仪表板上。

### 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。当可用时，这些分辨率将显示在此面板中，并带有“修复”或“修复全部”按钮。您可以从 Unified Manager 立即修复这些问题，而不必使用 ONTAP System Manager 或 ONTAP CLI。要查看所有问题，请点击查看[直接从 Unified Manager 修复 ONTAP 问题](#)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（应用存储效率节省后）和物理可用容量（不包括潜在的存储效率节省）、磁盘预计满载的天数以及基于配置的ONTAP存储效率设置的数据缩减率（不含 Snapshot 副本）。此外，它还会列出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库存页面。单击“剩余容量天数”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和云层上的每个磁盘类型排序的数据聚合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

在查看所有集群时，此面板会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之前的天数（基于每日增长率）。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“剩余性能容量天数”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，以及预计这三个指标达到其上限的天数。

## 工作负载 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指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总数。它还显示未分配 PSL 的工作负载数量。单击条形图可转到“工作负载”页面中分配给该策略的符合工作负载。单击条形图后面的数字即可查看分配给该策略的符合和不符合的工作负载。

## 安全面板

根据您当前的视图，安全面板显示所有集群或单个集群的高级安全状态。该面板显示：

- 过去 24 小时内收到的安全事件列表。点击事件，在事件详情页面查看事件详情
- 集群安全状态（合规和不合规集群的数量）
- 存储虚拟机安全状态（合规和不合规存储虚拟机的数量）
- 卷加密状态（已加密或未加密的卷的数量）
- 卷反勒索软件状态（启用或禁用反勒索软件的卷数量）

您可以点击合规与不合规集群、存储虚拟机、加密与非加密卷、卷防勒索状态柱状图，进入相应页面，查看已筛选集群、存储虚拟机、卷的安全详情。

合规性基于 ["NetApp ONTAP 9 安全强化指南"](#)。单击面板顶部的右箭头可在“安全”页面上查看所有集群的安全详细信息。有关信息，请参阅[查看集群和存储虚拟机的详细安全状态](#)。

## 数据保护面板

此面板显示数据中心内单个或所有集群的数据保护摘要。它显示ONTAP中过去 24 小时内发生的数据保护事件、

MetroCluster事件和活动事件的总数。单击每个事件的链接即可进入事件详细信息页面。您可以单击“查看全部”链接来查看事件管理库存页面中的所有活动保护事件。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，将考虑源集群中的卷数。
- 通过 IP 或 FC 受MetroCluster配置保护的数据中心中的集群数量或所有集群。
- 根据滞后状态，具有SnapMirror恢复点目标 (RPO) 滞后的卷关系的数量。

您可以将鼠标悬停在屏幕上来查看相应的计数和图例。您可以单击面板顶部的右箭头来查看数据保护页面上的单个或所有集群的详细信息。您还可以点击：

- 未受保护的卷和受 Snapshot 副本保护的卷的条形图，可转到“卷”页面并查看详细信息。
- 受MetroCluster配置保护或未受保护的集群的条形图，可转到“集群”页面并查看详细信息。
- 所有关系的条形图都会转到“关系”页面，其中会根据源集群过滤详细信息。

有关详细信息，请参阅 ["查看卷保护状态"](#)。

## 使用情况概览面板

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。

查看单个集群时，您可以选择按最高 IOPS、最高吞吐量（MB/s）或最高使用逻辑容量排序查看工作负载。

## 相关信息

["使用 Unified Manager 自动修复修复问题"](#)

["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"](#)

["音量/健康详情页面"](#)

["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** 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”选项为触发 Unified

Manager 事件的许多ONTAP问题提供了修复。

您可以通过选择左侧导航窗格上的“管理操作”选项直接从“管理操作”页面修复问题。您还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管理操作。

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采取特定措施。当可用时，这些解决方案将显示在管理操作中，并带有\*修复\*按钮。单击“修复”按钮即可修复该问题。您必须具有应用程序管理员或存储管理员角色。

Unified Manager 向集群发送ONTAP命令以进行请求的修复。修复完成后，此事件将被废弃。

某些管理操作使您能够使用“修复全部”按钮修复多个存储对象上的相同问题。例如，可能有 5 个卷发生“卷空间已满”事件，可以通过单击“启用卷自动增长”的 修复全部 管理操作来解决。只需单击一下，即可修复 5 个卷上的此问题。

有关可以使用自动修复功能管理的ONTAP问题和功能的信息，请参阅["Unified Manager 可以修复哪些问题"](#)。

当我看到“修复”或“修复全部”按钮时，我有哪些选项

管理操作页面为您提供了“修复”或“修复全部”按钮，用于修复 Unified Manager 通过事件通知的问题。

我们建议您根据需要单击按钮来解决问题。但是，如果您不确定是否要按照 Unified Manager 的建议解决问题，则可以执行以下操作：

| 您希望做什么？                              | 行动                                                   |
|--------------------------------------|------------------------------------------------------|
| 让 Unified Manager 修复所有已识别对象上的问题。     | 单击“修复全部”按钮。                                          |
| 此时不要修复任何已识别对象的问题，并隐藏此管理操作，直到再次引发该事件。 | 单击向下箭头，然后单击“全部关闭”。                                   |
| 仅修复部分已识别对象的问题。                       | 单击管理操作的名称以展开列表并显示所有单独的*修复*操作。然后按照修复或解除单个管理操作的步骤进行操作。 |

| 您希望做什么？                     | 操作               |
|-----------------------------|------------------|
| 让 Unified Manager 修复该问题。    | 单击“修复”按钮。        |
| 此时不要修复该问题并隐藏此管理操作，直到事件再次发生。 | 单击向下箭头，然后单击“关闭”。 |

| 您希望做什么？                | 操作                                                                                                                                                     |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 显示此事件的详细信息以更好地了解此问题。   | <ul style="list-style-type: none"> <li>单击“修复”按钮并查看将在出现的对话框中应用的修复。</li> <li>单击向下箭头，然后单击“查看事件详情”以显示事件详情页面。</li> </ul> <p>如果您想修复该问题，请在任一结果页面中单击“修复它”。</p> |
| 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，此修复会在下一个 15 分钟配置轮询中反映出来。在其他情况下，可能需要花费数小时来验证配置更改并让事件过时。

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\*进行中\*。

修复所有操作都以串行方式运行，因此当您查看\*进行中\*面板时，某些对象的状态为\*进行中\*，而其他对象的状态为\*已安排\*；这意味着它们仍在等待实施。

查看您选择修复的管理操作的状态

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 将 ONTAP 命令发送到集群后，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过滤器：

- \*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\*显示正在实施的管理行动以及计划实施的管理行动。
- \*推荐\*显示所有受监控集群当前处于活动状态的所有管理操作。

步骤

- 单击左侧导航窗格上的“管理操作”。或者，点击  在\*仪表板\*上的\*管理操作\*面板顶部，选择您想要查看的视图。  
  
将显示“管理操作”页面。
- 您可以单击“描述”字段中管理操作旁边的插入符号图标来查看有关该问题以及用于修复该问题的命令的详细信息。
- 要查看任何\*失败\*的操作，请在\*已完成\*视图中的\*状态\*列上进行排序。您可以使用\*过滤器\*工具来达到同样的目的。
- 如果您想查看有关失败的管理操作的更多信息，或者您决定要修复推荐的管理操作，您可以在单击管理操作旁边的插入符号图标后，从展开区域中单击“查看事件详细信息”。该页面上有一个“修复”按钮。

## Unified Manager 可以修复哪些问题

通过使用Active IQ Unified Manager的自动修复功能，您可以选择通过 Unified Manager 有效地解决某些ONTAP问题或管理某些ONTAP功能（例如反勒索软件监控）。

下表介绍了这些ONTAP问题或功能，您可以通过 Unified Manager Web UI 上的 [修复它](#) 或 [修复全部](#) 按钮直接管理这些问题或功能。

| 事件名称和描述                                                         | 管理操作           | “修复”操作                                                |
|-----------------------------------------------------------------|----------------|-------------------------------------------------------|
| <b>卷空间全满</b><br><br>该卷的空间几乎用尽，并且已突破容量满阈值。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，因此启用此功能，以便卷在需要时容量会增加。    |
| <b>索引节点全满</b><br><br>此卷的 inode 已用完，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%。                                   |
| <b>检测到存储层策略不匹配</b><br><br>该卷具有大量非活动数据，并且当前分层策略设置为“仅快照”或“无”。     | 启用自动云分层        | 由于卷已经驻留在FabricPool上，它将分层策略更改为“自动”，以便将非活动数据移动到成本较低的云层。 |
| <b>检测到存储层不匹配</b><br><br>该卷具有大量非活动数据，但它不驻留在支持云的存储层（FabricPool）上。 | 更改卷的存储层        | 将卷移动到支持云的存储层，并将分层策略设置为“自动”以将非活动数据移动到云层。               |
| <b>已禁用审核日志</b><br><br>存储虚拟机未启用审计日志                              | 为存储虚拟机启用审核日志记录 | 在存储虚拟机上启用审计日志记录。<br><br>请注意，存储虚拟机必须已经配置了本地或远程审计日志位置。  |
| <b>已禁用登录横幅</b><br><br>应启用集群的登录横幅，通过明确访问限制来提高安全性。                | 设置集群的登录横幅      | 将集群登录横幅设置为“访问仅限于授权用户”。                                |
| <b>已禁用登录横幅</b><br><br>应启用存储虚拟机的登录横幅，通过明确访问限制来提高安全性。             | 为存储虚拟机设置登录横幅   | 将存储虚拟机登录横幅设置为“仅限授权用户访问”。                              |

| 事件名称和描述                                                                                                  | 管理操作                          | “修复”操作                                                               |
|----------------------------------------------------------------------------------------------------------|-------------------------------|----------------------------------------------------------------------|
| <p>SSH 正在使用不安全密码</p> <p>带有后缀“-cbc”的密码被认为是不安全的。</p>                                                       | 从集群中删除不安全的密码                  | 从集群中删除不安全的密码 - 例如 aes192-cbc 和 aes128-cbc。                           |
| <p>SSH 正在使用不安全密码</p> <p>带有后缀“-cbc”的密码被认为是不安全的。</p>                                                       | 从存储虚拟机中删除不安全的密码               | 从存储虚拟机中删除不安全的密码 - 例如 aes192-cbc 和 aes128-cbc。                        |
| <p>已禁用 AutoSupport HTTPS 传输</p> <p>用于向技术支持发送AutoSupport消息的传输协议应该加密。</p>                                  | 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。                                    |
| <p>已超过集群负载不平衡阈值</p> <p>表示集群中节点之间的负载不平衡。当节点间性能容量使用差异超过 30% 时，生成此事件。</p>                                   | 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减少不平衡，然后移动该卷。                    |
| <p>已超过集群容量不平衡阈值</p> <p>表示集群中聚合之间的容量不平衡。当聚合之间的已用容量差异超过 70% 时，会生成此事件。</p>                                  | 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减少不平衡，然后移动该卷。                    |
| <p>已使用性能容量阈值被突破</p> <p>表示如果不通过一个或多个高度活跃的工作负载来降低利用率，则节点上的负载可能会被过度利用。当节点性能容量使用值超过100%且持续12小时以上时，生成此事件。</p> | 限制节点的高负载                      | Unified Manager 识别具有最高 IOPS 的卷，并使用历史预期和峰值 IOPS 水平应用 QoS 策略来减少节点上的负载。 |
| <p>已违反动态事件警告阈值</p> <p>表示由于某些工作负载的负载异常高，该节点已经处于过载状态。</p>                                                  | 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 水平应用 QoS 策略来减少节点上的负载。 |
| <p>无法接管</p> <p>故障转移当前已被禁用，因此在中断或重启期间对节点资源的访问将会丢失，直到节点再次可用为止。</p>                                         | 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。                            |

| 事件名称和描述                                                                                                                            | 管理操作                          | “修复”操作                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <p>选项 Cf.takeover.on_panic 配置为关闭</p> <p>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。</p>                        | 启用恐慌接管                        | Unified Manager 向集群发送适当的命令以将此设置更改为 <b>on</b> 。                                                                                        |
| <p>禁用 nodeshell 选项 snapmirror.enable</p> <p>旧的 nodeshell 选项“snapmirror.enable”设置为 <b>on</b>，这可能会在升级到ONTAP 9.3 或更高版本后在启动期间导致问题。</p> | 将 snapmirror.enable 选项设置为关闭   | Unified Manager 向集群发送适当的命令以将此设置更改为 <b>off</b> 。                                                                                       |
| <p>已启用 Telnet</p> <p>表示存在潜在的安全问题，因为 Telnet 不安全并且以未加密的方式传递数据。</p>                                                                   | 禁用 Telnet                     | Unified Manager 向集群发送适当的命令以禁用 Telnet。                                                                                                 |
| <p>配置存储虚拟机反勒索软件学习</p> <p>定期检查具有反勒索软件监控许可证的集群。验证存储虚拟机在这样的集群中是否仅支持 NFS 或 SMB 卷。</p>                                                  | 将存储虚拟机放入 `learning` 反勒索软件监控模式 | Unified Manager 将反勒索软件监控设置为 `learning` 通过集群管理控制台查看存储虚拟机的状态。存储虚拟机上创建的所有新卷上的反勒索软件监控都会自动转入学习模式。通过此功能，ONTAP 可以了解卷上的活动模式并检测由于潜在恶意攻击而导致的异常。 |
| <p>配置批量反勒索软件学习</p> <p>定期检查具有反勒索软件监控许可证的集群。验证卷在这样的集群中是否仅支持 NFS 或 SMB 服务。</p>                                                        | 将卷放入 `learning` 反勒索软件监控模式     | Unified Manager 将反勒索软件监控设置为 `learning` 通过集群管理控制台查看卷的状态。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。                                      |
| <p>启用批量反勒索软件</p> <p>定期检查具有反勒索软件监控许可证的集群。检测卷是否在 `learning` 反勒索软件监控模式超过 45 天，并确定将其置于主动模式的前景。</p>                                     | 将卷放入 `active` 反勒索软件监控模式       | Unified Manager 将反勒索软件监控设置为 `active` 通过集群管理控制台查看卷上的活动模式并检测由于潜在恶意攻击而导致的异常，并为数据保护措施创建警报。                                                |

| 事件名称和描述                                                                                      | 管理操作         | “修复”操作                                 |
|----------------------------------------------------------------------------------------------|--------------|----------------------------------------|
| <p>禁用批量反勒索软件</p> <p>定期检查具有反勒索软件监控许可证的集群。在卷上进行主动反勒索软件监控期间检测重复通知（例如，30 天内多次返回潜在勒索软件攻击的警告）。</p> | 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卷上的反勒索软件监控。 |

通过脚本覆盖管理操作

您可以创建自定义脚本并将其与警报关联，以针对特定事件采取特定操作，而不是选择“管理操作”页面或 Unified Manager 仪表板上可用的默认管理操作。

如果您想要针对某种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关联起来，并单独处理此类事件。在这种情况下，管理操作页面或 Unified Manager 仪表板上不会针对该特定事件类型生成管理操作。

## 管理集群

您可以使用 Unified Manager 监控、添加、编辑和删除集群来管理 ONTAP 集群。

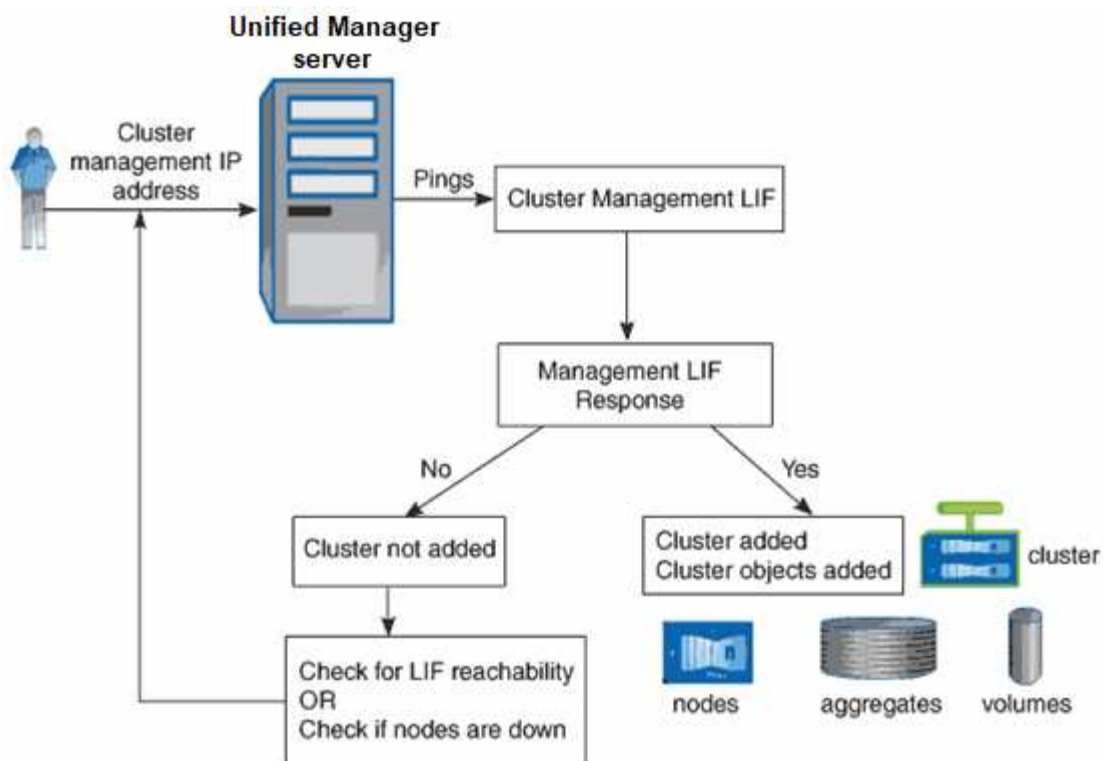
### 集群发现过程的工作原理

将集群添加到 Unified Manager 后，服务器会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。

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，此时间范围也是如此。例如，如果您向集群中的 SVM 添加两个新卷，您将在下一个轮询间隔（最长可达 15 分钟）后在 UI 中看到这些新对象。

下图说明了发现过程：





发现新集群的所有对象后，Unified Manager 开始收集前 15 天的历史性能数据。这些统计信息将通过数据连续性收集功能进行收集。添加集群后，此功能会立即为您提供两周以上的集群性能信息。数据连续性收集周期完成后，将收集实时集群性能数据，默认情况下每五分钟收集一次。



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。

## 查看监控集群列表

您可以使用“集群设置”页面来查看集群的清单。您可以查看有关集群的详细信息，例如其名称或 IP 地址和通信状态。

### 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”。

将显示存储环境中由 Unified Manager 管理的所有集群。集群列表按收集状态严重性级别列排序。您可以单击列标题来按不同列对集群进行排序。

## 添加集群

您可以将集群添加到 Active IQ Unified Manager，以便监控该集群。其中包括可通过获取集群的运行状况、容量、性能和配置等信息来发现并解决可能出现的任何问题。

## 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，并将应用程序访问权限设置为 *ontapi*、*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。
- Unified Manager 服务器上必须有足够的空间。如果已占用的空间量超过 90%，则您无法向此服务器添加集群。
- 您拥有所需的证书：

**SSL (HTTPS) 证书：**此证书归 Unified Manager 所有。全新安装 Unified Manager 时会生成默认的自签名 SSL (HTTPS) 证书。NetApp建议您将其升级为 CA 签名证书以获得更好的安全性。如果服务器证书过期，您应该重新生成它并重新启动 Unified Manager，以便服务合并新证书。有关重新生成 SSL 证书的更多信息，请参阅["生成 HTTPS 安全证书"](#)。

**EMS 证书：**此证书归 Unified Manager 所有。它用于对从ONTAP接收的 EMS 通知进行身份验证。

**用于相互 TLS 通信的证书：**在 Unified Manager 和ONTAP之间的相互 TLS 通信期间使用。根据ONTAP 版本，为集群启用基于证书的身份验证。如果运行ONTAP版本的集群低于 9.5，则不会启用基于证书的身份验证。

如果您正在更新旧版本的 Unified Manager，则不会自动为集群启用基于证书的身份验证。但是，您可以通过修改和保存集群详细信息来启用它。如果证书过期，您应该重新生成它以包含新证书。有关查看和重新生成证书的更多信息，请参阅["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，默认情况下不启用基于证书的身份验证。如果您使用 Unified Manager CLI 添加集群，则需要使用 Unified Manager UI 编辑该集群。你可以看到["支持的 Unified Manager CLI 命令"](#)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，并且您从服务器备份 Unified Manager 并将其还原到主机名或 IP 地址已更改的另一个 Unified Manager 服务器，则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，请参阅["编辑集群"](#)。
- 在集群级别，Active IQ接口为身份验证方法“cert”添加了两个新的用户组条目。

+

**集群证书：**此证书归ONTAP拥有。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证书。有关证书生成的信息，请参阅知识库 (KB) 文章 ["如何在系统管理器用户"](#)

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。如果您需要监控超出支持节点数的环境，则必须安装额外的 Unified Manager 实例来监控某些集群。要查看支持的节点数列表，请参阅 ["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. 在添加集群对话框中，根据需要指定值，然后单击\*提交\*。
4. 在授权主机对话框中，单击“查看证书”，查看集群的证书信息。
5. 单击“是”。

保存集群详细信息后，您可以看到集群的 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的每个 API 调用的证书。

发现新集群的所有对象后，Unified Manager 开始收集前 15 天的历史性能数据。这些统计信息将通过数据连续性收集功能进行收集。添加集群后，此功能会立即为您提供两周以上的集群性能信息。数据连续性收集周期完成后，将收集实时集群性能数据，默认情况下每五分钟收集一次。



- 收集 15 天的性能数据需要大量 CPU。NetApp建议您错开新集群的添加，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范围的间隙。
- 添加版本 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会自动创建具有只读权限的内部服务帐户用户（例如，clus-agent-xxxx）。如果出现以下情况，Unified Manager 将停止从这些集群收集数据 `clus-agent` 用户已被删除。

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不同步，并且 Unified Manager HTTPS 证书的开始日期晚于集群上的日期。您必须通过 NTP 或类似服务确保时钟同步。
- 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"](#)

#### 编辑集群

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，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。+ 如果您修改了添加到 Unified Manager 的集群的详细信息，则可以基于ONTAP版本查看 Mutual TLS 通信的证书详细信息。有关ONTAP版本的更多信息，请参阅[用于相互 TLS 通信的证书](#)。+ 您可以通过单击\*证书详情\*查看证书详情。如果证书已过期，请单击“重新生成”按钮以合并新证书。
4. 单击“提交”。
5. 在授权主机对话框中，单击“查看证书”，查看集群的证书信息。
6. 单击“是”。

相关信息

["添加用户"](#)

["查看集群列表和详细信息"](#)

## 删除集群

您可以使用集群设置页面从 Unified Manager 中删除集群。例如，如果集群发现失败，或者您想要退役存储系统时，您可以删除集群。

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。

此任务将从 Unified Manager 中删除选定的集群。集群被删除后，它将不再受到监控。在已删除的集群中注册的 Unified Manager 实例也将从集群中取消注册。

删除集群还会从 Unified Manager 中删除其所有存储对象、历史数据、存储服务以及所有相关事件。这些变化将在下一个数据收集周期后反映在库存页面和详细信息页面上。

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“删除数据源”消息对话框中，单击“删除”以确认删除请求。

相关信息

["添加用户"](#)

## 重新发现集群

您可以从“集群设置”页面手动重新发现集群，以获取有关集群的健康状况、监控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，该配对会触发重新获取 WFA 缓存的数据。

### 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 重新发现选定的集群并显示最新的运行状况和性能状态。

### 相关信息

## 监控 VMware 虚拟基础架构

Active IQ Unified Manager 提供对虚拟基础架构中虚拟机 (VM) 的可见性，并支持监控和排除虚拟环境中的存储和性能问题。您可以使用此功能来确定存储环境中的任何延迟问题，或者确定 vCenter Server 上报告的性能事件。

ONTAP 上的典型虚拟基础架构部署包括多种组件，这些组件分布在计算层、网络层和存储层上。如果虚拟机应用程序出现任何性能滞后，则可能是由于各个层的各种组件的延迟共同造成的。此功能对于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的存储和 vCenter Server 管理员和 IT 通才非常有用。

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预览视图在拓扑视图中都有 **VCENTER SERVER** 链接，可在新浏览器中启动 vCenter Server。您还可以使用\*扩展拓扑\*按钮启动 vCenter Server，然后单击\*在 vCenter 中查看\*按钮查看 vCenter Server 中的数据存储。

Unified Manager 以拓扑视图的形式呈现虚拟环境的底层子系统，以确定计算节点、网络或存储中是否出现了延迟问题。此外，此视图还会突出显示导致性能滞后的特定对象，以便于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：

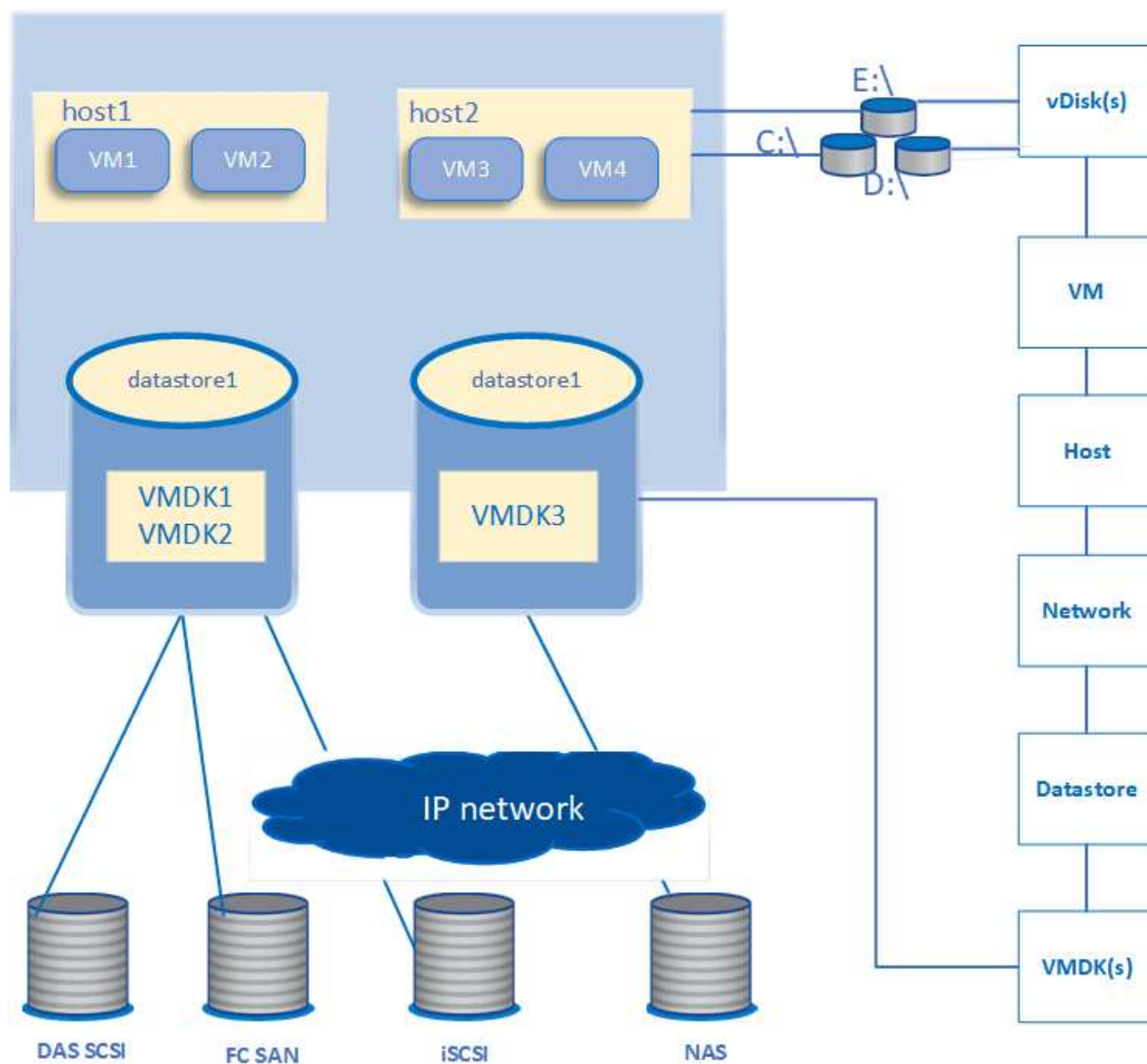
- vCenter Server：用于管理虚拟环境中的 VMware VM、ESXi 主机和所有相关组件的集中控制平面。有关 vCenter Server 的更多信息，请参阅 VMware 文档。
- 主机：运行 ESXi（VMware 提供的虚拟化软件）并托管虚拟机的物理或虚拟系统。
- 数据存储：数据存储是连接到 ESXi 主机的虚拟存储对象。数据存储库是 ONTAP 中的一种可管理的存储实体（例如 LUN 或卷），这些存储实体用作虚拟机文件（例如日志文件、脚本、配置文件和虚拟磁盘）的存储库。它们可通过 SAN 或 IP 网络连接来连接到环境中的主机。映射到 vCenter Server 的 ONTAP 之外的数

据存储库不受 Unified Manager 支持或显示。

- 虚拟机：VMware 虚拟机。
- 虚拟磁盘：属于虚拟机的数据存储区上的扩展名为 VMDK 的虚拟磁盘。虚拟磁盘中的数据存储于相应的 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。

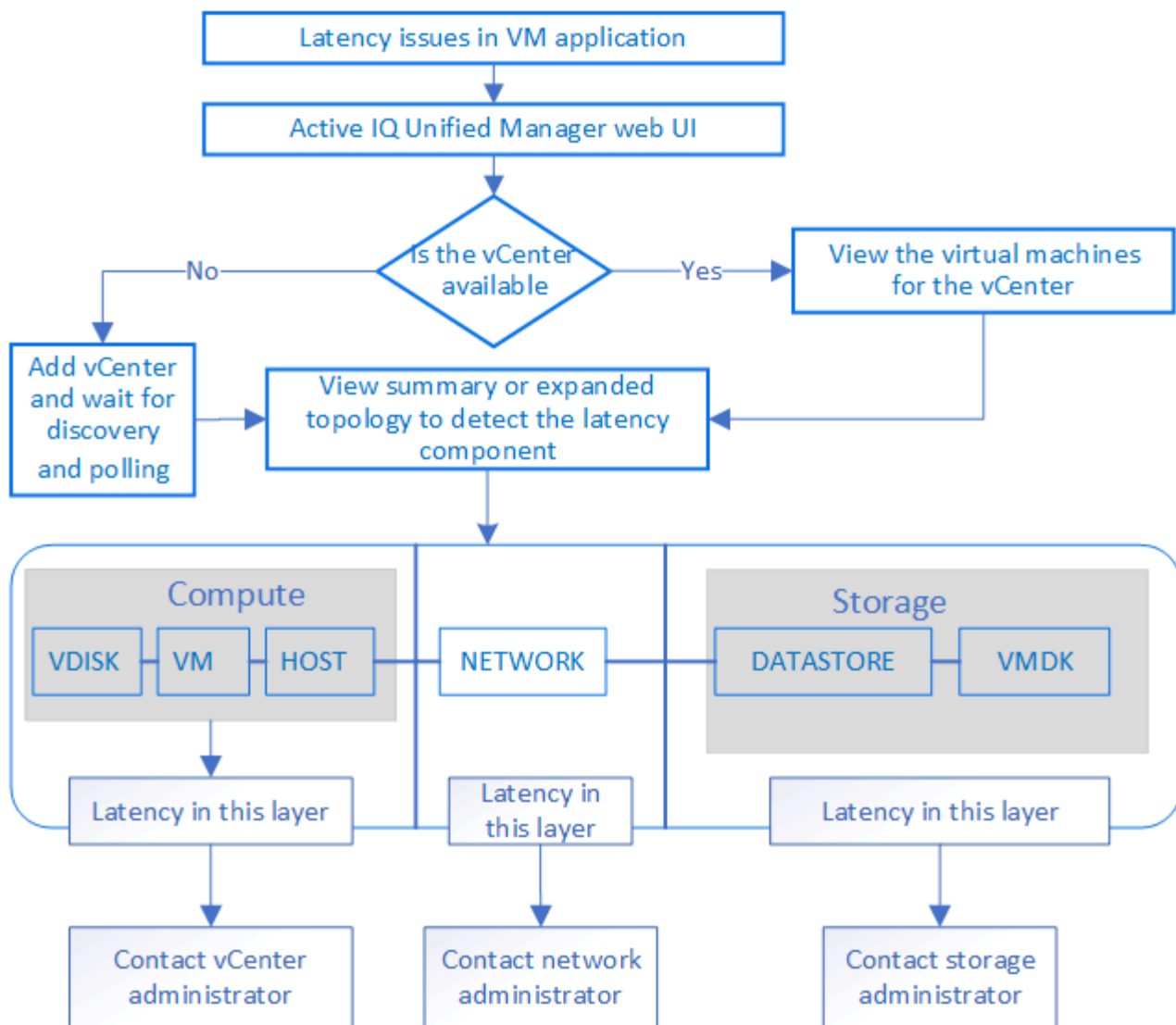
ONTAP上的 VMware 虚拟化



用户工作流程

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之外并映射到 vCenter Server 实例的数据存储库。也不支持这些数据存储库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) 映射数据 LIF (访问端点) 的数据存储。
- 不支持在多 LIF 配置中将卷或 LUN 导出为具有相同 IP 地址的不同集群上的数据存储，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 具有数据存储库 A。数据存储库 A 通过具有相同 IP 地址 xxxx 的数据 LIF 导出，并且虚拟机 A 在此数据存储库上创建。类似地，集群 B 具有数据存储库 B。数据存储库 B 通过具有相同 IP 地址 xxxx 的数据 LIF 导出，并在数据存储库 B 上创建 VM B。UM 既无法将 VM A 拓扑的数据存储库 A 映射到相应的ONTAP卷/LUN，也无法映射 VM B。

- 仅支持 NAS 和 SAN 卷（用于 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。
- 这些视图不允许您生成用于分析各个组件性能的报告。

- 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 中手动更改配置以指向切换和切换回场景中的活动 LUN。如果没有人工干预，他们的数据存储在将无法访问。

## 查看并添加 vCenter Server

要查看和排除虚拟机 (VM) 性能故障，必须在 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 Server 之前，请确保以下事项：

- 您知道 vCenter Server 名称。
- 您知道 vCenter Server 的 IP 地址并拥有所需的凭据。凭据必须属于 vCenter Server 管理员或具有 vCenter Server 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。



Unified Manager 对 VMware ESXi 和 vCenter Server 的支持提供英语和日语版本。

- vCenter Server 中的数据收集设置被设置为 *Level 3*，确保所有监控对象都达到所需的指标收集水平。间隔时间应为 *5 minutes*，保存期限应为 *1 day*。

有关详细信息，请参阅 VMware 文档中的《vSphere 监控和性能指南》的“数据收集级别”部分。

- 为了成功计算延迟值，vCenter Server 中的延迟值以毫秒为单位进行配置，而不是以微秒为单位。
- 将数据存储区添加到 vCenter Server 时，您可以同时使用主机的 IP 地址或完全限定域名 (FQDN)。如果您要添加 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。
- vCenter Server 的当前时间与 vCenter Server 时区同步。
- vCenter Server 可成功访问并发现。
- 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 Server，Unified Manager 都会收集配置数据，例如 vCenter Server 和 ESXi 服务器详细信息、ONTAP 映射、数据存储详细信息以及托管的虚拟机数量。此外，它还会收集这些组件的性能指标。

步骤

1. 转到 **VMWARE > vCenter**，并检查您的 vCenter Server 是否在列表中。



如果您的 vCenter Server 不可用，则必须添加 vCenter Server。

- a. 单击“添加”。
- b. 为 vCenter Server 添加正确的 IP 地址并确保该设备可访问。
- c. 添加具有 vCenter Server 只读访问权限的管理员或 root 用户的用户名和密码。



d. 如果您使用除默认 443 之外的任何端口，请添加自定义端口号。

e. 单击“保存”。

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。

当您接受证书时，vCenter Server 将被添加到可用 vCenter Server 列表中。添加设备后并不会立即收集关联虚拟机的数据，而是按照计划的间隔进行收集。

2. 如果您的 vCenter Server 在 **vCenters** 页面上可用，请将鼠标悬停在 **Status** 字段上检查其状态，以显示您的 vCenter Server 是否按预期运行，或者是否存在警告或错误。



添加 vCenter Server 允许您查看以下状态。但是，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 Server，并且已成功收集性能指标
- 黄色：“警告”（例如，当 vCenter Server 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 vCenter Server 无法访问）您可以单击列显示图标（显示/隐藏）来查看 vCenter Server 状态的状态消息并解决问题。

3. 如果 vCenter Server 无法访问或凭据已更改，请选择 **vCenter** > 编辑 来编辑 vCenter Server 详细信息。

4. 在“编辑 VMware vCenter Server”页面上进行必要的更改。

5. 单击“保存”。

## vCenter Server 数据收集开始

vCenter Server 收集实时 20 秒性能数据样本，并将其汇总为 5 分钟样本。Unified Manager 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。对于数据存储库，Unified Manager 根据从 ONTAP 获取的样本计算每小时的 IOPS 和延迟平均值。这些值可从整点获取。添加 vCenter Server 后，性能指标不会立即可用，只有下一个小时开始时才可用。性能数据轮询会在完成一轮配置数据收集后开始。

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，请参阅“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"](#)

## 移除 vCenter Server

您可以从 Active IQ Unified Manager 实例中删除 vCenter Server。例如，如果 vCenter Server 发现失败或不再需要该 vCenter Server，您可以将其移除。

删除 vCenter Server 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 Server 后，它将不再受到监控，同时还将不再监控其相关对象和历史数据。这些更改将反映在 vCenter 和虚拟机库存页面上。

## 开始之前

删除 vCenter Server 之前，请确保以下事项：

- 您具有应用程序管理员角色或存储管理员角色。
- 您应该了解 vCenter Server 名称以及与其关联的相应 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 Server，然后单击“删除”。
3. 在“删除 **vCenter**”消息对话框中，单击“确定”确认删除请求。

## 监控虚拟机

如果虚拟机 (VM) 应用程序出现任何延迟问题，您可能需要对此虚拟机进行监控以分析此问题的原因并解决此问题。当虚拟机的 vCenter Server 和托管虚拟机存储的ONTAP集群添加到 Unified Manager 时，虚拟机可用。

您可以在 **VMWARE > > 虚拟机** 页面上看到虚拟机的详细信息。显示可用性、状态、已用和已分配容量、网络延迟以及虚拟机、数据存储区和主机的 IOPS 和延迟等信息。对于支持多个数据存储区的虚拟机，网格显示延迟最严重的数据存储区的指标，星号图标 (\*) 表示其他数据存储区。如果单击该图标，则会显示附加数据存储的指标。其中一些列不可用于排序和过滤。



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 中删除集群，则在下一个发现周期之后，虚拟机将不再可用。

从此页面，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，例如连接到它的主机、虚拟磁盘和数据存储。拓扑视图按以下顺序显示特定层中的底层组件：虚拟磁盘 > **VM** > 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

要通过查看摘要拓扑中的虚拟机来确定性能问题：

1. 转到 **VMWARE > 虚拟机**。
2. 在搜索框中键入虚拟机的名称以搜索此虚拟机。您还可以通过单击“过滤器”按钮根据特定条件过滤搜索结果。但是，如果您找不到您的虚拟机，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、群集、数据存储区、文件夹或文件）的名称中使用特殊字符（例如 %, &、 、 \$、 #、 @、 !、 \、 /、 :、 、 ?、 "、 <、 >、 |、 ;、 '）。VMware vCenter Server 和 ESX/ESXi 服务器不会对这些显示名称中使用的特殊字符进行转义。但是，在 Unified Manager 中处理该名称时，显示方式会有所不同。例如，名为 ``%$VC_AIQUM_clone_191124%`` 在 vCenter Server 中显示为 ``%25$VC_AIQUM_clone_191124%25`` 在统一管理器中。在使用包含特殊字符的名称查询虚拟机时，必须注意此问题。

3. 检查此虚拟机的状态。VM 状态从 vCenter Server 检索。可用状态如下。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“工作负载分析器”按钮。您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更多信息，请参阅[\\_使用工作负载分析器排除工作负载故障\\_](#)。

## 查看扩展拓扑

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. 从摘要拓扑视图中，单击\*展开拓扑\*。您可以单独查看每个组件的详细拓扑，其中显示了每个对象的延迟数值。如果某个类别下有多个节点（例如数据存储库或 VMDK 中的多个节点），则延迟状况最差的节点会以红色突出显示。
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"](#)

## 查看灾难恢复设置中的虚拟基础架构

您可以查看MetroCluster配置或存储虚拟机 (存储 VM) 灾难恢复 (SVM DR) 设置中托管的数据存储库的配置和性能指标。

在 Unified Manager 上，您可以查看MetroCluster配置中作为 vCenter Server 中的数据存储附加的 NAS 卷或 LUN。MetroCluster配置中托管的数据存储库与标准环境中的数据存储库在相同的拓扑视图表示。

您还可以查看存储虚拟机灾难恢复配置中映射到 vCenter Server 中的数据存储区的 NAS 卷或 LUN。

## 查看MetroCluster配置中的数据存储

在查看MetroCluster配置中的数据存储之前，请注意以下先决条件：

- 在发生切换和切换回时，HA 对的主集群和辅助集群以及 vCenter Server 的发现应该是完整的。
- HA 对的主集群和辅助集群以及 vCenter Server 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，单击托管数据存储区的 VM。单击“工作负载分析器”或数据存储对象链接。在标准场景中，当托管卷或 LUN 的主站点按预期运行时，您可以看到主站点的 vServer 群集详细信息。
2. 在发生灾难并连续切换到辅助站点时，数据存储链接指向辅助集群中卷或 LUN 的性能指标。这在下一个集群和 vServer 发现（获取）周期完成后反映出来。
3. 成功切换后，数据存储链接再次反映主集群中卷或 LUN 的性能指标。这在下一个集群和 vServer 发现周期完成后反映出来。

查看存储虚拟机灾难恢复配置中的数据存储

在查看存储虚拟机灾难恢复配置中的数据存储之前，请注意以下先决条件：

- 在发生切换和切换回时，HA 对的主集群和辅助集群以及 vCenter Server 的发现应该是完整的。
- 源集群和目标集群以及存储虚拟机对等体都应由 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）数据存储区，如果发生灾难，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。

为了切换回主站点，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 VMFS 的 FC）数据存储，vCenter Server 将挂载的 LUN 格式化为 VMFS 格式。如果发生灾难，步骤包括启动辅助存储虚拟机、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。新的 LUN 应该作为主机存储适配器的 iSCSI 适配器下的设备可用。此后，应创建具有新 LUN 的新 VMFS 数据存储，并使用新名称注册旧 VM。虚拟机必须启动并运行。

如果发生恢复，则卷之间的数据应该同步。应使用 LUN 和以新名称注册的旧 VM 再次创建新的 VMFS 数据存储。

有关设置的信息，请参阅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，单击托管数据存储区的 VM 清单。单击数据存储对象链接。在标准场景中，您可以看到主存储VM中卷和LUN的性能数据。
2. 在发生灾难并连续切换到辅助存储虚拟机时，数据存储链接指向辅助存储虚拟机中的卷或 LUN 的性能指标。这在下一个集群和 vServer 发现（获取）周期完成后反映出来。
3. 成功切换后，数据存储链接再次反映主存储虚拟机中卷或 LUN 的性能指标。这在下一个集群和 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：
  - 仅在 `NORMAL`` 和 ``SWITCHOVER`` 各州都已开始采取行动。其他州，例如 ``PARTIAL_SWITCHOVER``，`PARTIAL_SWITCHBACK``，和 ``NOT_REACHABLE`` 不受支持。
  - 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，并且拓扑将继续指向主集群中的卷或 LUN。
- 对于存储虚拟机灾难恢复配置，请注意以下限制：
  - 不支持为 SAN 存储环境启用站点恢复管理器 (SRM) 或存储复制适配器 (SRA) 的配置。

## 预配和管理工作负载

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程序 API，用于配置、监控和管理数据中心中的存储工作负载。



Unified Manager 默认提供此功能。如果您不打算使用此功能，您可以从\*存储管理\*>\*功能设置\*中禁用它。

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您的存储环境。

此功能可实现以下功能：

- 自动发现添加的集群上的存储工作负载，从而轻松评估和部署存储工作负载
- 配置支持 NFS 和 CIFS 协议的 NAS 工作负载
- 配置支持 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 左侧窗格上的 **Provisioning、Storage > Workloads** 和 **Policies** 选项使您能够修改各种配置。

您可以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
- 根据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”页面向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

工作负载表示存储对象（例如卷或 LUN）的输入/输出 (I/O) 操作。存储的配置方式取决于预期的工作负载要求。仅当有流量往返于存储对象后，Active IQ Unified Manager 才会跟踪工作负载统计信息。例如，用户开始使用数据库或电子邮件应用程序后，即可获得工作负载 IOPS 和延迟值。

“工作负载”页面显示由 Unified Manager 管理的 ONTAP 集群的存储工作负载摘要。它提供了符合性能服务水平的存储工作负载以及不符合性能服务水平的存储工作负载的累积概览信息。它还使您能够评估整个数据中心集群的总容量、可用容量和已用容量和性能（IOPS）。



建议您评估不符合要求、不可用或不受任何性能服务级别管理的存储工作负载的数量，并采取必要的措施来确保其一致性、容量使用率和 IOPS。

工作负载页面包含以下两个部分：

- 工作负载概览：提供 Unified Manager 管理的 ONTAP 集群上的存储工作负载数量的概览。
- 数据中心概览：提供数据中心内存储工作负载的容量和 IOPS 概览。相关数据显示在数据中心级别和个人级别。

### 工作负载概述部分

工作负载概览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根据已分配和未分配的性能服务级别显示。

- 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：
  - 符合：存储工作负载的性能取决于分配给它们的性能服务级别。如果存储工作负载在相关性能服务级别中定义的阈值延迟范围内，则将其标记为“符合”。符合要求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相关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“不符合”。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离线状态，或者相应的集群无法访问，则会被标记为“不可用”。不可用的工作负载以红色标记。
- 未分配：未分配性能服务级别的存储工作负载被报告为“未分配”。该数字由信息图标传达。

总工作负载数是已分配工作负载和未分配工作负载的总和。

您可以单击此部分显示的工作负载总数，然后在工作负载页面查看它们。

按性能服务级别符合性子部分显示可用存储工作负载的总数：

- 符合各类绩效服务水平
- 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

数据中心概览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。通过使用这些数据，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的存储工作负载的以下信息：

- 数据中心内所有集群的总容量、可用容量和已用容量
- 数据中心内所有集群的总 IOPS、可用 IOPS 和已用 IOPS
- 基于每个性能服务级别的可用容量和已用容量
- 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

如何根据性能服务水平计算数据中心容量和性能

已用容量和 IOPS 是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的。

可用的 IOPS 是根据节点上的预期延迟和建议的性能服务级别计算的。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。

可用容量是根据预期延迟和聚合体的建议性能服务级别计算的。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。

查看工作负载

当您添加集群到 Unified Manager 时，每个集群上的存储工作负载都会自动被发现并显示在“工作负载”页面上。

仅当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供推荐（推荐的 PSL）。

FlexGroup 卷及其组成部分被排除在外。

工作负载概述

工作负载概览页面显示数据中心内工作负载的概览以及数据中心的空间和性能概览。

- **\*工作负载概览\*面板：**显示工作负载总数以及分配了或未分配 PSL 的工作负载数量。还显示了每个 PSL 的工作量计数的细分。单击计数将带您进入包含已过滤工作负载的“所有工作负载”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“分配系统推荐的 PSL”按钮为其分配系统推荐的 PSL。
- **\*数据中心概览\*面板：**显示数据中心的可用和已用空间（TiB）和性能（IOPS）。还显示每个 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 集群相关的存储工作负载。

对于新发现的尚未进行 I/O 操作的存储工作负载，状态为“等待 I/O”。在存储工作负载上开始 I/O 操作后，Unified Manager 开始分析，工作负载状态变为“学习中...”。分析完成后（从 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。

该页面还允许您为存储工作负载分配存储效率策略 (SEP) 和性能服务级别 (PSL)。您可以执行多项任务：

- 添加或配置存储工作负载
- 查看和过滤工作负载列表
- 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

## 添加或配置存储工作负载

您可以将存储工作负载添加或配置到支持的 LUN（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，请参阅["配置和管理工作负载"](#)。

## 查看和过滤工作负载

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 PSL 或名称搜索特定的存储工作负载。您可以使用过滤器图标输入特定的搜索条件。您可以根据不同的过滤条件进行搜索，例如按主机集群或存储虚拟机。**Capacity Total** 选项允许按工作负载的总容量（以 MB 为单位）进行过滤。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，都会显示主机集群和存储虚拟机等信息，以及分配的 PSL 和 SEP。

该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更多信息，请参阅["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。要查看“工作负载分析”页面上的性能和容量图表来分析对象，请单击“分析工作负载”按钮。

有关详细信息，请参阅 ["工作负载分析器显示哪些数据"](#)。

## 为工作负载分配策略

您可以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

您可以为单个工作负载分配 PSL 或 SEP，或者两者兼而有之。按照下面的步骤进行操作：

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。



4. 单击复选图标以应用更改。



您还可以选择一个工作负载并单击“更多操作”来分配策略。

#### 将策略分配给多个存储工作负载

您可以将 PSL 或 SEP 一起分配给多个存储工作负载。按照下面的步骤进行操作：

1. 选中要分配策略的工作负载的复选框，或选择数据中心内的所有工作负载。
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\*。将显示一个弹出窗口供您选择策略。
4. 选择适当的策略并单击\*应用\*。显示分配了策略的工作负载的数量。还列出了未分配策略的工作负载及其原因。



根据所选工作负载的数量，批量应用策略可能需要一些时间。您可以单击“在后台运行”按钮，并在操作在后台运行时继续执行其他任务。当批量分配完成后，您可以查看完成状态。如果您在多个工作负载上应用 PSL，则在批量分配的前一个作业运行时，您无法触发另一个请求。

#### 将系统推荐的 PSL 分配给工作负载

您可以将系统推荐的 PSL 分配给数据中心的尚未分配 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，并且对于那些 IOPS 和其他参数与任何可用 PSL 的定义不一致的工作负载将被跳过。存储工作负载 `Waiting for I/O` 学习状态也被排除在外。



Unified Manager 会在工作负载名称中查找特殊关键字来覆盖系统分析并为工作负载推荐不同的 PSL。当工作负载名称中包含字母“ora”时，建议使用极限性能 PSL。当工作负载名称中包含字母“vm”时，建议使用 **Performance** PSL。

另请参阅知识库 (KB) 文章 ["ActiveIQ Unified Manager 的“分配系统推荐的性能服务级别”不适应高度变化的工作负载"](#)

#### 配置文件共享卷

您可以从“配置工作负载”页面在现有集群和存储虚拟机（存储 VM）上创建支持 CIFS/SMB 和 NFS 协议的文件共享卷。

#### 开始之前

- 存储虚拟机必须具有用于配置文件共享卷的空间。
- 您的存储虚拟机上应启用 SMB 和/或 NFS 服务。
- 为了在工作负载上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“Provision Workload”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** 字段会过滤该集群可用的存储 VM。从列表中选择所需的 Storage VM。

根据存储虚拟机上支持的 SMB 和 NFS 服务，在主机信息部分启用 NAS 选项。

3. 在存储和优化部分，分配存储容量和 PSL，还可以选择为工作负载分配 SEP。

在创建工作负载时，SEP 的规范会分配给 LUN，而 PSL 的定义则会应用于工作负载。

4. 如果您想要强制执行已分配给工作负载的 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体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，则要配置工作负载的聚合体应该具有支持“极限性能”策略的性能和容量目标的能力，例如 SSD 存储。



除非您选中此复选框，否则 PSL 不会应用于工作负载，并且仪表板上的工作负载状态将显示为未分配。

5. 选择 **NAS** 选项。

如果您看不到启用的 **NAS** 选项，请验证您选择的存储虚拟机是否支持 SMB 或 NFS，或两者。



如果您的存储虚拟机同时启用了 SMB 和 NFS 服务，您可以选中 **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，指定用于访问文件共享卷的主机或网络的 IP 地址。您可以输入多个主机的值（以英文逗号分隔）。

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，则重新使用该策略。如果为同一主机创建了多个 NFS 共享，则会对所有文件共享重复使用此同一主机中具有匹配规则的可用导出策略。在使用 API 配置 NFS 共享时，可以为单个策略指定规则，也可以通过提供特定策略密钥重复使用策略。

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“保存”。

此时，此工作负载将添加到存储工作负载列表中。

## 配置 LUN

您可以从“配置工作负载”页面在现有集群和存储虚拟机（存储 VM）上创建支持 CIFS/SMB 和 NFS 协议的 LUN。

### 开始之前

- 存储虚拟机必须具有用于配置 LUN 的空间。
- 在创建 LUN 的存储 VM 上必须同时启用 iSCSI 和 FCP。

- 为了在工作负载上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“Provision Workload”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** 字段会过滤该集群可用的存储 VM。

2. 从列表中选择支持 iSCSI 和 FCP 服务的存储虚拟机。

根据您的选择, SAN 选项在主机信息部分中启用。

3. 在“存储和优化”部分中, 分配存储容量和 PSL, 以及可选的工作负载的 SEP。

在创建工作负载时, SEP 的规范会分配给 LUN, 而 PSL 的定义则会应用于工作负载。

4. 如果您想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体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, 则要配置工作负载的聚合体应该具有支持“极限性能”策略的性能和容量目标的能力, 例如 SSD 存储。



除非您选中此复选框, 否则 PSL 不会应用于工作负载, 并且工作负载的状态在仪表板上显示为 unassigned。

5. 选择 **SAN** 选项。如果您看不到启用的 **SAN** 选项, 请验证您选择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器对 LUN 的访问。您可以分配现有的启动器组 (igroup), 或者定义和映射新的 igroup。



如果在配置 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。

如果要创建一个新的 igroup, 请选择“创建新的启动器组”按钮, 然后输入该 igroup 的信息。

8. 单击“保存”。

LUN 已添加到存储工作负载列表中。

## 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将 PSL 分配给工作负载, 也可以在之后通过编辑工作负载来分配 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 是对存储服务目标的描述。PSL 使存储提供商能够指定工作负载的性能和容量目标。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 都受峰值、预期和绝对最小 IOP 以及预期延迟的控制。

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固定策略。这些预定义的 PSL 是：
  - 至高性能
  - 性能
  - 值

极限性能、性能和价值 PSL 适用于数据中心中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种性能服务级别。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。

- 数据库日志的极致
  - 数据库共享数据的极致
  - 数据库数据的极致
- 用户定义：如果预定义的性能服务级别不能满足您的要求，那么您可以创建新的 PSL 来满足您的需求。有关信息，请参阅["创建和编辑性能服务级别"](#)。
  - 超越极限：超越极限 PSL 是系统推荐的 PSL，建议用于需要高于极限的 IOP 的工作负载。根据工作负载的 IOPS、容量和延迟进行内部分析，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一个 Beyond Extreme PSL。您可以将 PSL 应用于工作负载以确保最佳性能。

工作负载的 IOP 参数是根据工作负载行为动态生成的，并以以下格式附加到 Beyond Extreme PSL 的名称中 `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`。例如，如果系统确定工作负载的峰值和预期 IOP 为 106345 和 37929 分别为工作负载生成的 Beyond Extreme PSL 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 会被标记为 ``User-defined`` 在类型中。

通过分配 **PSL** 来管理工作负载

您可以从 策略 > 性能服务级别 页面访问 PSL，也可以使用存储提供程序 API 访问。通过为存储工作负载分配 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，请参阅["将系统推荐的 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。



您不能修改系统定义或当前分配给工作负载的 PSL。您无法删除已分配给工作负载的 PSL，或者它是唯一可用的 PSL。

此页面显示以下信息：

| 字段 | 描述       |
|----|----------|
| 名称 | PSL 的名称。 |

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 字段         | 描述                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 类型         | 该策略是系统定义的还是用户定义的。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 预期 IOPS/TB | 应用程序预计在 LUN 或文件共享上执行的最小 IOPS 数。预期 IOPS 根据分配的存储对象大小指定分配的最小预期 IOPS。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 峰值 IOPS/TB | <p>应用程序在 LUN 或文件共享上可以执行的最大 IOPS 数。峰值 IOPS 根据分配的存储对象大小或使用的存储对象大小指定可能分配的最大 IOPS。</p> <p>峰值 IOPS 基于分配策略。分配策略是已分配空间或已使用空间。当分配策略设置为allocated-space时，峰值IOPS是根据存储对象的大小来计算的。当分配策略设置为已用空间时，峰值 IOPS 是根据存储对象中存储的数据量计算的，同时考虑存储效率。默认情况下，分配策略设置为已用空间。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 绝对最小 IOPS  | <p>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：</p> <ul style="list-style-type: none"> <li>• 极限性能：如果预期 IOPS <math>\geq</math> 6144/TB，则绝对最小 IOPS = 1000</li> <li>• 性能：如果预期 IOPS <math>\geq</math> 2048/TB 且 <math>&lt;</math> 6144/TB，则绝对最小 IOPS = 500</li> <li>• 值：如果预期 IOPS <math>\geq</math> 128/TB 且 <math>&lt;</math> 2048/TB，则绝对最小 IOPS = 75</li> </ul> <p>系统定义的数据库 PSL 的默认值如下：</p> <ul style="list-style-type: none"> <li>• 数据库日志的极限：如果预期 IOPS <math>\geq</math> 22528，则绝对最小 IOPS = 4000</li> <li>• 数据库共享数据的极限：如果预期 IOPS <math>\geq</math> 16384，则绝对最小 IOPS = 2000</li> <li>• 数据库数据的极端情况：如果预期 IOPS <math>\geq</math> 12288，则绝对最小 IOPS = 2000</li> </ul> <p>自定义 PSL 的绝对最小 IOPS 的较高值最大可以为 75000。较低值的计算方法如下：</p> <p>1000/预期延迟</p> |
| 预期延迟       | 存储 IOPS 的预期延迟（以每次操作的毫秒数 (ms/op) 为单位）。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 容量         | 集群中可用和已用的总容量。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| 字段   | 描述                  |
|------|---------------------|
| 工作负载 | 已分配 PSL 的存储工作负载的数量。 |

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，请参阅以下知识库文章：  
[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Infrastructure\\_Management/Active\\_IQ\\_Unified\\_Manager/What\\_is\\_Performance\\_Budgeting%3F](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F)["什么是绩效预算？"]

因工作负载超出 **PSL** 定义的阈值而生成的事件

请注意，如果工作负载在前一小时内有 30% 的时间超过预期延迟值，Unified Manager 将生成以下事件之一来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
- 工作负载 LUN 延迟阈值已超出性能服务级别策略所定义的范围。

您可能需要分析工作负载以查看导致较高延迟值的原因。

有关详细信息，请参阅以下链接：

- ["卷事件"](#)
- ["当违反绩效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 | 描述和用例                             | 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<br><br>非常适合延迟敏感的应用程序 | 1           | 12288   | 6144    | 1000      |
| 性能     | 提供高吞吐量和低延迟<br><br>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     | 描述和用例                                                                                         | 预期延迟（毫秒/操作） | IOPS 峰值 | 预期 IOPS | 绝对最小 IOPS |
|------------|-----------------------------------------------------------------------------------------------|-------------|---------|---------|-----------|
| 值          | <p>提供高存储容量和适度延迟</p> <p>非常适合电子邮件、Web 内容、文件共享和备份目标等大容量应用程序</p>                                  | 17          | 512     | 128     | 75        |
| 数据库日志的极致   | <p>以最低的延迟提供最大的吞吐量。</p> <p>非常适合支持数据库日志的数据库应用程序。由于数据库日志极其突发且对日志记录的需求不断增加，因此此 PSL 可提供最高的吞吐量。</p> | 1           | 45056   | 22528   | 4000      |
| 数据库共享数据的极致 | <p>以最低的延迟提供非常高的吞吐量。</p> <p>非常适合存储在公共数据存储中但跨数据库共享的数据库应用程序数据。</p>                               | 1           | 32768   | 16384   | 2000      |
| 数据库数据的极致   | <p>以最低的延迟提供高吞吐量。</p> <p>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。</p>                                       | 1           | 24576   | 12288   | 2000      |

## 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，您可以创建针对您的工作负载进行优化的性能服务级别。

### 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。

您可以从“性能服务级别”页面创建和编辑自定义性能服务级别，方法是定义访问存储的应用程序所需的服务级别目标。



如果性能服务级别当前已分配给工作负载，则您无法修改它。

步骤

- 在左侧导航窗格的“设置”下，选择“策略”>“性能服务级别”。
- 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          | 请按照以下步骤操作...          |
|-------------|-----------------------|
| 创建新的性能服务级别  | 单击“添加”。               |
| 编辑现有的性能服务级别 | 选择现有的性能服务级别，然后单击“编辑”。 |

显示添加或编辑性能服务级别的页面。

- 通过指定性能目标来定制性能服务级别，然后单击\*提交\*以保存性能服务级别。

您可以从“工作负载”页面或在配置新的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

存储效率策略 (SEP) 使您能够定义工作负载的存储效率特征。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来分配 SEP。

存储效率包括使用精简配置、重复数据删除和数据压缩等技术来提高存储利用率并降低存储成本。在创建 SEP 时，您可以单独或一起使用这些节省空间的技术来实现最大的存储效率。当您策略与存储工作负载关联时，指定的策略设置就会分配给它们。 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 不能满足您的要求，您可以创建自己的策略。

您无法修改系统定义或当前分配给工作负载的 SEP。您无法删除已分配给工作负载的 SEP，或者它是唯一可用的 SEP。

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 SEP。此页面显示以下信息：



| 字段     | 描述                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 名称     | SEP 的名称。                                                                                                                                           |
| 类型     | 该策略是系统定义的还是用户定义的。                                                                                                                                  |
| 空间预留   | 该卷是精简配置的还是厚配置的。                                                                                                                                    |
| 重复数据删除 | 工作负载上是否启用了重复数据删除： <ul style="list-style-type: none"> <li>• 内联：重复数据删除在工作负载写入时发生</li> <li>• 背景：重复数据删除发生在工作负载中</li> <li>• 禁用：工作负载上禁用重复数据删除</li> </ul> |
| 数据压缩   | 工作负载是否启用数据压缩： <ul style="list-style-type: none"> <li>• 内联：数据压缩在工作负载写入时进行</li> <li>• 背景：数据压缩发生在工作负载中</li> <li>• 禁用：工作负载上禁用数据压缩</li> </ul>           |
| 工作负载   | 已分配 SEP 的存储工作负载数量                                                                                                                                  |

## 创建自定义存储效率策略的指南

如果现有的 SEP 不符合您的存储工作负载的策略要求，您可以创建自定义 SEP。但是，建议您尝试将系统定义的 SEP 用于存储工作负载，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。您可以在仪表板上的容量面板和容量：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（不含 Snapshot 副本）。

## 创建和编辑存储效率策略

当系统定义的存储效率策略不符合您的工作负载要求时，您可以创建针对您的工作负载优化的存储效率策略。

### 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。

您可以从“存储效率策略”页面创建和编辑自定义存储效率策略，方法是定义访问存储的应用程序所需的存储效率特征。



如果存储效率策略当前已分配给工作负载，则您无法修改该策略。

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要编辑现有的存储效率策略，单击相应的按钮。

| 目的          | 请按照以下步骤操作...       |
|-------------|--------------------|
| 创建新的存储效率策略  | 点击“添加”             |
| 编辑现有的存储效率策略 | 选择现有的存储效率策略并单击“编辑” |

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来定制存储效率策略，然后单击\*提交\*以保存存储效率策略。

您可以从“工作负载”页面或在配置新的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

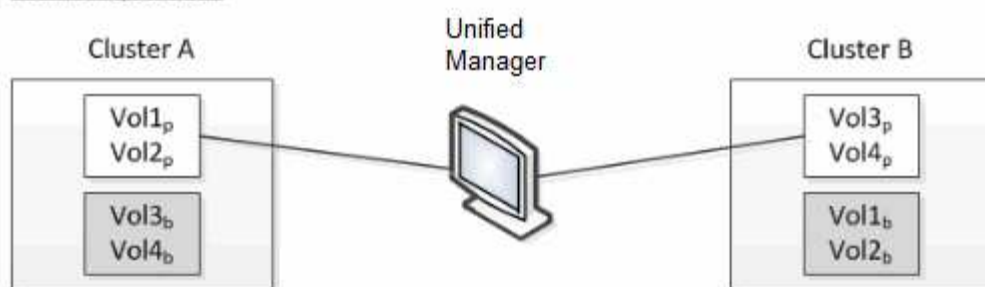
Unified Manager Web UI 中对MetroCluster配置的监控支持使您能够检查MetroCluster通过FC 和 IP 配置中的任何连接问题。尽早发现连接问题使您能够有效地管理MetroCluster配置。

### 切换和切回期间的卷行为

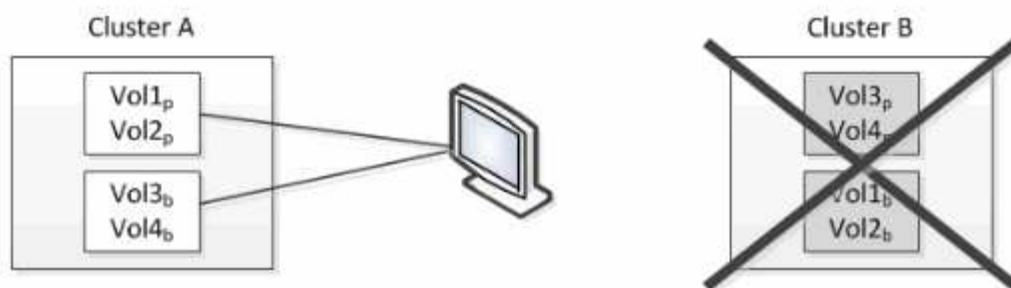
触发切换或切回的事件会导致活动卷从灾难恢复组中的一个集群移动到另一个集群。集群上处于活动状态并向客户端提供数据的卷将停止，而另一个集群上的卷将激活并开始提供数据。 Unified Manager 仅监控处于活动状态且正在运行的卷。

由于卷从一个集群移动到另一个集群，因此建议您监视两个集群。 Unified Manager 的单个实例可以监控MetroCluster配置中的两个集群，但有时两个位置之间的距离需要使用两个 Unified Manager 实例来监控两个集群。下图显示了 Unified Manager 的单个实例：

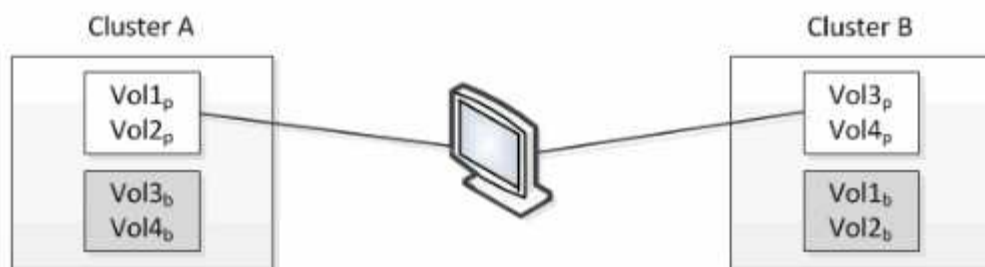
### Normal operation



### Cluster B fails --- switchover to Cluster A



### Cluster B is repaired --- switchover back to Cluster B



□ = active and monitored

■ = inactive and not monitored

名称中带有 p 的卷表示主卷，名称中带有 b 的卷表示由 SnapMirror 创建的镜像备份卷。

正常运行期间：

- 集群 A 有两个活动卷：Vol1<sub>p</sub> 和 Vol2<sub>p</sub>。
- 集群 B 有两个活动卷：Vol3<sub>p</sub> 和 Vol4<sub>p</sub>。
- 集群 A 有两个非活动卷：Vol3<sub>b</sub> 和 Vol4<sub>b</sub>。
- 集群 B 有两个非活动卷：Vol1<sub>b</sub> 和 Vol2<sub>b</sub>。

Unified Manager 收集与每个活动卷相关的信息（统计数据、事件等）。Vol1<sub>p</sub> 和 Vol2<sub>p</sub> 统计数据由 Cluster A 收集，Vol3<sub>p</sub> 和 Vol4<sub>p</sub> 统计数据由 Cluster B 收集。

灾难性故障导致活动卷从集群 B 切换到集群 A 后：

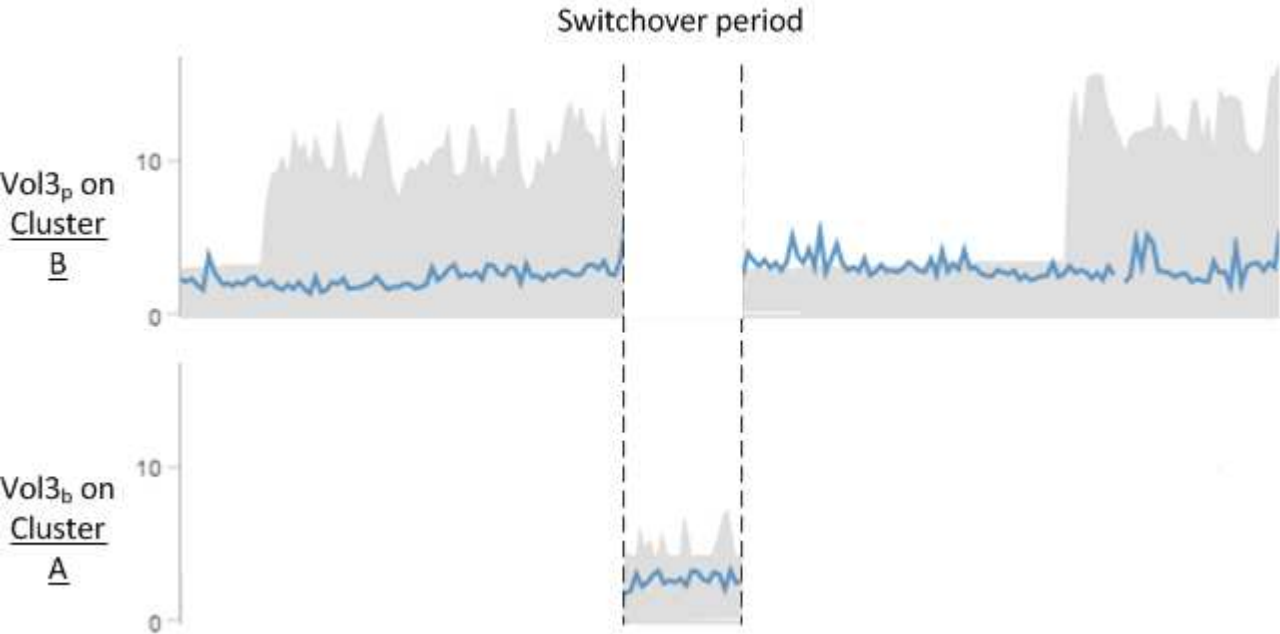
- 集群 A 有四个活动卷：Vol1<sub>p</sub>、Vol2<sub>p</sub>、Vol3<sub>b</sub> 和 Vol4<sub>b</sub>。
- 集群 B 有四个非活动卷：Vol3<sub>p</sub>、Vol4<sub>p</sub>、Vol1<sub>b</sub> 和 Vol2<sub>b</sub>。

与正常运行期间一样，Unified Manager 会收集与每个活动卷相关的信息。但在这种情况下，Vol1p 和 Vol2p 统计信息由 Cluster A 收集，Vol3b 和 Vol4b 统计信息也由 Cluster 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 中有关 Vol3p 的信息与 Vol3b 的信息不同：

- 在切换到集群 A 期间，Vol3p 统计数据 and 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 修复并执行切换时，Vol3p 在集群 B 上再次处于活动状态，并具有历史统计数据和切换期间的统计数据间隙。在发生另一次切换之前，无法从集群 A 查看 Vol3b：



- 处于非活动状态的MetroCluster卷（例如，切换回集群 A 上的 Vol3b）将显示消息“此卷已被删除”。该卷实际上并未被删除，但由于它不是活动卷，因此当前未被 Unified Manager 监控。
- 如果单个 Unified Manager 正在监控MetroCluster配置中的两个集群，则卷搜索将返回当时处于活动状态的卷的信息。例如，如果发生了切换并且 Vol3 在集群 A 上变为活动状态，则搜索“Vol3”将返回集群 A 上 Vol3b 的统计信息和事件。

通过 FC 配置的MetroCluster的集群连接状态定义

通过 FC 配置的MetroCluster中的集群之间的连接可以是以下状态之一：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 | 描述                         | 显示的图标 |
|------|----------------------------|-------|
| 最佳   | MetroCluster配置中的集群之间的连接正常。 |       |

| 连接状态 | 描述                                                                                              | 显示的图标                                                                                                                                                                                                |
|------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 受影响  | 一个或多个错误损害了故障转移可用性的状态；但是， MetroCluster 配置中的两个集群仍然处于启动状态。例如，当 ISL 链路断开时、当集群间 IP 链路断开时或当伙伴集群不可访问时。 |                                                                                                                   |
| 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，当合作伙伴集群因灾难而关闭或为了测试目的而计划切换时。           | <p>切换时出现错误：</p>  <p>切换成功：</p>  |

## MetroCluster over FC 的数据镜像状态定义

FC 配置上的MetroCluster提供数据镜像以及在整个站点不可用时启动故障转移的附加功能。通过 FC 配置的MetroCluster中集群之间的数据镜像状态可以是“正常”或“镜像不可用”。了解状态使您能够有效地管理MetroCluster配置。

| 数据镜像状态 | 描述                                                                | 显示的图标                                                                                                                                                                                                    |
|--------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 正常     | MetroCluster配置中的集群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，当合作伙伴集群因灾难而关闭或为了测试目的而计划切换时。 | <p>切换时出现错误：</p>  <p>切换成功：</p>  |

## 监控MetroCluster配置

您可以监控MetroCluster配置中的连接问题。详细信息包括集群内的组件和连接状态以及MetroCluster配置中集群之间的连接状态。在这里，您将了解如何监控由MetroCluster over FC 和MetroCluster over IP 配置保护的集群中的连接问题。

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 使用系统运行状况警报来指示MetroCluster配置中的组件和连接的状态。

开始之前

- MetroCluster配置中的本地集群和远程集群都必须添加到Active IQ Unified Manager。
- 在MetroCluster over IP 配置中，如果要支持调解器，则应通过相应的 API 配置调解器并将其添加到集群中。
- 您必须具有操作员、应用程序管理员或存储管理员角色。

通过 **FC** 配置监控**MetroCluster**中的连接问题

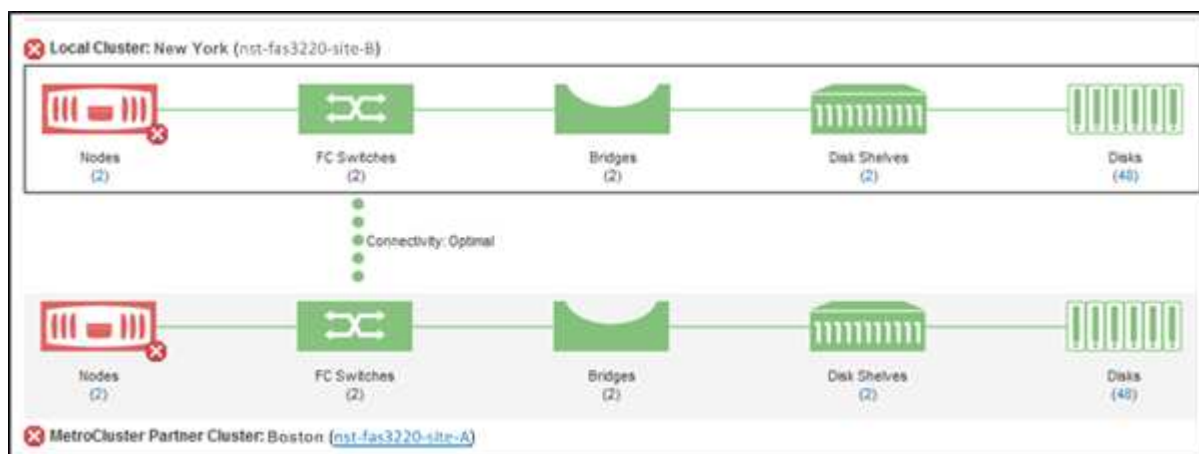
对于MetroCluster over FC 配置中的集群，连接图表显示在 集群/运行状况 详细信息页面上。请按照以下步骤操作。

步骤

1. 在左侧导航窗格中，单击“存储”>“集群”。

显示所有受监控集群的列表。

2. 从 **Protection: MetroCluster** 视图中，单击要查看MetroCluster over FC 配置详细信息的集群的名称。或者，您可以按MetroCluster配置中的集群进行过滤。
3. 在“集群/运行状况”详细信息页面中，单击“MetroCluster连接”选项卡。“MetroCluster Connectivity”选项卡仅适用于 FC 配置上的MetroCluster 。



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/健康详情页面中显示的信息来纠正任何连接问题。例如，如果集群中的节点和交换机之间的连接中断，则会显示以下图标：



如果将指针移到图标上，您可以查看有关所生成事件的详细信息。

如果您发现MetroCluster配置中存在连接问题，则必须登录系统管理器或访问ONTAP CLI 来解决这些问题。

有关确定群集健康状况的更多信息，请参阅["确定MetroCluster通过 FC 配置中的集群运行状况"](#)。

### 监控MetroCluster通过 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”。

显示所有受监控集群的列表。

2. 从 **Protection: MetroClusters** 视图中，单击要查看MetroCluster over IP 配置详细信息的集群的名称。或者，您可以按MetroCluster配置中的集群进行过滤。
3. 单击插入符号展开行 `v` 图标。仅当集群受到MetroCluster over IP 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结构，以及用于连接的中介器（如果有）。您可以查看以下信息：

- 跨站点连接
- 两个站点的健康和可用性问题的（如果有）
- 调解员相关问题
- 复制相关问题。



报告以下状态：严重 (❌)，错误 (⚠️) 或正常 (✅)。您还可以查看同一拓扑中主数据和镜像数据的聚合数据复制状态。

在下图中，您可以看到源集群和目标集群之间的站点间连接不可用，并且它们之间的中介器未配置。



4. 单击状态图标。显示带有错误定义的消息。如果您的MetroCluster over IP 配置中出现了与该问题相关的事件，您可以单击消息上的“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/运行状况”详细信息页面的“配置”选项卡上的“MetroCluster概述”和“保护”部分中查看更多配置详细信息。



仅对于MetroCluster over IP 配置，您才可以在 **Clusters** 页面上查看集群拓扑。对于MetroCluster over FC 配置中的集群，拓扑显示在“集群/运行状况”详细信息页面上的“MetroCluster连接”选项卡上。

## 相关信息

- ["集群/健康详情页面"](#)
- 有关 关系： **MetroCluster** 视图的信息，请参阅["监控MetroCluster配置"](#)。
- 有关\*关系：过去 1 个月转移状态\*视图的信息，请参阅["关系：最近 1 个月的转移状态视图"](#)。
- 有关\*关系：过去 1 个月转移率\*视图的信息，请参阅["关系：过去 1 个月的转移率视图"](#)。
- 有关“关系：所有关系”视图的信息，请参阅["关系：所有关系视图"](#)。

## 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。您可以识别中断集群组件（例如聚合、节点和存储虚拟机）镜像的问题或任何风险。

Unified Manager 使用系统运行状况警报来监控MetroCluster配置中的组件和连接的状态。

### 开始之前

MetroCluster配置中的本地和远程集群都必须添加到 Unified Manager

### 查看**MetroCluster over IP** 配置的复制

对于MetroCluster over IP 配置，数据复制状态显示在受MetroCluster over IP 保护的集群的拓扑预览视图中，该视图来自 Unified Manager 左侧导航窗格中的以下视图：

- 存储 > 集群 > 保护： **MetroCluster** 视图
- 保护 > 关系 > \*关系： MetroCluster\*视图

有关信息，请参阅["监控MetroCluster over IP 中的连接问题"](#)。

### 查看**MetroCluster**通过 **FC** 配置的复制

按照以下步骤确定MetroCluster通过 FC 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”。

显示受监控集群的列表。



2. 从“**Health: All Clusters**”视图中，单击要查看MetroCluster复制详细信息的集群的名称。在“集群/运行状况详细信息”页面上，单击“MetroCluster复制”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，以及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，您可以查看有关所生成事件的详细信息。

您可以使用集群/健康详情页面中显示的信息来纠正任何复制问题。如果您发现MetroCluster配置中存在镜像问题，则必须登录系统管理器或访问ONTAP CLI 来解决这些问题。

相关信息

["集群/健康详情页面"](#)

## 管理配额

您可以使用用户和组配额来限制用户或用户组可以使用的磁盘空间量或文件数量。您可以查看用户和用户组配额信息，例如磁盘和文件使用情况以及对磁盘设置的各种限制。

### 什么是配额限制

用户配额限制是 Unified Manager 服务器用来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。如果超出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 服务器会向超过配额软限制或达到配额硬限制且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，以通知指定的收件人有关用户或用户组配额事件的信息。

您可以使用ONTAP系统管理器或ONTAP CLI 指定配额限制。

### 查看用户和用户组配额

存储虚拟机/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、磁盘和文件的限制设置、已使用的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”>“存储虚拟机”。
2. 在\*Health: All Storage VMs\*视图中，选择一个存储虚拟机，然后单击\*User and Group Quotas\*选项卡。

相关信息

["添加用户"](#)

## 创建规则以生成电子邮件地址

您可以创建规则，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来指定电子邮件地址。当违反配额时，系统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。
- 您必须已查看“生成用户和组配额电子邮件地址的规则”页面上的指南。

您必须定义配额电子邮件地址的规则，并按照您想要执行的顺序输入它们。例如，如果您要使用电子邮件地址 [abc@xyz.com](mailto:abc@xyz.com) 接收有关 abc 的配额违规通知，并使用电子邮件地址 `dl-$GROUP@$DOMAIN` 接收所有其他组的配额违规通知，则必须按以下顺序列出规则：

- 如果 (`$USER == 'abc'`) 则 [abc@xyz.com](mailto:abc@xyz.com)
- if ( `$GROUP == *` ) then `dl-$GROUP@$DOMAIN`

如果您指定的规则均不满足任何条件，则使用默认规则：

如果 (`$USER_OR_GROUP == *`) 则 `$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. 根据您的标准输入规则。
3. 单击“验证”以验证规则的语法。

如果规则的语法不正确，则会显示错误消息。您必须更正语法并再次单击\*验证\*。

4. 单击“保存”。
5. 验证您创建的电子邮件地址是否显示在存储\*VM/健康\*详细信息页面的\*用户和组配额\*选项卡中。

## 为用户和用户组配额创建电子邮件通知格式

您可以创建一种通知格式，当出现与配额相关的问题（超出软限制或达到硬限制）时，向用户或用户组发送电子邮件。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

### 步骤

1. 在左侧导航窗格中，单击“常规”>“配额电子邮件格式”。
2. 输入或修改“发件人”、“主题”和“电子邮件详细信息”字段中的详细信息。
3. 单击“预览”即可预览电子邮件通知。
4. 单击“关闭”关闭预览窗口。
5. 如果需要，修改电子邮件通知的内容。
6. 单击“保存”。

## 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“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生成的电子邮件地址时，您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。
- 您必须已经查看过[“创建规则的指南”](#)。

如果您编辑电子邮件地址，则生成用户和组配额电子邮件地址的规则将不再适用于该配额。要将通知发送到指定规则生成的电子邮件地址，您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”>“SVM”。
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 | <div>a. 删除“电子邮件地址”字段中的电子邮件地址。</div> <div>b. 单击“保存”。</div> <div>c. 按 F5 刷新浏览器以重新加载“编辑电子邮件地址”对话框。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。</div> |
| 您希望将通知发送到指定的电子邮件地址     | <div>a. 在*电子邮件地址*字段中修改电子邮件地址。</div> <div>b. 单击“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。</div>                                                |

## 详细了解配额

了解有关配额的概念有助于您有效地管理用户配额和用户组配额。

### 配额流程概述

配额分为软配额和硬配额两种类别。当超出指定限制时，软配额会导致ONTAP发送通知，而当超出指定限制时，硬配额会阻止写入操作成功。

当ONTAP收到用户或用户组向FlexVol volume写入的请求时，它会检查该卷上是否为用户或用户组激活了配额，并确定以下内容：

- 是否会达到硬限制

如果是，则达到硬限制时写入操作失败，并发送硬配额通知。

- 软限制是否会被突破

如果是，则当超出软限制时写入操作成功，并发送软配额通知。

- 写入操作是否不会超出软限制

如果是，则写入操作成功，不发送通知。

## 关于配额

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量的方法。您可以使用 `/etc/quotas` 文件。配额适用于特定卷或 qtree。

## 为什么使用配额

您可以使用配额来限制FlexVol卷中的资源使用情况，在资源使用情况达到特定水平时提供通知，或者跟踪资源使用情况。

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

您可以使用“健康状况：所有存储虚拟机”视图中“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。

## 电子邮件通知格式页面

电子邮件通知格式页面显示当出现与配额相关的问题（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：超出用户或组配额磁盘空间软限制、超出用户或组配额文件计数软限制、达到用户或组配额磁盘空间硬限制或达到用户或组配额文件计数硬限制。

- 从

显示发送电子邮件的电子邮件地址，您可以修改该地址。默认情况下，这是通知页面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。您可以根据您的要求修改文本。例如，您可以提供与配额属性相关的信息并减少关键字的数量。但是，您不应该修改关键字。

有效关键字如下：

- \$事件名称

指定导致电子邮件通知的事件名称。

- \$QUOTA\_TARGET

指定配额适用的 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计数软限制

- \$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

指定用户或用户组的名称。

#### 命令按钮

命令按钮使您能够预览、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。

- 恢复出厂默认设置

使您能够将通知格式恢复为出厂默认值。

- 节省

保存对通知格式所做的更改。

通过“生成用户和组配额电子邮件地址的规则”页面，您可以创建规则，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，会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。您还可以添加评论来解释规则。

#### 如何定义规则

您必须按照要执行的顺序输入规则。如果满足第一条规则的标准，则根据该规则生成电子邮件地址。如果不满足该标准，则考虑下一个规则的标准，依此类推。每行列出一条单独的规则。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顺序。但是，您不能更改默认规则的顺序。

例如，如果您要使用电子邮件地址 [qtree1@xyz.com](mailto:qtree1@xyz.com) 接收有关 qtree1 配额违规的通知，并使用电子邮件地址 [admin@xyz.com](mailto:admin@xyz.com) 接收所有其他 qtree 的配额违规通知，则必须按以下顺序列出规则：

- 如果 (`$QTREE == 'qtree1'`) 则 [qtree1@xyz.com](mailto:qtree1@xyz.com)
- 如果 (`$QTREE == *`) 则 [admin@xyz.com](mailto:admin@xyz.com)

如果您指定的规则均不满足任何条件，则使用默认规则：

如果 (`$USER_OR_GROUP == *`) 则 `$USER_OR_GROUP@$DOMAIN`

如果多个用户具有相同的配额，则用户的名称将显示为逗号分隔的值，并且规则不适用于该配额。

#### 如何添加评论

您可以添加注释以描述此规则。您应该在每个注释的开头使用#，并且每行列出一个单独的注释。

#### 规则语法

规则的语法必须是下列之一：

- 如果 (`valid variableoperator *`) 然后 email ID@domain name

if 是关键字并且是小写的。运算符是 `==`。电子邮件 ID 可以包含任意字符、有效变量 `$USER_OR_GROUP`、`$USER` 或 `$GROUP`，或者任意字符和有效变量 `$USER_OR_GROUP`、`$USER` 或 `$GROUP` 的组合。域名可以包含任意字符、有效变量 `$DOMAIN` 或任意字符和有效变量 `$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。

- 如果 (`valid variableoperator `string``) 然后 email ID@domain name

if 是关键字并且是小写的。运算符可以是 `contains` 或 `==`。电子邮件 ID 可以包含任意字符、有效变量 `$USER_OR_GROUP`、`$USER` 或 `$GROUP`，或者任意字符和有效变量 `$USER_OR_GROUP`、`$USER` 或 `$GROUP` 的组合。域名可以包含任意字符、有效变量 `$DOMAIN` 或任意字符和有效变量 `$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。

## 命令按钮

命令按钮使您能够保存、验证或取消已创建的规则：

- 证实

验证所创建规则的语法。如果验证期间出现错误，则会显示生成错误的规则以及错误消息。

- 恢复出厂默认设置

使您能够将地址规则恢复为出厂默认值。

- 节省

验证规则的语法，如果没有错误则保存规则。如果验证期间出现错误，则会显示生成错误的规则以及错误消息。

## 故障排除

故障排除信息可帮助您识别和解决使用 Unified Manager 时遇到的问题。

### 向 Unified Manager 数据库目录添加磁盘空间

Unified Manager 数据库目录包含从ONTAP系统收集的所有健康和性能数据。某些情况下可能需要您增加数据库目录的大小。

例如，如果 Unified Manager 从大量集群（每个集群都有许多节点）收集数据，则数据库目录可能会已满。当数据库目录已满 90% 时，您将收到警告事件；当数据库目录已满 95% 时，您将收到严重事件。



当目录达到 95% 满度后，将不再从集群收集其他数据。

根据 Unified Manager 是在 VMware ESXi 服务器、Red Hat Linux 服务器还是 Microsoft Windows 服务器上运行，向数据目录添加容量所需的步骤会有所不同。

### 为VMware虚拟机数据盘添加空间

如果需要增加 Unified Manager 数据库的数据磁盘空间量，您可以在安装后使用 Unified Manager 维护控制台增加磁盘空间来增加容量。

#### 开始之前

- 您必须具有 vSphere Client 的访问权限。
- 虚拟机一定不能有本地存储的快照。
- 您必须拥有维护用户凭证。

我们建议您在增加虚拟磁盘的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，然后向数据添加更多磁盘容量 disk 3。有关详细信

息，请参阅 VMware 文档。

在极少数情况下，Unified Manager 部署使用“硬盘 2”而不是“硬盘 3”作为数据磁盘。如果您的部署中出现这种情况，请增加较大磁盘的空间。数据磁盘的空间总是比其他磁盘大。

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. 单击控制台窗口，然后使用您的用户名和密码登录维护控制台。
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。

## 为Linux主机的数据目录添加空间

如果您分配的磁盘空间不足 `/opt/netapp/data`` 目录以支持 Unified Manager，当您最初设置 Linux 主机然后安装 Unified Manager 时，您可以在安装后通过增加 `/opt/netapp/data`` 目录。

### 开始之前

您必须具有安装了 Unified Manager 的 Red Hat Enterprise Linux 机器的 root 用户访问权限。

我们建议您在增加数据目录的大小之前备份 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 服务和相关的 MySQL 软件：`systemctl stop ocieau ocie mysqld`
3. 创建临时备份文件夹（例如，`/backup-data`）具有足够的磁盘空间来包含当前 `/opt/netapp/data`` 目录。
4. 复制现有 `/opt/netapp/data`` 目录到备份数据目录：

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

5. 如果启用了 SE Linux：
  - a. 获取现有文件夹的 SE Linux 类型 `/opt/netapp/data`` 文件夹：

```
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：

- a. `cd /opt/netapp/data`
- b. `rm -rf *`

7. 扩大规模 `/opt/netapp/data` 通过 LVM 命令或添加额外的磁盘将目录大小增加到至少 150 GB。



如果您已经创建 `/opt/netapp/data` 从磁盘，那么您不应该尝试安装 `/opt/netapp/data` 作为 NFS 或 CIFS 共享。因为在这种情况下，如果您尝试扩展磁盘空间，一些 LVM 命令，例如 `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）保持不变：

```
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` 这样这个多余的文件就不会在将来导致数据库错误。

11. 复制内容 `backup-data` 回到扩展 `/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，按照所示顺序启动 `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
```

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，您可以向安装 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. 按照与您想要使用的方法相对应的步骤来添加更多空间：

| 选项                                         | 描述                                                  |
|--------------------------------------------|-----------------------------------------------------|
| 在物理服务器上，向安装 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：<br><a href="#">"扩展基本卷"</a>   |
| 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：<br><a href="#">"添加硬盘驱动器"</a> |
| 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：<br><a href="#">"增加磁盘分区的大小"</a>  |

修改性能统计收集间隔

性能统计信息的默认收集间隔为5分钟。如果您发现大型集群的收集未在默认时间内完成，则可以将此间隔更改为 10 或 15 分钟。此设置会影响此 Unified Manager 实例所监控的所有集群的统计信息收集。

开始之前

您必须拥有授权登录 Unified Manager 服务器维护控制台的用户 ID 和密码。

横幅消息指出了性能统计数据收集未按时完成的问题 Unable to consistently collect from cluster <cluster\_name> or Data collection is taking too long on cluster <cluster\_name>.

仅当由于统计信息收集问题而需要时才应更改收集间隔。请勿因任何其他原因更改此设置。



将此值从默认设置 5 分钟更改为其他值可能会影响 Unified Manager 报告的性能事件的数量和频率。例如，当超过策略 30 分钟时，系统定义的性能阈值会触发事件。当使用 5 分钟收集时，必须超过该政策连续六次收集。对于 15 分钟的收集，政策必须仅超出两个收集期。

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 以维护用户身份登录 Unified Manager 主机。

将显示 Unified Manager 维护控制台提示。

2. 键入标有“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字，然后按 Enter。

如果您将 Unified Manager 收集间隔更改为 10 或 15 分钟，并且您当前已连接到外部数据提供商（例如 Graphite），则必须更改数据提供商传输间隔，使其等于或大于 Unified Manager 收集间隔。

## 更改 Unified Manager 保留事件和性能数据的时间长度

默认情况下，Unified Manager 会为所有受监控的集群存储 6 个月的事件数据和性能数据。此后，旧数据将被自动删除，为新数据腾出空间。此默认时间范围适用于大多数配置，但具有许多集群和节点的超大型配置可能需要减少保留期，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类数据的保留期限。这些设置会影响此 Unified Manager 实例所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数据。每天将 5 分钟的统计数据汇总为每小时的性能统计数据。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）。

仅当空间不足或备份和其他操作需要很长时间才能完成时，才应减少保留期。缩短保留期具有以下影响：

- 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数据的位置将为空白。
- 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，警告较旧的性能事件可能在其关联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份数，

然后单击\*保存\*。

## 未知的身份验证错误

当您执行与身份验证相关的操作（例如添加、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

如果您为以下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
- 绑定 OpenLDAP 身份验证服务的可分辨名称

### 纠正措施

1. 在左侧导航窗格中，单击“常规”>“远程身份验证”。
2. 根据您选择的身份验证服务，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”以使用您指定的详细信息测试身份验证。
4. 单击“保存”。

## 未找到用户

当您执行与身份验证相关的操作（例如添加、编辑、删除或测试远程用户或组）时，会显示以下错误消息：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不正确的值，则可能会出现此问题。

### 纠正措施

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适当信息。
3. 单击“保存”。

## 使用其他身份验证服务添加 **LDAP** 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择的模板中的值。如果 LDAP 服务器不使用相同的值，操作可能会失败。

### 原因

OpenLDAP 中的用户配置不正确。

### 纠正措施

您可以使用以下解决方法之一手动修复此问题。

如果您的 LDAP 用户对象类和组对象类分别是用户和组，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. 完成文本字段。

如果您的 LDAP 用户对象类和组对象类分别是 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. 完成文本字段。

如果前两种解决方法不适用，请致电 `option-set` API，并设置 `auth.ldap.userObjectClass` 和 `auth.ldap.groupObjectClass` 选项为正确的值。

## Windows 系统上的 NetApp 可管理性 SDK 日志轮换问题

在 Windows 操作系统上将基于 ONTAPI API 的集群添加到 Unified Manager 后，`nmsdk.log` 文件大小增加并超出 10 MB 的大小限制。

### 原因

如果没有发生日志轮换，则可能会发生此问题。

### 纠正措施

1. 停止 Unified Manager。
2. 在 Windows 上安装 Unified Manager 时，请安装 Logrotate 版本 0.0.0.18。欲了解更多信息，请参阅["NetApp 可管理性 SDK 技术报告的安全强化指南"](#)。
3. 启动 Unified Manager。

# 管理事件和警报

## 管理活动

事件可帮助您识别受监控集群中的问题。

### 什么是 **Active IQ** 平台事件

Unified Manager 可以显示Active IQ平台发现的事件。这些事件是通过针对 Unified Manager 监控的所有存储系统生成的AutoSupport消息运行一组规则而创建的。

有关详细信息，请参阅 ["如何生成 Active IQ 平台事件"](#)。

Unified Manager 会自动检查新规则文件，并且仅在有更新规则时下载新文件。在没有外部网络访问的站点中，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事件与现有的 Unified Manager 事件不重叠，它们可以识别有关系统配置、布线、最佳实践和可用性问题的事件或风险。

有关启用平台事件的更多信息，请参阅["启用Active IQ门户事件"](#)。有关上传规则文件的更多信息，请参阅["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混合云的存储系统操作。看 ["NetApp Active IQ"](#)了解更多信息。

### 什么是事件管理系统事件

事件管理系统 (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。集中监控和管理简化了关键 EMS 事件和基于这些 EMS 事件的警报通知的配置。

当您集群添加到 Unified Manager 时，Unified Manager 地址将作为通知目标添加到集群。一旦集群中发生事件，就会立即报告 EMS 事件。

在 Unified Manager 中接收 EMS 事件的方法有两种：

- 一定数量的重要 EMS 事件会自动报告。
- 您可以订阅接收单独的 EMS 事件。

Unified Manager 生成的 EMS 事件的报告方式根据生成事件的方法而有所不同：

| 功能         | 自动 <b>EMS</b> 消息 | 订阅的 <b>EMS</b> 消息 |
|------------|------------------|-------------------|
| 可用的 EMS 事件 | EMS 事件子集         | 所有 EMS 活动         |

| 功能                         | 自动 <b>EMS</b> 消息                         | 订阅的 <b>EMS</b> 消息                                     |
|----------------------------|------------------------------------------|-------------------------------------------------------|
| 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）     | 格式不具体，为“收到错误 EMS”。详细消息提供了实际 EMS 事件的点符号格式              |
| 收到的消息                      | 一旦发现集群                                   | 将每个所需的 EMS 事件添加到 Unified Manager 后，以及在下一个 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、已确认、已解决和已过时状态 | EMS 事件在集群刷新后（即事件创建后 15 分钟）将失效                         |
| 捕获 Unified Manager 停机期间的事件 | 是的，当系统启动时，它会与每个集群通信以获取缺失的事件              | 否                                                     |
| 活动详情                       | 建议的纠正措施直接从 ONTAP 导入，以提供一致的解决方案           | 事件详情页面中未提供纠正措施                                        |



一些新的自动 EMS 事件是信息事件，表明先前的事件已得到解决。例如，“FlexGroup Constituents Space Status All OK”信息事件表示“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进行管理，但是，如果同一卷收到另一个“空间问题”错误事件，则该事件将自动过时。

## 自动添加到 **Unified Manager** 的 **EMS** 事件

以下 ONTAP EMS 事件会自动添加到 Unified Manager。当 Unified Manager 监控的任何集群触发时，将会生成这些事件。

监控运行 ONTAP 9.5 或更高版本软件的集群时，可以获得以下 EMS 事件：

| 统一管理器事件名称                | <b>EMS</b> 活动名称       | 受影响的资源 | 统一管理器严重性 |
|--------------------------|-----------------------|--------|----------|
| 用于聚合重新定位的云层访问被拒绝         | arl.netra.ca.check.失败 | 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.失败  | 聚合     | 错误       |
| FabricPool 镜像复制重新同步已完成   | waf. ca.重新同步.完成       | 集群     | 错误       |
| FabricPool 空间接近全满        | fabricpool.几乎.已满      | 集群     | 错误       |
| NVMe-oF 宽限期已开始           | nvmf.宽限期.开始           | 集群     | 警告       |

| 统一管理器事件名称                        | EMS 活动名称                      | 受影响的资源 | 统一管理器严重性 |
|----------------------------------|-------------------------------|--------|----------|
| NVMe-oF 宽限期处于活动状态                | nvmf.宽限期.活跃                   | 集群     | 警告       |
| NVMe-oF 宽限期已结束                   | nvmf.宽限期.已过期                  | 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.iamCreds已过期         | 节点     | 错误       |
| Cloud AWS IAMCredsInvalid        | cloud.aws.iamCreds无效          | 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.iamRole无效           | 节点     | 错误       |
| Cloud AWS IAMRoleNotFound        | cloud.aws.iamRoleNotFound     | 节点     | 错误       |
| 无法解析云层主机                         | objstore.host.无法解析            | 节点     | 错误       |
| 云层集群间网络接口已关闭                     | objstore.interclusterlifedown | 节点     | 错误       |
| 请求与云层签名不匹配                       | osc.签名不匹配                     | 节点     | 错误       |
| 一个 NFSv4 池已用尽                    | Nblade.nfsV4PoolExhaust       | 节点     | 批判的      |
| 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       |



| 统一管理器事件名称           | EMS 活动名称                      | 受影响的资源        | 统一管理器严重性 |
|---------------------|-------------------------------|---------------|----------|
| NVMeNS 联机           | NVMeNS.离线                     | 命名空间          | 信息       |
| NVMeNS 脱机           | NVMeNS.online                 | 命名空间          | 信息       |
| NVMeNS 空间不足         | NVMeNS 空间不足                   | 命名空间          | 警告       |
| 同步复制未同步             | 短信状态不同步                       | SnapMirror 关系 | 警告       |
| 同步复制已还原             | 短信状态同步                        | SnapMirror 关系 | 信息       |
| 同步复制自动重新同步失败        | 短信重新同步尝试失败                    | 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.cifsMaxSessPerUserConn | SVM           | 错误       |
| CIFS NetBIOS 名称冲突   | Nblade.cifsNbName冲突           | SVM           | 错误       |
| 尝试连接不存在的 CIFS 共享    | Nblade.cifs无私共享               | SVM           | 批判的      |
| CIFS 卷影复制操作失败       | cifs.shadowcopy.失败            | SVM           | 错误       |
| AV 服务器发现病毒          | Nblade.vscan病毒检测              | SVM           | 错误       |
| 没有可用于病毒扫描的 AV 服务器连接 | Nblade.vscanNoScannerConn     | SVM           | 批判的      |
| 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       |

| 统一管理器事件名称               | EMS 活动名称                                    | 受影响的资源 | 统一管理器严重性 |
|-------------------------|---------------------------------------------|--------|----------|
| 用户未经授权尝试访问 AV 服务器       | Nblade.vscanBadUserPriv Access              | SVM    | 错误       |
| FlexGroup 成分卷存在空间问题     | flexgroup.constituents.有.空间.问题              | 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.有.inodes.问题          | 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               | 监视器.vol.nearFull.inc.sav                    | 卷      | 警告       |
| 卷逻辑空间全满                 | 监视器.vol.full.inc.sav                        | 卷      | 错误       |
| 卷逻辑空间正常                 | 监视器.vol.one.ok.inc.sav                      | 卷      | 信息       |
| WAFL 卷自动调整大小失败          | wافل.vol.自动调整大小失败                           | 卷      | 错误       |
| WAFL 卷自动调整大小已完成         | wافل.vol.自动大小.完成                            | 卷      | 信息       |
| WAFL READDIR 文件操作超时     | wافل.readdir.expired                        | 卷      | 错误       |

## 订阅ONTAP EMS 活动

您可以订阅接收由安装了 ONTAP 软件的系统所生成的事件管理系统 (Event Management System, EMS) 事件。部分 EMS 事件会自动报告给 Unified Manager，但只有您订阅了这些事件，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，因为这可能会在接收同一问题的两个事件时造成混淆。

您可以订阅任意数量的 EMS 事件。您订阅的所有事件都会经过验证，并且只有经过验证的事件才会应用于您在 Unified Manager 中监控的集群。\_ONTAP 9 EMS 事件目录\_提供了指定版本的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。



如果您没有收到您订阅的 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。这样做会将待处理的 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。

要查看您可以订阅的 EMS 事件的名称，您可以从 ONTAP 集群 shell 中使用 ``event route show`` 命令（ONTAP 9 之前版本）或 ``event catalog show`` 命令（ONTAP 9 或更高版本）。

#### ["如何在 Active IQ Unified Manager 中配置和接收来自 ONTAP EMS 事件订阅的警报"](#)

4. 单击“添加”。

EMS 事件已添加到“已订阅的 EMS 事件”列表中，但“适用于集群”列显示您添加的 EMS 事件的状态为“未知”。

5. 单击“保存并关闭”以向集群注册 EMS 事件订阅。
6. 再次单击\*订阅 EMS 事件\*。

您添加的 EMS 事件的“适用于集群”列中将显示状态“是”。

如果状态不是“是”，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，该事件会显示在“事件”页面上。您可以选择事件以在事件详细信息页面中查看有关 EMS 事件的详细信息。您还可以管理事件的处理方式，或者针对事件创建警报。

## 收到事件时会发生什么情况

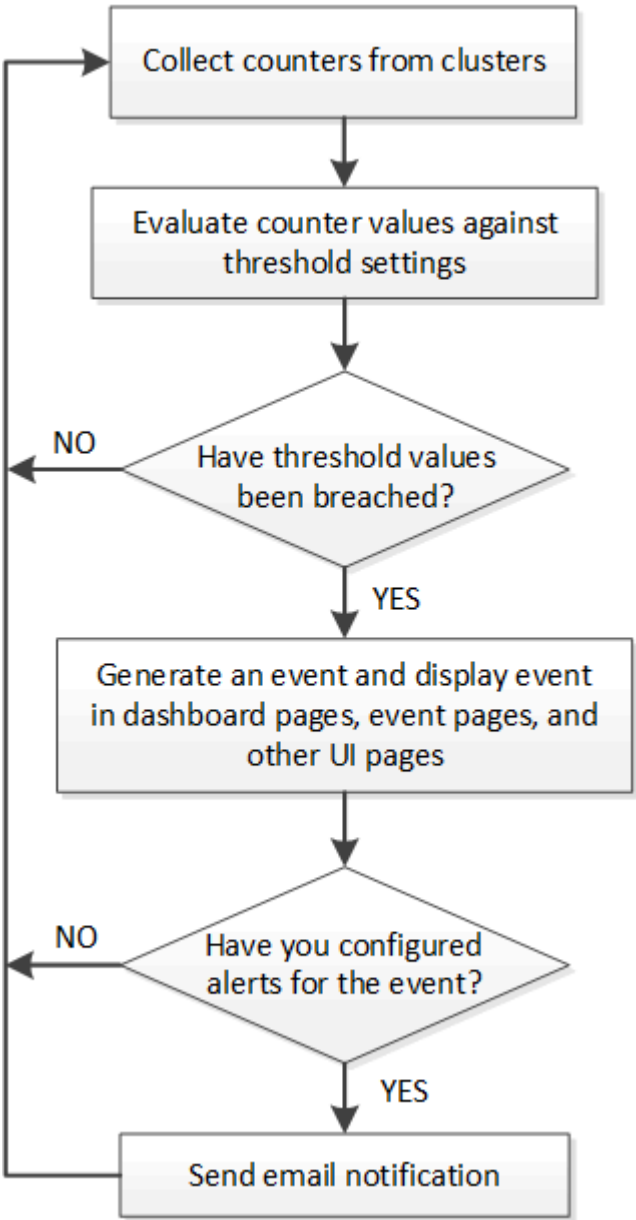
当 Unified Manager 收到事件时，它会显示在“仪表板”页面、“事件管理”库存页面、“集群/性能”页面的“摘要”和“资源管理器”选项卡以及特定于对象的库存页面（例如，“卷/运行状况”库存页面）中。

当 Unified Manager 检测到同一集群组件连续多次出现同一事件条件时，它会将所有出现的事件视为单个事件，而不是单独的事件。事件的持续时间会增加，以表明事件仍然有效。

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。该警报将导致以下操作启动：

- 可以将有关该事件的电子邮件发送给所有 Unified Manager 管理员用户。
- 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。

该工作流程如下图所示。



查看活动和活动详情

您可以查看由 Unified Manager 触发的事件的详细信息，以便采取纠正措施。例如，如果存在健康事件“卷离线”，您可以单击该事件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。

事件详情包括事件来源、事件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”视图显示过去 7 天内生成的、影响级别为事件或风险的新事件和已确认（活动

) 事件。

- 2. 如果您想查看特定类别的事件，例如容量事件或性能事件，请单击\*查看\*并从事件类型菜单中选择。
- 3. 单击要查看其详细信息的事件名称。

事件详情显示在事件详情页面中。

### 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，新事件和已确认事件显示在事件管理库存页面上。

- 2. 从“过滤器”窗格中，选择“分配给”区域中的“未分配”过滤器选项。

### 确认并解决事件

您应该在开始处理生成事件的问题之前确认该事件，这样您就不会继续收到重复的警报通知。对特定事件采取纠正措施后，您应该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。

您可以同时确认并解决多个事件。



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，执行以下操作来确认事件：

| 目的             | 操作                                                                                                                             |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|
| 确认并将单个事件标记为已解决 | <div>a. 单击事件名称。</div> <div>b. 从事件详细信息页面确定事件的原因。</div> <div>c. 单击*确认*。</div> <div>d. 采取适当的纠正措施。</div> <div>e. 单击“标记为已解决”。</div> |

| 目的             | 操作                                                                                                                                              |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 确认并将多个事件标记为已解决 | <ol style="list-style-type: none"> <li>从相应的事件详细信息页面确定事件的原因。</li> <li>选择事件。</li> <li>单击*确认*。</li> <li>采取适当的纠正措施。</li> <li>单击“标记为已解决”。</li> </ol> |

事件被标记为已解决后，该事件将被移至已解决事件列表。

- 可选：在\*注释和更新\*区域，添加有关如何处理事件的注释，然后单击\*发布\*。

## 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另一个用户。例如，当存储对象频繁出现问题时，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

- 必须正确配置用户的姓名和电子邮件 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

- 在左侧导航窗格中，单击“事件管理”。
- 在\*事件管理\*库存页面中，选择一个或多个要分配的事件。
- 通过选择以下选项之一来分配事件：

| 如果您想将事件分配给... | 操作                                                                                                                                                                                                                                                                                                  |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 你自己           | 单击“分配给”>“我”。                                                                                                                                                                                                                                                                                        |
| 其他用户          | <ol style="list-style-type: none"> <li>单击*分配给*&gt;*其他用户*。</li> <li>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。</li> <li>单击*分配*。</li> </ol> <p>电子邮件通知已发送给用户。</p> <div>  <p>如果您不输入用户名或从下拉列表中选择用户，然后单击“分配”，则该事件仍未分配。</p> </div> |

## 禁用不需要的事件

默认情况下，所有事件均启用。您可以全局禁用事件，以防止生成对您的环境不重要的事件的通知。当您想要恢复接收已禁用的事件的通知时，您可以启用这些事件。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

当您禁用事件时，系统中先前生成的事件将被标记为过时，并且不会触发为这些事件配置的警报。当您启用已禁用的事件时，将从下一个监控周期开始生成这些事件的通知。

当您禁用某个对象的某个事件时（例如，`vol offline` 事件），然后您启用该事件，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。仅当重新启用事件后对象状态发生变化时，Unified Manager 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 | <div>a. 单击“禁用”。</div> <div>b. 在“禁用事件”对话框中，选择事件严重性。</div> <div>c. 在匹配事件列中，根据事件严重性选择要禁用的事件，然后单击向右箭头将这些事件移动到禁用事件列。</div> <div>d. 单击“保存并关闭”。</div> <div>e. 验证您禁用的事件是否显示在“事件设置”页面的列表视图中。</div> |
| 启用事件 | <div>a. 选中要启用的一个或多个事件的复选框。</div> <div>b. 单击“启用”。</div>                                                                                                                                    |

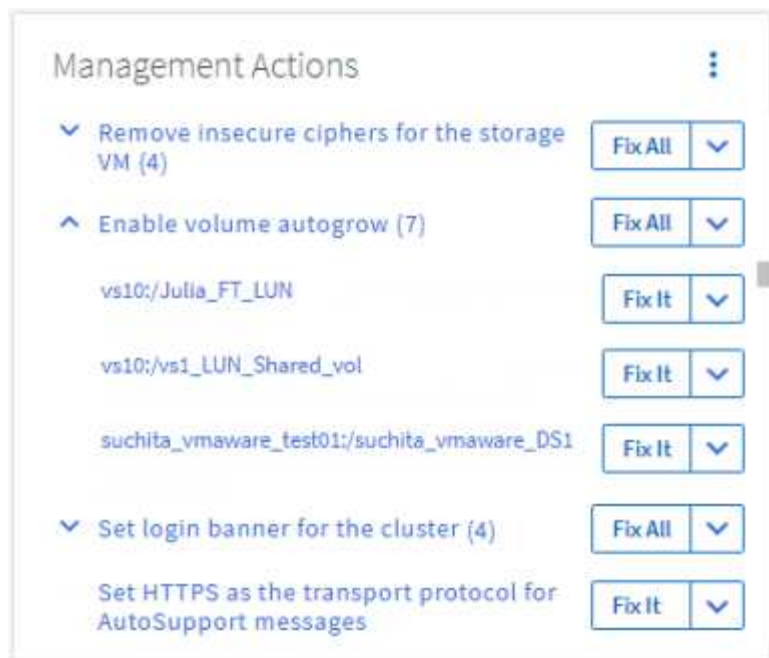
## 使用 Unified Manager 自动修复功能解决问题

对于某些事件，Unified Manager 可以彻底诊断并使用 **Fix It** 按钮提供单一解决方案。当可用时，这些解决方案将显示在仪表板、事件详细信息页面以及左侧导航菜单上的工作负载分析选择中。

大多数事件都有多种可能的解决方案，这些解决方案显示在事件详细信息页面中，以便您可以使用ONTAP系统管理器或ONTAP CLI 实施最佳解决方案。当 Unified Manager 确定存在一个解决方案来修复该问题、并且可以使用ONTAP CLI 命令解决该问题时，可以执行 修复 操作。

### 步骤

1. 要从\*仪表板\*查看可修复的事件，请单击\*仪表板\*。



2. 要解决 Unified Manager 可以修复的任何问题，请单击“修复”按钮。要修复多个对象上存在的问题，请单击“修复全部”按钮。

有关可通过自动修复修复的问题的信息，请参阅[Unified Manager 可以修复哪些问题](#)。

## 启用和禁用Active IQ事件报告

默认情况下，Active IQ平台事件在 Unified Manager 用户界面中生成并显示。如果您发现这些事件太“嘈杂”，或者您不想在 Unified Manager 中查看这些事件，那么您可以禁用这些事件的生成。如果您想恢复接收这些通知，可以稍后启用它们。

开始之前

您必须具有应用程序管理员角色。

当您禁用此功能时，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。开始时间取决于 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来禁用或启用Active IQ平台事件：

| 目的              | 操作                                        |
|-----------------|-------------------------------------------|
| 禁用Active IQ平台事件 | 在* Active IQ Portal Events*面板中，将滑块按钮向左移动。 |
| 启用Active IQ平台事件 | 在* Active IQ Portal Events*面板中，将滑块按钮向右移动。 |



## 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，并在有更新的规则时下载新文件。但是，在没有外部网络访问的站点中，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安装或升级 Unified Manager 到特定版本时，捆绑的Active IQ规则将自动可供上传。但是，建议您大约每月从 NetApp 的支持站点下载一次新规则文件，以确保生成更新的事件并且您的存储系统继续以最佳状态运行。

### 开始之前

- 必须启用Active IQ门户事件报告。此功能默认启用。有关信息，请参阅["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](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 KB 文章。



在 Windows 系统上，在没有网络连接的站点中， NetApp KB 文章默认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`文件并上传它以查看所有规则的知识库文章。

2. 将规则文件传输到可以带入安全区域的某些媒体，然后将其复制到安全区域中的系统上。
3. 在左侧导航窗格中，单击“存储管理”>“事件设置”。
4. 在\*事件设置\*页面中，单击\*上传规则\*按钮。
5. 在“上传规则”对话框中，导航到并选择规则`.zip`下载的文件并单击\*上传\*。

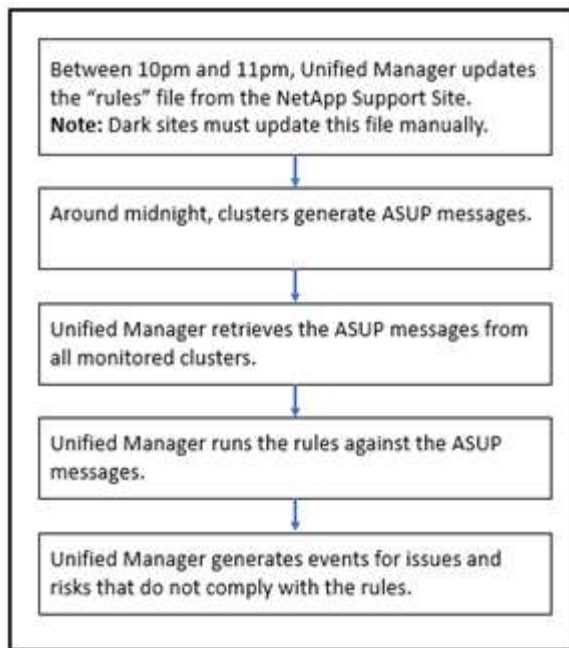
此过程可能需要几分钟时间。

规则文件在 Unified Manager 服务器上解压缩。当您管理的集群在午夜后生成AutoSupport文件时，Unified Manager 会根据规则文件检查集群并根据需要生成新的风险和事件。

有关详细信息，请参阅此知识库 (KB) 文章：["如何在Active IQ Unified Manager中手动更新 AIQCA Secure 规则"](#)。

## 如何生成 Active IQ 平台事件

Active IQ平台事件和风险转换为 Unified Manager 事件，如下图所示。

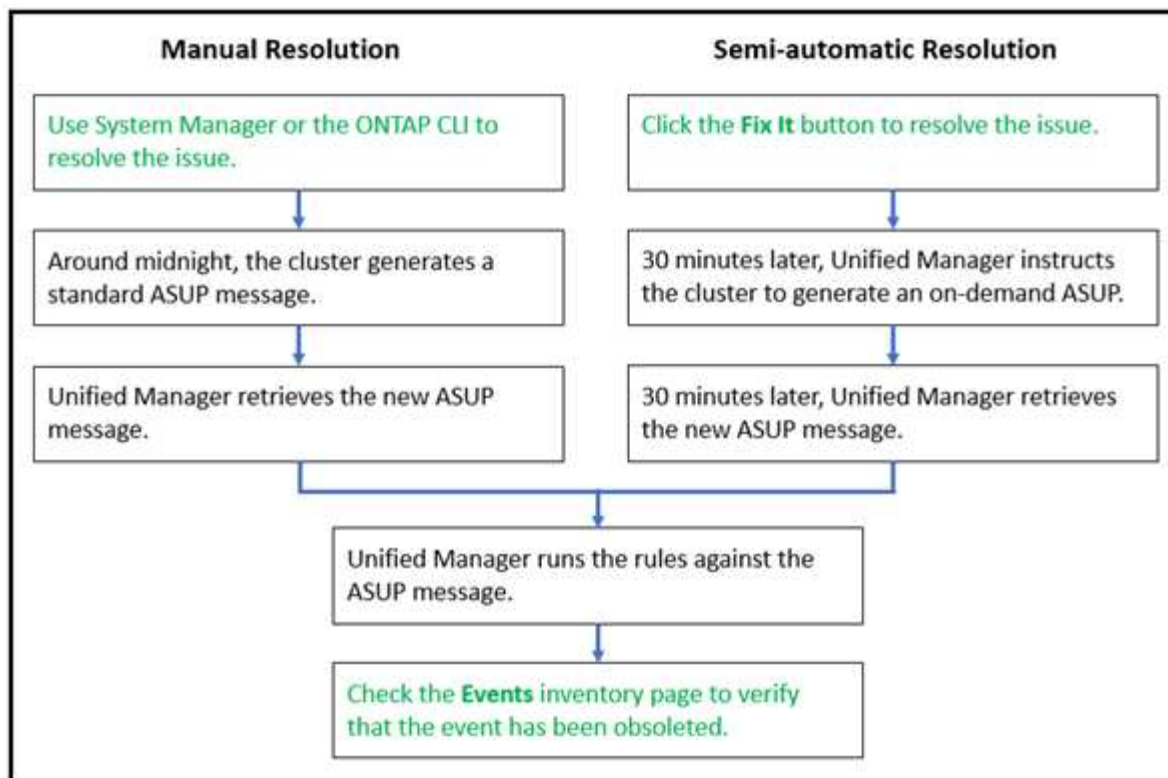


如您所见，在Active IQ平台上编译的规则文件保持最新，集群AutoSupport消息每天生成，并且 Unified Manager 每天更新事件列表。

## 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解决，并且具有相同的可用状态。但是，当您使用“修复”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，您必须登录系统管理器或ONTAP命令行界面来解决问题。只有在集群于午夜生成新的AutoSupport消息后，您才能够验证该问题。

当使用“修复”按钮执行半自动解决方案时，您可以在数小时内验证修复是否成功。

## 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 服务器中保留的月份数。

开始之前

您必须具有应用程序管理员角色。

保留事件超过 6 个月可能会影响服务器性能，因此不建议这样做。

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份数，然后单击\*保存\*。

## Unified Manager 维护窗口是什么

当您安排了集群维护并且不想收到大量不必要的通知时，您可以定义 Unified Manager 维护窗口来抑制特定时间范围内的事件和警报。

当维护窗口开始时，“对象维护窗口已启动”事件将发布到事件管理库存页面。维护时段结束后，此事件将自动失效。

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，并且不会针对

这些事件发送任何警报或其他类型的通知。但是，您可以通过选择“事件管理”库存页面上的“查看”选项之一来查看维护时段内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，还可以取消计划维护窗口。

#### 安排维护时段以禁用集群事件通知

如果您计划对集群进行停机，例如，升级集群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。

在维护时段期间，仍会生成与该集群上所有对象相关的事件，但它们不会出现在事件页面中，并且不会针对这些事件发送任何警报或其他类型的通知。

您输入的维护窗口时间基于 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。

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”。

滑块按钮旁边会出现“已安排”消息。

当达到开始时间时，集群进入维护模式并生成“对象维护窗口已开始”事件。

#### 更改或取消计划的维护时段

如果您已配置将来发生的 Unified Manager 维护窗口，则可以更改开始时间和结束时间或取消发生维护窗口。

#### 开始之前

您必须具有应用程序管理员或存储管理员角色。

如果您在计划的维护时段结束时间之前完成了集群维护，并且想要再次开始接收来自集群的事件和警报，则取消当前正在运行的维护时段很有用。

#### 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...                                                  |
|---------------|-----------------------------------------------------------|
| 更改计划维护时段的时间范围 | a. 单击滑块按钮旁边的文本“Scheduled”。<br>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长度   | a. 单击滑块按钮旁边的文本“Active”。<br>b. 更改结束日期和时间，然后单击“应用”。         |
| 取消计划的维护时段     | 选择滑块按钮并将其向左移动。                                            |
| 取消活动维护时段      | 选择滑块按钮并将其向左移动。                                            |

## 查看维护时段内发生的事件

如有必要，您可以查看 Unified Manager 维护时段内为所有存储对象生成的事件。一旦维护窗口结束并且所有系统资源恢复运行，大多数事件将出现在过时状态。

### 开始之前

必须至少完成一个维护窗口，然后才能获得任何事件。

默认情况下，维护时段内发生的事件不会出现在事件管理库存页面上。

### 步骤

1. 在左侧导航窗格中，单击“事件”。

默认情况下，所有活动（新事件和已确认）事件都会显示在事件管理库存页面上。

2. 从视图窗格中，选择选项\*维护期间生成的所有事件\*。

显示过去 7 天内所有维护时段会话和所有集群触发的事件列表。

3. 如果单个集群有多个维护窗口，您可以单击\*触发时间\*日历图标并选择您感兴趣的维护窗口事件的时间段。

## 管理主机系统资源事件

Unified Manager 包含一项服务，用于监控安装了 Unified Manager 的主机系统上的资源问题。诸如可用磁盘空间不足或主机系统内存不足等问题可能会触发管理站事件，这些事件会以横幅消息的形式显示在 UI 顶部。

管理站事件表明安装了 Unified Manager 的主机系统存在问题。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严重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                                                          |
|-----------|-------------------------------------------------------------|
| 查看活动详情    | 单击事件横幅可显示包含该问题的建议解决方案的事件详细信息页面。                             |
| 查看所有管理站事件 | a. 在左侧导航窗格中，单击“事件管理”。<br>b. 在事件管理清单页面的过滤器窗格中，单击源类型列表中的管理站框。 |

### 了解更多活动信息

了解有关事件的概念有助于您有效地管理集群和集群对象并适当地定义警报。

#### 事件状态定义

事件的状态可以帮助您确定是否需要采取适当的纠正措施。事件可以是新的、已确认的、已解决的或已过时的。请注意，新事件和已确认事件均被视为活动事件。

事件状态如下：

- 新的

新事件的状态。

- 已确认

您确认事件时的状态。

- 已解决

事件被标记为已解决时的状态。

- 过时的

事件被自动纠正或事件原因不再有效时的状态。



您无法确认或解决过时的事件。

#### 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的变化。

当触发事件“Cluster Not Reachable”时，事件状态为“New”。当您确认该事件时，事件状态将更改为“已确认”。当您采取适当的纠正措施后，您必须将事件标记为已解决。事件状态随后变为“已解决”。

如果由于断电而生成“群集不可达”事件，则当电源恢复时，群集将开始运行，无需任何管理员干预。因此，“集群

不可达”事件不再有效，并且事件状态在下一个监控周期中变为“过时”。

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有关事件状态的信息。SNMP 陷阱还包括有关事件状态的信息。

#### 事件严重性类型的说明

每个事件都与严重性类型相关联，以帮助确定需要立即采取纠正措施的事件的优先级。

- 批判的

出现问题，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

事件源经历了您应该注意的事件，或者群集对象的性能计数器超出了正常范围，应该进行监视以确保其不会达到严重程度。这种严重程度的事件不会导致服务中断，并且可能不需要立即采取纠正措施。

性能警告事件由用户定义、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，就会发生该事件。例如，当删除任何存储对象或发生任何配置更改时，就会生成严重性类型为信息的事件。

当 ONTAP 检测到配置更改时，会直接从 ONTAP 发送信息事件。

#### 事件影响级别的说明

每个事件都与一个影响级别（事件、风险、事件或升级）相关联，以帮助确定需要立即采取纠正措施的事件的优先级。

- 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存储空间的事件。影响级别为“事故”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

风险是一系列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的事件。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况的变化。影响级别为“事件”的事件仅供参考，不需要采取纠正措施。

- 升级

升级事件是Active IQ平台报告的一种特定类型的事件。这些事件标识了需要您升级ONTAP软件、节点固件或操作系统软件（以获取安全公告）才能解决的问题。您可能希望立即对其中一些问题采取纠正措施，而其他问题可能要等到下次预定的维护时再解决。

## 事件影响区域的说明

事件分为六个影响领域（可用性、容量、配置、性能、保护和安全），以使您能够专注于您负责的事件类型。

- 可用性

如果存储对象离线、协议服务中断、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

如果您的聚合、卷、LUN 或命名空间正在接近或已达到大小阈值，或者增长率对于您的环境而言异常，容量事件会通知您。

- 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。

- 表现

性能事件会通知您集群上的资源、配置或活动状况，这些状况可能会对受监控的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、目标容量问题、SnapVault关系问题或保护作业问题的事件或风险。任何托管二级卷和保护关系的ONTAP对象（尤其是聚合、卷和 SVM）都归类到保护影响区域中。

- 安全

安全事件会根据定义参数通知您ONTAP集群、存储虚拟机 (SVM) 和卷的安全性 ["NetApp ONTAP 9 安全强化指南"](#)。

此外，该区域还包括从Active IQ平台报告的升级事件。

## 如何计算对象状态

对象状态由当前处于“新”或“已确认”状态的最严重事件决定。例如，如果对象状态为“错误”，则该对象事件之一的严重性类型为“错误”。采取纠正措施后，事件状态将变为“已解决”。

## 动态性能事件图表详细信息

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争用集群组件中延迟或使用



## 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到上次分析该事件的时间。图表还显示处于争用的集群组件的历史性能统计数据。

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移动到利用率较低的组件。移动工作负载将会减少当前组件的工作量，甚至可能使该组件不再发生争用。此部分的顶部是检测到事件并最后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），最后分析的时间会更新。

当您将光标悬停在图表上时，延迟和活动图表会显示主要工作负载的名称。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对其进行排序，包括“sharks”、“bullies”或“victims”，并显示有关其延迟及其在争用集群组件上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["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。具有非常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更多信息，请参阅["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名并确定排序顺序的信息，请参阅["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 24 小时的性能统计数据。每个工作负载的实际值和预期值均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才参与其中，因此其性能统计数据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，因此如果事件超过 30 天，则不会显示任何性能数据。

### • 工作负载排序列

#### ◦ 延迟图表

显示上次分析时该事件对工作负载延迟的影响。

#### ◦ 组件使用情况列

显示有关争用中的集群组件的工作负载使用情况的详细信息。在图表中，实际使用情况是一条蓝线。红色条突出显示事件持续时间，从检测时间到最后分析时间。有关详细信息，请参阅["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

显示网络处理、数据处理和聚合组件的利用率历史记录（以百分比表示），或显示 QoS 策略组组件的活动历史记录（以百分比表示）。该图表不显示网络或互连组件。您可以指向统计信息来查看特定时间点的使用情况统计信息。

#### ◦ 总写入 **MB/s** 历史记录

仅适用于MetroCluster资源组件，显示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/秒 (MBps) 为单位）。

- 事件历史

显示红色阴影线来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之后发生的事件。

## Unified Manager 检测到的配置更改

Unified Manager 监控集群的配置变化，以帮助确定变化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 (●) 来指示检测到变化的日期和时间。

您可以查看性能资源管理器页面和工作负载分析页面中的性能图表，以了解更改事件是否影响了所选集群对象的性能。如果在性能事件发生时或大约同时检测到变化，则该变化可能导致问题，从而触发事件警报。

Unified Manager 可以检测以下变更事件，这些事件被归类为信息事件：

- 卷在聚合体之间移动。

Unified Manager 可以检测移动何时进行、完成或失败。如果 Unified Manager 在卷移动期间关闭，则当它重新启动时，它会检测卷移动并显示其更改事件。

- 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) 限制发生变化。

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，这也可能会触发策略组的事件。延迟逐渐恢复正常，并且由峰值引起的任何事件都会消失。

- HA 对中的节点接管或归还其配对节点的存储。

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，Unified Manager 将不会检测到该事件。

- ONTAP升级或恢复操作已成功完成。

显示先前版本和新版本。

## 事件和严重性类型列表

您可以使用事件列表来熟悉事件类别、事件名称以及您可能在 Unified Manager 中看到的每个事件的严重性类型。事件按照对象类别的字母顺序列出。

### 聚合事件

聚合事件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。

影响区域：可用性

星号 (\*) 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<br>(ocumEvtAggregateStateOffline)                             | 意外事件 | 聚合  | 批判的 |
| 聚合失败<br>(ocumEvtAggregateStateFailed)                              | 意外事件 | 聚合  | 批判的 |
| 聚合限制<br>(ocumEvtAggregateStateRestricted)                          | 风险   | 聚合  | 警告  |
| 聚合重建<br>(ocumEvtAggregateRaidStateReconstructing)                  | 风险   | 聚合  | 警告  |
| 聚合降级<br>(ocumEvtAggregateRaidStateDegraded)                        | 风险   | 聚合  | 警告  |
| 云层部分可达<br>(ocumEventCloudTierPartiallyReachable)                   | 风险   | 聚合  | 警告  |
| 云层无法访问<br>(ocumEventCloudTierUnreachable)                          | 风险   | 聚合  | 错误  |
| 拒绝云层访问以进行聚合重新定位<br>*(arlNetraCaCheckFailed)                        | 风险   | 聚合  | 错误  |
| 存储故障转移期间拒绝云层访问以进行聚合重定位<br>*(gbNetraCaCheckFailed)                  | 风险   | 聚合  | 错误  |
| MetroCluster聚合滞后<br>(ocumEvtMetroClusterAggregateLeftBehind)       | 风险   | 聚合  | 错误  |
| MetroCluster聚合镜像降级<br>(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 |
|---------------------------------------------------|------|-----|-----|
| 聚合空间几乎已满<br>(ocumEvtAggregateNearlyFull)          | 风险   | 聚合  | 警告  |
| 聚合空间已满<br>(ocumEvtAggregateFull)                  | 风险   | 聚合  | 错误  |
| 满载前的总天数<br>(ocumEvtAggregateDaysUntilFullSoon)    | 风险   | 聚合  | 错误  |
| 聚合过度提交<br>(ocumEvtAggregateOvercommitted)         | 风险   | 聚合  | 错误  |
| 聚合几乎过度承诺<br>(ocumEvtAggregateAlmostOvercommitted) | 风险   | 聚合  | 警告  |
| 聚合快照保留已满<br>(ocumEvtAggregateSnapReserveFull)     | 风险   | 聚合  | 警告  |
| 总体增长率异常<br>(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 |
|-------------|------|-----|-----|
| 发现的总量（不适用）  | 事件   | 聚合  | 信息  |
| 聚合重命名（不适用）  | 事件   | 聚合  | 信息  |
| 已删除的集合（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 |
|-------------------------------------------------------------|------|-----|-----|
| 聚合 IOPS 临界阈值被突破<br>(ocumAggregateIopsIncident)              | 意外事件 | 聚合  | 批判的 |
| 超出聚合 IOPS 警告阈值<br>(ocumAggregateIopsWarning)                | 风险   | 聚合  | 警告  |
| 总计 MB/s 临界阈值突破<br>(ocumAggregateMbpsIncident)               | 意外事件 | 聚合  | 批判的 |
| 超出聚合 MB/s 警告阈值<br>(ocumAggregateMbpsWarning)                | 风险   | 聚合  | 警告  |
| 聚合延迟临界阈值突破<br>(ocumAggregateLatencyIncident)                | 意外事件 | 聚合  | 批判的 |
| 超出聚合延迟警告阈值<br>(ocumAggregateLatencyWarning)                 | 风险   | 聚合  | 警告  |
| 已使用总体性能容量临界阈值已突破<br>(ocumAggregatePerfCapacityUsedIncident) | 意外事件 | 聚合  | 批判的 |
| 已使用总体性能容量警告阈值已突破<br>(ocumAggregatePerfCapacityUsedWarning)  | 风险   | 聚合  | 警告  |
| 总体利用率临界阈值被突破<br>(ocumAggregateUtilizationIncident)          | 意外事件 | 聚合  | 批判的 |
| 超出聚合利用率警告阈值<br>(ocumAggregateUtilizationWarning)            | 风险   | 聚合  | 警告  |

| 事件名称（陷阱名称）                                              | 影响级别 | 源类型 | 严重性 |
|---------------------------------------------------------|------|-----|-----|
| 聚合磁盘过度利用阈值超出<br>(ocumAggregateDisksOverUtilizedWarning) | 风险   | 聚合  | 警告  |
| 聚合动态阈值突破<br>(ocumAggregateDynamicEventWarning)          | 风险   | 聚合  | 警告  |

## 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 (\*) 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<br>(ocumEvtDisksNoSpare s)                              | 风险   | 集群  | 警告  |
| 集群不可访问<br>(ocumEvtClusterUnreachable)                            | 风险   | 集群  | 错误  |
| 集群监控失败<br>(ocumEvtClusterMonitoringFailed)                       | 风险   | 集群  | 警告  |
| 集群FabricPool许可证容量限制已超出<br>(ocumEvtExternalCapacityTierSpaceFull) | 风险   | 集群  | 警告  |
| NVMe-oF 宽限期开始*(nvmfGracePeriodStart)                             | 风险   | 集群  | 警告  |
| NVMe-oF 宽限期活动*(nvmfGracePeriodActive)                            | 风险   | 集群  | 警告  |

| 事件名称（陷阱名称）                                                                 | 影响级别 | 源类型 | 严重性 |
|----------------------------------------------------------------------------|------|-----|-----|
| NVMe-oF 宽限期已过期<br>*(nvmfGracePeriodExpired)                                | 风险   | 集群  | 警告  |
| 对象维护窗口已启动<br>(objectMaintenanceWindowStarted)                              | 事件   | 集群  | 批判的 |
| 对象维护窗口结束<br>(objectMaintenanceWindowEnded)                                 | 事件   | 集群  | 信息  |
| MetroCluster剩余磁盘<br>(ocumEvtSpareDiskLeftBehind)                           | 风险   | 集群  | 错误  |
| MetroCluster自动计划外切换已禁用<br>(ocumEvtMccAutomaticUnplannedSwitchOverDisabled) | 风险   | 集群  | 警告  |
| 集群用户密码已更改<br>*(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 |
|------------------------------------------------------|------|-----|-----|
| 集群容量不平衡阈值突破<br>(ocumConformanceNodeImbalanceWarning) | 风险   | 集群  | 警告  |
| 集群云层规划<br>(clusterCloudTierPlanningWarning)          | 风险   | 集群  | 警告  |
| FabricPool镜像复制重新同步已完成*<br>(wafCaResyncComplete)      | 事件   | 集群  | 警告  |
| FabricPool空间几乎已满<br>*(fabricpoolNearlyFull)          | 风险   | 集群  | 错误  |

| 事件名称（陷阱名称）      | 影响级别 | 源类型 | 严重性 |
|-----------------|------|-----|-----|
| 节点已添加（不适用）      | 事件   | 集群  | 信息  |
| 节点已移除（不适用）      | 事件   | 集群  | 信息  |
| 集群已移除（不适用）      | 事件   | 集群  | 信息  |
| 群集添加失败（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  | 批判的 |
| 收到关键 EMS（不适用）   | 事件   | 集群  | 批判的 |
| 已收到警报 EMS（不适用）  | 事件   | 集群  | 错误  |
| 错误 EMS 已收到（不适用） | 事件   | 集群  | 警告  |
| 警告 EMS 已收到（不适用） | 事件   | 集群  | 警告  |
| 收到调试 EMS（不适用）   | 事件   | 集群  | 警告  |
| 通知 EMS 已收到（不适用） | 事件   | 集群  | 警告  |
| 信息 EMS 已收到（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 |
|-------------------------|-------------------|
| 批判的                     | 紧急<br>批判的         |
| 错误                      | 警报                |



|    |                            |
|----|----------------------------|
| 警告 | 错误<br>警告<br>调试<br>通知<br>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 |
|-----------------------------------------------|------|-----|-----|
| 集群负载不平衡阈值突破()                                 | 风险   | 集群  | 警告  |
| 集群 IOPS 临界阈值被突破<br>(ocumClusterIopsIncident)  | 意外事件 | 集群  | 批判的 |
| 集群 IOPS 警告阈值超出<br>(ocumClusterIopsWarning)    | 风险   | 集群  | 警告  |
| 集群 MB/s 临界阈值突破<br>(ocumClusterMbpsIncident)   | 意外事件 | 集群  | 批判的 |
| 集群 MB/s 警告阈值超出<br>(ocumClusterMbpsWarning)    | 风险   | 集群  | 警告  |
| 集群动态阈值被突破<br>(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<br>(ocumClusterASUPHttpsConfiguredDisabled) | 风险   | 集群  | 警告  |

| 事件名称（陷阱名称）                                          | 影响级别 | 源类型 | 严重性 |
|-----------------------------------------------------|------|-----|-----|
| 日志转发未加密<br>(ocumClusterAuditLogUnencrypted)         | 风险   | 集群  | 警告  |
| 默认本地管理员用户已启用<br>(ocumClusterDefaultAdminEnabled)    | 风险   | 集群  | 警告  |
| FIPS 模式已禁用<br>(ocumClusterFipsDisabled)             | 风险   | 集群  | 警告  |
| 登录横幅已禁用<br>(ocumClusterLoginBannerDisabled)         | 风险   | 集群  | 警告  |
| 登录横幅已更改<br>(ocumClusterLoginBannerChanged)          | 风险   | 集群  | 警告  |
| 日志转发目的地已更改<br>(ocumLogForwardDestinationsChanged)   | 风险   | 集群  | 警告  |
| NTP 服务器名称已更改<br>(ocumNtpServerNamesChanged)         | 风险   | 集群  | 警告  |
| NTP 服务器数量低<br>(securityConfigNTPServerCountLowRisk) | 风险   | 集群  | 警告  |
| 集群对等通信未加密<br>(ocumClusterPeerEncryptionDisabled)    | 风险   | 集群  | 警告  |
| SSH 正在使用不安全的密码<br>(ocumClusterSSHInsecure)          | 风险   | 集群  | 警告  |
| 已启用 Telnet 协议<br>(ocumClusterTelnetEnabled)         | 风险   | 集群  | 警告  |

| 事件名称（陷阱名称）                                                          | 影响级别 | 源类型 | 严重性 |
|---------------------------------------------------------------------|------|-----|-----|
| 某些ONTAP用户帐户的密码使用安全性较低的 MD5 哈希函数<br>(ocumClusterMD5PasswordHashUsed) | 风险   | 集群  | 警告  |
| 集群使用自签名证书<br>(ocumClusterSelfSignedCertificate)                     | 风险   | 集群  | 警告  |
| 集群远程 Shell 已启用<br>(ocumClusterRshDisabled)                          | 风险   | 集群  | 警告  |
| 集群证书即将过期<br>(ocumEvtClusterCertificateAboutToExpire)                | 风险   | 集群  | 警告  |
| 集群证书已过期<br>(ocumEvtClusterCertificateExpired)                       | 风险   | 集群  | 错误  |

## 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。

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 - 备用块几乎已用完<br>(ocumEvtClusterFlashDiskFewerSpareBlockError) | 风险   | 集群  | 错误  |
| 闪存磁盘 - 无备用块<br>(ocumEvtClusterFlashDiskNoSpareBlockCritical)     | 意外事件 | 集群  | 批判的 |
| 一些未分配的磁盘<br>(ocumEvtClusterUnassignedDisksSome)                  | 风险   | 集群  | 警告  |

| 事件名称（陷阱名称）                         | 影响级别 | 源类型 | 严重性 |
|------------------------------------|------|-----|-----|
| 部分故障磁盘<br>(ocumEvtDisksSomeFailed) | 意外事件 | 集群  | 批判的 |

## 机箱事件

机箱事件为您提供有关数据中心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。

### 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 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-----|-----|
| 磁盘架风扇故障<br>(ocumEvtShelfFanFailed)                                                                                                                                                                   | 意外事件 | 储物架 | 批判的 |
| 磁盘架电源故障<br>(ocumEvtShelfPowerSupplyFailed)                                                                                                                                                           | 意外事件 | 储物架 | 批判的 |
| 未配置磁盘架多路径<br>(ocumDiskShelfConnectivityNotInMultiPath)<br><br>此活动不适用于： <ul style="list-style-type: none"> <li>• MetroCluster配置中的集群</li> <li>• 以下平台：<br/>FAS2554、FAS2552、FAS2520 和 FAS2240</li> </ul> | 风险   | 节点  | 警告  |
| 磁盘架路径故障<br>(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  |
| 磁盘架已移除（不适用） | 事件   | 节点  | 信息  |

## 风扇事件

风扇事件为您提供有关数据中心节点上风扇状态的信息，以便您监控潜在问题。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。

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 |
|---------------------------------------------|------|-----|-----|
| 一个或多个风扇发生故障<br>(ocumEvtFansOneOrMoreFailed) | 意外事件 | 节点  | 批判的 |

## 闪存卡事件

闪存卡事件为您提供有关数据中心节点上安装的闪存卡的状态信息，以便您监控潜在问题。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。

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 |
|------------------------------------|------|-----|-----|
| 离线抽认卡<br>(ocumEvtFlashCardOffline) | 意外事件 | 节点  | 批判的 |

## 索引节点事件

当 inode 已满或接近已满时，inode 事件会提供信息，以便您可以监控潜在问题。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。

影响区域：容量

| 事件名称（陷阱名称）                              | 影响级别 | 源类型 | 严重性 |
|-----------------------------------------|------|-----|-----|
| Inode 几乎已满<br>(ocumEvtInodesAlmostFull) | 风险   | 卷   | 警告  |
| Inode 已满<br>(ocumEvtInodesFull)         | 风险   | 卷   | 错误  |

## 网络接口 (LIF) 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。

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 |
|------------------------------------------------|------|-----|-----|
| 网络接口状态关闭<br>(ocumEvtLifStatusDown)             | 风险   | 接口  | 错误  |
| FC/FCoE 网络接口状态关闭<br>(ocumEvtFCLifStatusDown)   | 风险   | 接口  | 错误  |
| 网络接口故障转移不可能<br>(ocumEvtLifFailoverNotPossible) | 风险   | 接口  | 警告  |
| 网络接口不在主端口<br>(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 |
|--------------------------------------------------|------|-----|-----|
| 网络接口 MB/s 临界阈值突破<br>(ocumNetworkLifMbpsIncident) | 意外事件 | 接口  | 批判的 |
| 网络接口 MB/s 警告阈值已超出<br>(ocumNetworkLifMbpsWarning) | 风险   | 接口  | 警告  |
| FC 网络接口 MB/s 临界阈值突破<br>(ocumFcplifMbpsIncident)  | 意外事件 | 接口  | 批判的 |

| 事件名称（陷阱名称）                                              | 影响级别 | 源类型 | 严重性 |
|---------------------------------------------------------|------|-----|-----|
| FC 网络接口 MB/s 警告阈值超出<br>(ocumFcpLifMbpsWarning)          | 风险   | 接口  | 警告  |
| NVMf FC 网络接口 MB/s 临界阈值突破<br>(ocumNvmfFcLifMbpsIncident) | 意外事件 | 接口  | 批判的 |
| NVMf FC 网络接口 MB/s 警告阈值超出<br>(ocumNvmfFcLifMbpsWarning)  | 风险   | 接口  | 警告  |

## LUN 事件

LUN 事件为您提供有关 LUN 状态的信息，以便您可以监控潜在问题。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。

影响区域：可用性

星号 (\*) 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 | 批判的 |
| LUN 已销毁*(lunDestroy)                                   | 事件   | LUN | 信息  |
| LUN 映射了 igroup 中不受支持的操作系统<br>(igroupUnsupportedOsType) | 意外事件 | LUN | 警告  |
| 访问 LUN 的单一活动路径<br>(ocumEvtLunSingleActivePath)         | 风险   | LUN | 警告  |
| 没有访问 LUN 的活动路径<br>(ocumEvtLunNotReachable)             | 意外事件 | LUN | 批判的 |

| 事件名称（陷阱名称）                                                 | 影响级别 | 源类型 | 严重性 |
|------------------------------------------------------------|------|-----|-----|
| 没有访问 LUN 的优化路径<br>(ocumEvtLunOptimizedPathInactive)        | 风险   | LUN | 警告  |
| 没有从 HA 合作伙伴访问 LUN 的路径<br>(ocumEvtLunHaPathInactive)        | 风险   | LUN | 警告  |
| 没有从 HA 对中的一个节点访问 LUN 的路径<br>(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 快照复制空间不足<br>(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 |
|--------------------------------------------------------|------|-----|-----|
| LUN 映射了 igroup 中不受支持的操作系统<br>(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 |
|-------------------------------------------|------|-----|-----|
| LUN IOPS 临界阈值被突破<br>(ocumLunIopsIncident) | 意外事件 | LUN | 批判的 |
| LUN IOPS 警告阈值超出<br>(ocumLunIopsWarning)   | 风险   | LUN | 警告  |
| LUN MB/s 临界阈值超出<br>(ocumLunMbpsIncident)  | 意外事件 | LUN | 批判的 |



| 事件名称（陷阱名称）                                                                      | 影响级别 | 源类型 | 严重性 |
|---------------------------------------------------------------------------------|------|-----|-----|
| 超出 LUN MB/s 警告阈值<br>(ocumLunMbpsWarning)                                        | 风险   | LUN | 警告  |
| LUN 延迟 ms/op 临界阈值<br>超出<br>(ocumLunLatencyIncident)                             | 意外事件 | LUN | 批判的 |
| LUN 延迟 ms/op 警告阈值<br>已超出<br>(ocumLunLatencyWarning)                             | 风险   | LUN | 警告  |
| LUN 延迟和 IOPS 临界阈<br>值被突破<br>(ocumLunLatencyIopsIncident)                        | 意外事件 | LUN | 批判的 |
| LUN 延迟和 IOPS 警告阈<br>值超出<br>(ocumLunLatencyIopsWarning)                          | 风险   | LUN | 警告  |
| LUN 延迟和 MB/s 临界阈<br>值被突破<br>(ocumLunLatencyMbpsIncident)                        | 意外事件 | LUN | 批判的 |
| 超出 LUN 延迟和 MB/s 警<br>告阈值<br>(ocumLunLatencyMbpsWarning)                         | 风险   | LUN | 警告  |
| LUN 延迟和聚合性能容量<br>使用临界阈值被突破<br>(ocumLunLatencyAggregatePerfCapacityUsedIncident) | 意外事件 | LUN | 批判的 |
| LUN 延迟和聚合性能容量<br>使用警告阈值已突破<br>(ocumLunLatencyAggregatePerfCapacityUsedWarning)  | 风险   | LUN | 警告  |

| 事件名称（陷阱名称）                                                                              | 影响级别 | 源类型 | 严重性 |
|-----------------------------------------------------------------------------------------|------|-----|-----|
| LUN 延迟和聚合利用率临界阈值被突破<br>(ocumLunLatencyAggregateUtilizationIncident)                     | 意外事件 | LUN | 批判的 |
| LUN 延迟和聚合利用率警告阈值超出<br>(ocumLunLatencyAggregateUtilizationWarning)                       | 风险   | LUN | 警告  |
| LUN 延迟和节点性能容量使用临界阈值被突破<br>(ocumLunLatencyNodePerfCapacityUsedIncident)                  | 意外事件 | LUN | 批判的 |
| LUN 延迟和节点性能容量使用警告阈值已突破<br>(ocumLunLatencyNodePerfCapacityUsedWarning)                   | 风险   | LUN | 警告  |
| LUN 延迟和已用节点性能容量 - 超出接管临界阈值<br>(ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident) | 意外事件 | LUN | 批判的 |
| LUN 延迟和已用节点性能容量 - 超出接管警告阈值<br>(ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)  | 风险   | LUN | 警告  |
| LUN 延迟和节点利用率临界阈值被突破<br>(ocumLunLatencyNodeUtilizationIncident)                          | 意外事件 | LUN | 批判的 |
| LUN 延迟和节点利用率警告阈值超出<br>(ocumLunLatencyNodeUtilizationWarning)                            | 风险   | LUN | 警告  |
| QoS LUN 最大 IOPS 警告阈值超出<br>(ocumQosLunMaxIopsWarning)                                    | 风险   | LUN | 警告  |

| 事件名称（陷阱名称）                                                       | 影响级别 | 源类型 | 严重性 |
|------------------------------------------------------------------|------|-----|-----|
| QoS LUN 最大 MB/s 警告<br>阈值超出<br>(ocumQosLunMaxMbpsWarning)         | 风险   | LUN | 警告  |
| 工作负载 LUN 延迟阈值超出性能服务级别策略所定义的范围<br>(ocumConformanceLatencyWarning) | 风险   | LUN | 警告  |

#### 管理工作站事件

管理站事件为您提供有关安装 Unified Manager 的服务器状态的信息，以便您监控潜在问题。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。

#### 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几乎已满<br>(ocumEvtUnifiedManagerDiskSpaceNearlyFull) | 风险   | 管理站 | 警告  |
| 管理服务器磁盘空间已满<br>(ocumEvtUnifiedManagerDiskSpaceFull)         | 意外事件 | 管理站 | 批判的 |
| 管理服务器内存不足<br>(ocumEvtUnifiedManagerMemoryLow)               | 风险   | 管理站 | 警告  |
| 管理服务器内存即将耗尽<br>(ocumEvtUnifiedManagerMemoryAlmostOut)       | 意外事件 | 管理站 | 批判的 |
| MySQL 日志文件大小增加；需要重新启动<br>(ocumEvtMysqlLogFileSizeWarning)   | 意外事件 | 管理站 | 警告  |
| 总审计日志大小分配即将满                                                | 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 |
|------------------|------|-----|-----|
| 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  |
| 审计日志文件被篡改        | 风险   | 管理站 | 警告  |
| 审计日志文件已删除        | 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 |
|------------------------------------------------------------|------|-----|-----|
| 性能数据分析受到影响<br>(ocumEvtUnifiedManagerDataMissingAnalyze)    | 风险   | 管理站 | 警告  |
| 性能数据收集受到影响<br>(ocumEvtUnifiedManagerDataMissingCollection) | 意外事件 | 管理站 | 批判的 |



最后两个性能事件仅适用于 Unified Manager 7.2。如果其中任何一个事件处于“新”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。

## MetroCluster 网桥事件

MetroCluster Bridge 事件为您提供有关网桥状态的信息，以便您可以监控 FC 配置上的 MetroCluster 中的潜在问题。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。

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 |
|------------------------------------|------|-----------------|-----|
| 桥不可达<br>(ocumEvtBridgeUnreachable) | 意外事件 | MetroCluster 桥接 | 批判的 |

| 事件名称（陷阱名称）                             | 影响级别 | 源类型             | 严重性 |
|----------------------------------------|------|-----------------|-----|
| 桥温异常(ocumEvtBridgeTemperatureAbnormal) | 意外事件 | MetroCluster 桥接 | 批判的 |

### MetroCluster 连接事件

连接事件为您提供有关集群组件之间以及MetroCluster over FC 和MetroCluster over IP 配置中的集群之间的连接的信息，以便您可以监控潜在问题。事件按影响区域进行分组，并提供事件和陷阱名称、影响级别、源类型和严重性。

两种配置中常见的事件

这些连接事件对于MetroCluster over FC 和MetroCluster over IP 配置都很常见。

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合作伙伴之间的所有链路均已关闭(ocumEvtMetroClusterAllLinksBetweenPartnersDown)           | 意外事件 | MetroCluster 关系 | 批判的 |
| MetroCluster合作伙伴无法通过对等网络访问(ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork) | 意外事件 | MetroCluster 关系 | 批判的 |
| MetroCluster灾难恢复能力受到影响(ocumEvtMetroClusterDRStatusImpacted)                           | 风险   | MetroCluster 关系 | 批判的 |
| MetroCluster配置已切换(ocumEvtMetroClusterDRStatusImpacted)                                | 风险   | MetroCluster 关系 | 警告  |

### 基于 FC 的MetroCluster配置

这些事件与 FC 配置上的MetroCluster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 |
|--------------------------------------------------------------------------|------|----------------------|-----|
| 所有交换机间链路均断开<br>(ocumEvtMetroClusterAllISLBetweenSwitchesDown)            | 意外事件 | MetroCluster 交换机间连接  | 批判的 |
| FC-SAS 桥接至存储堆栈链路关闭<br>(ocumEvtBridgeSasPortDown)                         | 意外事件 | MetroCluster 网桥堆栈连接  | 批判的 |
| MetroCluster配置部分切换<br>(ocumEvtMetroClusterDRStatusPartiallyImpacted)     | 风险   | MetroCluster 关系      | 错误  |
| 节点到 FC 交换机所有 FC-VI 互连链路关闭<br>(ocumEvtMccNodeSwitchFcviLinksDown)         | 意外事件 | MetroCluster 节点交换机连接 | 批判的 |
| 节点到 FC 交换机一个或多个 FC 发起方链路断开<br>(ocumEvtMccNodeSwitchFcLinksOneOrMoreDown) | 风险   | MetroCluster 节点交换机连接 | 警告  |
| 节点到 FC 切换所有 FC 发起方链路关闭<br>(ocumEvtMccNodeSwitchFcLinksDown)              | 意外事件 | MetroCluster 节点交换机连接 | 批判的 |
| 切换到 FC-SAS 桥接器 FC 链路关闭<br>(ocumEvtMccSwitchBridgeFcLinksDown)            | 意外事件 | MetroCluster 交换机网桥连接 | 批判的 |
| 节点间所有 FC VI 互连链路均已关闭<br>(ocumEvtMccInterNodeLinksDown)                   | 意外事件 | 节点间连接                | 批判的 |
| 节点间一个或多个 FC VI 互连链路断开<br>(ocumEvtMccInterNodeLinksOneOrMoreDown)         | 风险   | 节点间连接                | 警告  |

| 事件名称（陷阱名称）                                                        | 影响级别 | 源类型    | 严重性 |
|-------------------------------------------------------------------|------|--------|-----|
| 节点到桥接链路断开<br>(ocumEvtMccNodeBridgeLinksDown)                      | 意外事件 | 节点网桥连接 | 批判的 |
| 节点到存储堆栈所有 SAS 链接均关闭 (<br>ocumEvtMccNodeStackLinksDown)            | 意外事件 | 节点堆栈连接 | 批判的 |
| 节点到存储堆栈一个或多个 SAS 链接断开 (<br>ocumEvtMccNodeStackLinksOneOrMoreDown) | 风险   | 节点堆栈连接 | 警告  |

#### MetroCluster over IP 配置

这些事件与MetroCluster over IP 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 |
|--------------------------------------------------------------------|------|-----------------|-----|
| MetroCluster IP 站点间连接状态已关闭<br>(mccIntersiteconnectivityStatusDown) | 风险   | MetroCluster 关系 | 批判的 |
| MetroCluster-IP 节点到交换机的连接脱机<br>(mcclpPortStatusOffline)            | 风险   | 节点              | 错误  |

#### MetroCluster交换机事件

MetroCluster over FC 配置的MetroCluster交换机事件为您提供有关MetroCluster交换机状态的信息，以便您可以监控潜在问题。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。

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 |
|------------------------------------------|------|------------------|-----|
| 开关温度异常(ocumEvtSwitchTemperatureAbnormal) | 意外事件 | MetroCluster 交换机 | 批判的 |

| 事件名称（陷阱名称）                                                                                                                                                                                         | 影响级别 | 源类型              | 严重性 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------------------|-----|
| 交换机不可达<br>(ocumEvtSwitchUnreachable)                                                                                                                                                               | 意外事件 | MetroCluster 交换机 | 批判的 |
| 交换机风扇故障<br>(ocumEvtSwitchFansOneOrMoreFailed)                                                                                                                                                      | 意外事件 | MetroCluster 交换机 | 批判的 |
| 开关电源故障<br>(ocumEvtSwitchPowerSuppliesOneOrMoreFailed)                                                                                                                                              | 意外事件 | MetroCluster 交换机 | 批判的 |
| <div>  <div>           此事件仅适用于Cisco交换机。         </div> </div> 开关温度传感器故障<br>(ocumEvtSwitchTemperatureSensorFailed) | 意外事件 | MetroCluster 交换机 | 批判的 |

## NVMe 命名空间事件

NVMe 命名空间事件为您提供有关命名空间状态的信息，以便您可以监控潜在问题。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 (\*) 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<br>*(nvmeNamespaceStatusOffline)     | 事件   | 命名空间 | 信息  |
| NVMeNS 在线<br>*(nvmeNamespaceStatusOnline)      | 事件   | 命名空间 | 信息  |
| NVMeNS 空间不足<br>*(nvmeNamespaceSpaceOutOfSpace) | 风险   | 命名空间 | 警告  |



| 事件名称（陷阱名称）                           | 影响级别 | 源类型  | 严重性 |
|--------------------------------------|------|------|-----|
| NVMeNS 销毁<br>*(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 临界阈值被突破<br>(ocumNvmeNamespaceIopsIncident)           | 意外事件 | 命名空间 | 批判的 |
| NVMe 命名空间 IOPS 警告阈值已超出<br>(ocumNvmeNamespaceIopsWarning)            | 风险   | 命名空间 | 警告  |
| NVMe 命名空间 MB/s 临界阈值被突破<br>(ocumNvmeNamespaceMbpsIncident)           | 意外事件 | 命名空间 | 批判的 |
| 超出 NVMe 命名空间 MB/s 警告阈值<br>(ocumNvmeNamespaceMbpsWarning)            | 风险   | 命名空间 | 警告  |
| NVMe 命名空间延迟 ms/op 临界阈值突破<br>(ocumNvmeNamespaceLatencyIncident)      | 意外事件 | 命名空间 | 批判的 |
| NVMe 命名空间延迟 ms/op 警告阈值已超出<br>(ocumNvmeNamespaceLatencyWarning)      | 风险   | 命名空间 | 警告  |
| NVMe 命名空间延迟和 IOPS 临界阈值被突破<br>(ocumNvmeNamespaceLatencyIopsIncident) | 意外事件 | 命名空间 | 批判的 |
| NVMe 命名空间延迟和 IOPS 警告阈值超出<br>(ocumNvmeNamespaceLatencyIopsWarning)   | 风险   | 命名空间 | 警告  |

| 事件名称（陷阱名称）                                                          | 影响级别 | 源类型  | 严重性 |
|---------------------------------------------------------------------|------|------|-----|
| NVMe 命名空间延迟和 MB/s 临界阈值被突破<br>(ocumNvmeNamespaceLatencyMbpsIncident) | 意外事件 | 命名空间 | 批判的 |
| 超出 NVMe 命名空间延迟和 MB/s 警告阈值<br>(ocumNvmeNamespaceLatencyMbpsWarning)  | 风险   | 命名空间 | 警告  |

## 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 (\*) 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 |
|-------------------------------------------------------------|------|-----|-----|
| 节点根卷空间几乎已满<br>(ocumEvtClusterNodeRootVolumeSpaceNearlyFull) | 风险   | 节点  | 警告  |
| 云 AWS MetadataConnFail<br>*(ocumCloudAwsMetadataConnFail)   | 风险   | 节点  | 错误  |
| 云 AWS IAMCredsExpired<br>*(ocumCloudAwsIamCredsExpired)     | 风险   | 节点  | 错误  |
| 云 AWS IAMCredsInvalid<br>*(ocumCloudAwsIamCredsInvalid)     | 风险   | 节点  | 错误  |
| 云 AWS IAMCredsNotFound<br>*(ocumCloudAwsIamCredsNotFound)   | 风险   | 节点  | 错误  |

| 事件名称（陷阱名称）                                                            | 影响级别 | 源类型 | 严重性 |
|-----------------------------------------------------------------------|------|-----|-----|
| 云 AWS IAMCredsNotInitialized<br>*(ocumCloudAwsIamCredsNotInitialized) | 事件   | 节点  | 信息  |
| 云 AWS IAMRoleInvalid<br>*(ocumCloudAwsIamRoleInvalid)                 | 风险   | 节点  | 错误  |
| 云 AWS IAMRoleNotFound<br>*(ocumCloudAwsIamRoleNotFound)               | 风险   | 节点  | 错误  |
| 云层主机无法解析<br>*(ocumObjstoreHostUnresolvable)                           | 风险   | 节点  | 错误  |
| 云层集群间网络接口关闭<br>*(ocumObjstoreInterClusterLifDown)                     | 风险   | 节点  | 错误  |
| 其中一个 NFSv4 池已耗尽<br>*(nbladeNfsv4PoolExhaust)                          | 意外事件 | 节点  | 批判的 |
| 请求不匹配云层签名*<br>(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 监视器内存最大值<br>*(ocumQosMonitorMemoryMaxed) | 风险   | 节点  | 错误  |
| QoS 监控内存减少<br>*(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 |
|-------------------------------------------------------------------|------|-----|-----|
| 节点 IOPS 临界阈值被突破<br>(ocumNodeIopsIncident)                         | 意外事件 | 节点  | 批判的 |
| 节点 IOPS 警告阈值超出<br>(ocumNodeIopsWarning)                           | 风险   | 节点  | 警告  |
| 节点 MB/s 临界阈值突破<br>(ocumNodeMbpsIncident)                          | 意外事件 | 节点  | 批判的 |
| 节点 MB/s 警告阈值超出<br>(ocumNodeMbpsWarning)                           | 风险   | 节点  | 警告  |
| 节点延迟 ms/op 临界阈值突破<br>(ocumNodeLatencyIncident)                    | 意外事件 | 节点  | 批判的 |
| 节点延迟 ms/op 警告阈值超出<br>(ocumNodeLatencyWarning)                     | 风险   | 节点  | 警告  |
| 节点性能容量使用临界阈值已突破<br>(ocumNodePerfCapacityUsedIncident)             | 意外事件 | 节点  | 批判的 |
| 节点性能容量使用警告阈值超出<br>(ocumNodePerfCapacityUsedWarning)               | 风险   | 节点  | 警告  |
| 已用节点性能容量 - 超出接管临界阈值<br>(ocumNodePerfCapacityUsedTakeoverIncident) | 意外事件 | 节点  | 批判的 |

| 事件名称（陷阱名称）                                                       | 影响级别 | 源类型 | 严重性 |
|------------------------------------------------------------------|------|-----|-----|
| 已用节点性能容量 - 超出接管警告阈值<br>(ocumNodePerfCapacityUsedTakeoverWarning) | 风险   | 节点  | 警告  |
| 节点利用率临界阈值被突破<br>(ocumNodeUtilizationIncident)                    | 意外事件 | 节点  | 批判的 |
| 节点利用率警告阈值超出<br>(ocumNodeUtilizationWarning)                      | 风险   | 节点  | 警告  |
| 节点 HA 对过度利用阈值被突破<br>(ocumNodeHaPairOverUtilizedInformation)      | 事件   | 节点  | 信息  |
| 节点磁盘碎片阈值超出<br>(ocumNodeDiskFragmentationWarning)                 | 风险   | 节点  | 警告  |
| 性能容量使用阈值超出<br>(ocumNodeOverUtilizedWarning)                      | 风险   | 节点  | 警告  |
| 节点动态阈值被突破<br>(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- <i>&lt;advisory ID&gt;</i> (ocumx) | 风险   | 节点  | 批判的 |

## NVRAM 电池事件

NVRAM 电池事件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。

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<br>(ocumEvtNvramBatteryLow)          | 风险   | 节点  | 警告  |
| NVRAM电池放电(ocumEvtNvramBatteryDischarged)        | 风险   | 节点  | 错误  |
| NVRAM电池过度充电<br>(ocumEvtNvramBatteryOverCharged) | 意外事件 | 节点  | 批判的 |

#### 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变化或问题，例如端口是否关闭。

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 |
|-----------------------------------|------|-----|-----|
| 端口状态关闭<br>(ocumEvtPortStatusDown) | 意外事件 | 节点  | 批判的 |

影响区域：性能

| 事件名称（陷阱名称）                                        | 影响级别 | 源类型 | 严重性 |
|---------------------------------------------------|------|-----|-----|
| 网络端口 MB/s 临界阈值突破<br>(ocumNetworkPortMbpsIncident) | 意外事件 | 端口  | 批判的 |
| 网络端口 MB/s 警告阈值超出<br>(ocumNetworkPortMbpsWarning)  | 风险   | 端口  | 警告  |
| FCP 端口 MB/s 临界阈值突破<br>(ocumFcpPortMbpsIncident)   | 意外事件 | 端口  | 批判的 |

| 事件名称（陷阱名称）                                             | 影响级别 | 源类型 | 严重性 |
|--------------------------------------------------------|------|-----|-----|
| FCP 端口 MB/s 警告阈值超出<br>(ocumFcpPortMbpsWarning)         | 风险   | 端口  | 警告  |
| 网络端口利用率临界阈值被突破<br>(ocumNetworkPortUtilizationIncident) | 意外事件 | 端口  | 批判的 |
| 网络端口利用率警告阈值超出<br>(ocumNetworkPortUtilizationWarning)   | 风险   | 端口  | 警告  |
| FCP 端口利用率临界阈值被突破<br>(ocumFcpPortUtilizationIncident)   | 意外事件 | 端口  | 批判的 |
| FCP 端口利用率警告阈值超出<br>(ocumFcpPortUtilizationWarning)     | 风险   | 端口  | 警告  |

## 电源事件

电源事件为您提供有关硬件状态的信息，以便您可以监控潜在问题。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。

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 |
|------------------------------------------------|------|-----|-----|
| 一个或多个电源发生故障(ocumEvtPowerSupplyOneOrMoreFailed) | 意外事件 | 节点  | 批判的 |

## 保护事件

保护事件会告诉您作业是否失败或中止，以便您可以监控问题。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。

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<br>(ocumEvtProtectionJobTaskFailed) | 意外事件 | 卷或存储服务 | 批判的 |
| 保护作业已中止<br>(ocumEvtProtectionJobAborted)   | 风险   | 卷或存储服务 | 警告  |

## 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。

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 空间几乎已满(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 | 批判的 |
| 超出 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 | 批判的 |
| 超出 Qtree 空间软限制(ocumEvtQtreeSpaceSoftLimitBreached) | 风险   | qtree | 警告  |



## 服务处理器事件

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。

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<br>(ocumEvtServiceProcessorNotConfigured) | 风险   | 节点  | 警告  |
| 服务处理器离线<br>(ocumEvtServiceProcessorOffline)        | 风险   | 节点  | 错误  |

## SnapMirror 关系事件

SnapMirror 关系事件可以为您提供有关异步和同步 SnapMirror 关系的状态的信息，您可以监控这些信息以确定是否存在潜在问题。存储虚拟机和卷都会生成异步 SnapMirror 关系事件，但仅为卷关系生成同步 SnapMirror 关系事件。对于作为存储虚拟机灾难恢复关系一部分的组成卷，不会生成任何事件。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。

影响区域：保护

星号 (\*) 标识已转换为 Unified Manager 事件的 EMS 事件。



SnapMirror 关系事件是针对受存储虚拟机灾难恢复保护的存储虚拟机生成的，但不针对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 |
|--------------------------------------------------------------|------|---------------|-----|
| 镜像复制不健康<br>(ocumEvtSnapmirrorRelationshipUnhealthy)          | 风险   | SnapMirror 关系 | 警告  |
| 镜像复制中断<br>(ocumEvtSnapmirrorRelationshipStateBrokenoff)      | 风险   | SnapMirror 关系 | 错误  |
| 镜像复制初始化失败<br>(ocumEvtSnapmirrorRelationshipInitializeFailed) | 风险   | SnapMirror 关系 | 错误  |

| 事件名称（陷阱名称）                                                       | 影响级别 | 源类型           | 严重性 |
|------------------------------------------------------------------|------|---------------|-----|
| 镜像复制更新失败<br>(ocumEvtSnapmirrorRelationshipUpdateFailed)          | 风险   | SnapMirror 关系 | 错误  |
| 镜像复制滞后错误<br>(ocumEvtSnapMirrorRelationshipLagError)              | 风险   | SnapMirror 关系 | 错误  |
| 镜像复制滞后警告<br>(ocumEvtSnapMirrorRelationshipLagWarning)            | 风险   | SnapMirror 关系 | 警告  |
| 镜像复制重新同步失败<br>(ocumEvtSnapmirrorRelationshipResyncFailed)        | 风险   | SnapMirror 关系 | 错误  |
| 同步复制不同步<br>*(syncSnapmirrorRelationshipOutofsync)                | 风险   | SnapMirror 关系 | 警告  |
| 同步复制已恢复*<br>(syncSnapmirrorRelationshipInSync)                   | 事件   | SnapMirror 关系 | 信息  |
| 同步复制自动重新同步失败*<br>(syncSnapmirrorRelationshipAutoSyncRetryFailed) | 风险   | SnapMirror 关系 | 错误  |
| 在集群上添加了 ONTAP 调解器<br>(SnapmirrorMediatorAdded)                   | 事件   | 集群            | 信息  |
| ONTAP 调解器已从集群中删除<br>(snapmirrorMediatorRemoved)                  | 事件   | 集群            | 信息  |
| 无法从集群访问 ONTAP 调解器<br>(SnapmirrorMediatorUnreachable)             | 风险   | 调解器           | 警告  |

| 事件名称（陷阱名称）                                                                | 影响级别 | 源类型 | 严重性 |
|---------------------------------------------------------------------------|------|-----|-----|
| 无法从集群访问 ONTAP 调解器<br>(SnapmirrorMediatorMisconfigured)                    | 风险   | 调解器 | 错误  |
| ONTAP 调解器连接已重新建立、重新同步并准备好进行SnapMirror主动同步<br>(snapmirrorMediatorInQuorum) | 事件   | 调解器 | 信息  |

#### 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。卷和存储虚拟机保护关系均支持异步镜像和保险库关系事件。但存储虚拟机灾难恢复仅不支持 Vault 关系。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。

影响区域：保护



还会为受存储虚拟机灾难恢复保护的存储虚拟机生成SnapMirror和 Vault 关系事件，但不会为任何组成对象关系生成事件。

| 事件名称（陷阱名称）                                                            | 影响级别 | 源类型           | 严重性 |
|-----------------------------------------------------------------------|------|---------------|-----|
| 异步镜像和保险库不健康<br>(ocumEvtMirrorVaultRelationshipUnhealthy)              | 风险   | SnapMirror 关系 | 警告  |
| 异步镜像和保险库断开<br>(ocumEvtMirrorVaultRelationshipStateBrokenoff)          | 风险   | SnapMirror 关系 | 错误  |
| 异步镜像和 Vault 初始化失败<br>(ocumEvtMirrorVaultRelationshipInitializeFailed) | 风险   | SnapMirror 关系 | 错误  |
| 异步镜像和 Vault 更新失败<br>(ocumEvtMirrorVaultRelationshipUpdateFailed)      | 风险   | SnapMirror 关系 | 错误  |

| 事件名称（陷阱名称）                                                         | 影响级别 | 源类型           | 严重性 |
|--------------------------------------------------------------------|------|---------------|-----|
| 异步镜像和 Vault 滞后错误<br>(ocumEvtMirrorVaultRelationshipLagError)       | 风险   | SnapMirror 关系 | 错误  |
| 异步镜像和 Vault 滞后警告<br>(ocumEvtMirrorVaultRelationshipLagWarning)     | 风险   | SnapMirror 关系 | 警告  |
| 异步镜像和 Vault 重新同步失败<br>(ocumEvtMirrorVaultRelationshipResyncFailed) | 风险   | SnapMirror 关系 | 错误  |



Active IQ 门户（Config Advisor）引发“SnapMirror 更新失败”事件。

## Snapshot 事件

快照事件提供有关快照状态的信息，使您能够监视快照中是否存在潜在问题。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

| 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  |

## SnapVault 关系事件

SnapVault 关系事件为您提供有关 SnapVault 关系状态的信息，以便您可以监控潜在问题。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。

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 不健康<br>(ocumEvtSnapVaultRelationshipUnhealthy)          | 风险   | SnapMirror 关系 | 警告  |
| 异步保险库断开<br>(ocumEvtSnapVaultRelationshipStateBrokenoff)          | 风险   | SnapMirror 关系 | 错误  |
| 异步 Vault 初始化失败<br>(ocumEvtSnapVaultRelationshipInitializeFailed) | 风险   | SnapMirror 关系 | 错误  |
| 异步 Vault 更新失败<br>(ocumEvtSnapVaultRelationshipUpdateFailed)      | 风险   | SnapMirror 关系 | 错误  |
| 异步 Vault 滞后错误<br>(ocumEvtSnapVaultRelationshipLagError)          | 风险   | SnapMirror 关系 | 错误  |
| 异步 Vault 滞后警告<br>(ocumEvtSnapVaultRelationshipLagWarning)        | 风险   | SnapMirror 关系 | 警告  |
| 异步 Vault 重新同步失败<br>(ocumEvtSnapvaultRelationshipResyncFailed)    | 风险   | SnapMirror 关系 | 错误  |

#### 存储故障转移设置事件

存储故障转移 (SFO) 设置事件为您提供有关存储故障转移是否被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。

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断开<br>(ocumEvtSfoInterconnectOneOrMoreLinksDown) | 风险   | 节点  | 警告  |
| 存储故障转移已禁用<br>(ocumEvtSfoSettingsDisabled)                       | 风险   | 节点  | 错误  |

| 事件名称（陷阱名称）                                          | 影响级别 | 源类型 | 严重性 |
|-----------------------------------------------------|------|-----|-----|
| 未配置存储故障转移<br>(ocumEvtSfoSettingsNot Configured)     | 风险   | 节点  | 错误  |
| 存储故障转移状态 - 接管<br>(ocumEvtSfoStateTakeover)          | 风险   | 节点  | 警告  |
| 存储故障转移状态 - 部分交还<br>(ocumEvtSfoStatePartialGiveback) | 风险   | 节点  | 错误  |
| 存储故障转移节点状态关闭<br>(ocumEvtSfoNodeStatusDown)          | 风险   | 节点  | 错误  |
| 存储故障转移接管不可能<br>(ocumEvtSfoTakeoverNotPossible)      | 风险   | 节点  | 错误  |

#### 存储服务事件

存储服务事件为您提供有关存储服务的创建和订阅的信息，以便您可以监控潜在问题。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。

##### 影响区域：配置

| 事件名称（陷阱名称）   | 影响级别 | 源类型  | 严重性 |
|--------------|------|------|-----|
| 已创建存储服务（不适用） | 事件   | 存储服务 | 信息  |
| 已订购存储服务（不适用） | 事件   | 存储服务 | 信息  |
| 存储服务已取消（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 |
|----------------------------------------------------------------------------|------|------|-----|
| 意外删除托管SnapMirror关系<br>ocumEvtStorageServiceUnsupportedRelationshipDeletion | 风险   | 存储服务 | 警告  |
| 存储服务成员卷意外删除<br>(ocumEvtStorageServiceUnexpectedVolumeDeletion)             | 意外事件 | 存储服务 | 批判的 |

### 存储架事件

存储架事件会告诉您存储架是否有异常，以便您监控潜在问题。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。

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 |
|-------------------------------------------|------|-----|-----|
| 异常电压范围(ocumEvtShelfVoltageAbnormal)       | 风险   | 储物架 | 警告  |
| 异常电流范围(ocumEvtShelfCurrentAbnormal)       | 风险   | 储物架 | 警告  |
| 温度异常<br>(ocumEvtShelfTemperatureAbnormal) | 风险   | 储物架 | 警告  |

### 存储虚拟机事件

存储虚拟机 (SVM) 事件为您提供有关存储虚拟机 (SVM) 状态的信息，以便您监控潜在问题。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 (\*) 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 |
|----------------------------------------------------------|------|-----|-----|
| 存储虚拟机 CIFS 服务关闭<br>(ocumEvtVserverCifsServiceStatusDown) | 意外事件 | SVM | 批判的 |
| 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<br>*(nbladeCifsNoPrivShare)             | 意外事件 | SVM | 批判的 |
| 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  |
| 许多 CIFS 连接*(nbladeCifsManyAuths)                         | 风险   | SVM | 错误  |
| 超出最大 CIFS 连接数<br>*(nbladeCifsMaxOpenSameFile)            | 风险   | SVM | 错误  |
| 超出每个用户的最大 CIFS 连接数<br>*(nbladeCifsMaxSessPerUsrConn)     | 风险   | SVM | 错误  |
| SVM FC/FCoE 服务关闭<br>(ocumEvtVserverFcServiceStatusDown)  | 意外事件 | SVM | 批判的 |
| SVM iSCSI 服务关闭<br>(ocumEvtVserverIscsiServiceStatusDown) | 意外事件 | SVM | 批判的 |
| 存储虚拟机 NFS 服务关闭<br>(ocumEvtVserverNfsServiceStatusDown)   | 意外事件 | SVM | 批判的 |



| 事件名称（陷阱名称）                                        | 影响级别 | 源类型 | 严重性 |
|---------------------------------------------------|------|-----|-----|
| 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  |
| 存储虚拟机已停止<br>(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  |
| 没有用于病毒扫描的 AV 服务器连接*(nbladeVscanNoScannerConn)     | 意外事件 | SVM | 批判的 |
| 未注册 AV 服务器*(nbladeVscanNoRegdScanner)             | 风险   | SVM | 错误  |
| 无响应的 AV 服务器连接*(nbladeVscanConnInactive)           | 事件   | SVM | 信息  |
| 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 |
|-------------|------|-----|-----|
| 发现 SVM（不适用） | 事件   | SVM | 信息  |

| 事件名称（陷阱名称）    | 影响级别 | 源类型 | 严重性 |
|---------------|------|-----|-----|
| 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 临界阈值被突破<br>(ocumSvmIopsIncident) | 意外事件 | SVM | 批判的 |
| 超出 SVM IOPS 警告阈值<br>(ocumSvmIopsWarning)  | 风险   | SVM | 警告  |
| 超出 SVM MB/s 临界阈值<br>(ocumSvmMbpsIncident) | 意外事件 | SVM | 批判的 |
| 超出 SVM MB/s 警告阈值<br>(ocumSvmMbpsWarning)  | 风险   | SVM | 警告  |
| SVM 延迟临界阈值超出<br>(ocumSvmLatencyIncident)  | 意外事件 | SVM | 批判的 |
| 超出 SVM 延迟警告阈值<br>(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 |
|---------------------------------------------|------|-----|-----|
| 审计日志已禁用<br>(ocumVserverAuditLogDisabled)    | 风险   | SVM | 警告  |
| 登录横幅已禁用<br>(ocumVserverLoginBannerDisabled) | 风险   | SVM | 警告  |

| 事件名称（陷阱名称）                                              | 影响级别 | 源类型 | 严重性 |
|---------------------------------------------------------|------|-----|-----|
| SSH 使用不安全的密码<br>(ocumVserverSSHInsecure)                | 风险   | SVM | 警告  |
| 登录横幅已更改<br>(ocumVserverLoginBannerChanged)              | 风险   | SVM | 警告  |
| 存储虚拟机反勒索软件监控已禁用<br>(antiRansomwareSvmStateDisabled)     | 风险   | SVM | 警告  |
| 存储虚拟机反勒索软件监控已启用（学习模式）<br>(antiRansomwareSvmStateDryrun) | 事件   | SVM | 信息  |
| 适用于反勒索软件监控的存储虚拟机（学习模式）<br>(ocumEvtSvmArwCandidate)      | 事件   | SVM | 信息  |

#### 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。

影响区域：容量

| 事件名称（陷阱名称）                                                             | 影响级别 | 源类型    | 严重性 |
|------------------------------------------------------------------------|------|--------|-----|
| 超出用户或组配额磁盘空间软限制<br>(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached) | 风险   | 用户或组配额 | 警告  |
| 达到用户或组配额磁盘空间硬限制<br>(ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)  | 意外事件 | 用户或组配额 | 批判的 |

| 事件名称（陷阱名称）                                                             | 影响级别 | 源类型    | 严重性 |
|------------------------------------------------------------------------|------|--------|-----|
| 违反用户或组配额文件计数软限制<br>(ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached) | 风险   | 用户或组配额 | 警告  |
| 达到用户或组配额文件数硬限制<br>(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)   | 意外事件 | 用户或组配额 | 批判的 |

## 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。

星号 (\*) 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 |
|---------------------------------------------------|------|-----|-----|
| 音量限制<br>(ocumEvtVolumeRestricted)                 | 风险   | 卷   | 警告  |
| 卷离线<br>(ocumEvtVolumeOffline)                     | 意外事件 | 卷   | 批判的 |
| 卷部分可用<br>(ocumEvtVolumePartiallyAvailable)        | 风险   | 卷   | 错误  |
| 卷已卸载（不适用）                                         | 事件   | 卷   | 信息  |
| 已安装卷（不适用）                                         | 事件   | 卷   | 信息  |
| 卷已重新安装（不适用）                                       | 事件   | 卷   | 信息  |
| 卷连接路径非活动状态<br>(ocumEvtVolumeJunctionPathInactive) | 风险   | 卷   | 警告  |

| 事件名称（陷阱名称）         | 影响级别 | 源类型 | 严重性 |
|--------------------|------|-----|-----|
| 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 - 已禁用（不适用） | 事件   | 卷   | 信息  |
| 卷自动调整最大容量已修改（不适用）  | 事件   | 卷   | 信息  |
| 卷自动调整增量大小已修改（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 |
|-----------------------------------------------------|------|-----|-----|
| 精简配置卷空间风险<br>(ocumThinProvisionVolumeSpaceAtRisk)   | 风险   | 卷   | 警告  |
| 容量效率操作错误<br>(ocumEvtVolumeEfficiencyOperationError) | 风险   | 卷   | 错误  |
| 卷空间已满<br>(ocumEvtVolumeFull)                        | 风险   | 卷   | 错误  |
| 卷空间几乎已满<br>(ocumEvtVolumeNearlyFull)                | 风险   | 卷   | 警告  |
| 卷逻辑空间已满<br>(volumeLogicalSpaceFull)                 | 风险   | 卷   | 错误  |
| 卷逻辑空间几乎已满<br>(volumeLogicalSpaceNearlyFull)         | 风险   | 卷   | 警告  |
| 卷逻辑空间正常<br>(volumeLogicalSpaceAllOK)                | 事件   | 卷   | 信息  |

| 事件名称（陷阱名称）                                                       | 影响级别 | 源类型 | 严重性 |
|------------------------------------------------------------------|------|-----|-----|
| 卷快照保留空间已满<br>(ocumEvtSnapshotFull)                               | 风险   | 卷   | 警告  |
| 快照副本过多<br>(ocumEvtSnapshotTooMany)                               | 风险   | 卷   | 错误  |
| 卷 Qtree 配额过载(ocumEvtVolumeQtreeQuotaOvercommitted)               | 风险   | 卷   | 错误  |
| 卷 Qtree 配额几乎过量使用<br>(ocumEvtVolumeQtreeQuotaAlmostOvercommitted) | 风险   | 卷   | 警告  |
| 成交量增长率异常<br>(ocumEvtVolumeGrowthRateAbnormal)                    | 风险   | 卷   | 警告  |
| 交易量满之前的天数<br>(ocumEvtVolumeDaysUntilFullSoon)                    | 风险   | 卷   | 错误  |
| 卷空间保证已禁用（不适用）                                                    | 事件   | 卷   | 信息  |
| 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  |
| 卷快照预留天数直至满<br>(ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)    | 风险   | 卷   | 错误  |
| FlexGroup组成部分存在空间问题<br>*(flexGroupConstituentsHaveSpaceIssues)   | 风险   | 卷   | 错误  |

| 事件名称（陷阱名称）                                                              | 影响级别 | 源类型 | 严重性 |
|-------------------------------------------------------------------------|------|-----|-----|
| FlexGroup组成部分空间状态全部正常<br>*(flexGroupConstituentsSpaceStatusAllOK)       | 事件   | 卷   | 信息  |
| FlexGroup组成部分存在Inode 问题<br>*(flexGroupConstituentsHaveInodesIssues)     | 风险   | 卷   | 错误  |
| FlexGroup组成部分 Inode 状态全部正常<br>*(flexGroupConstituentsInodesStatusAllOK) | 事件   | 卷   | 信息  |
| WAFL卷自动调整大小失败 *(wafVolAutoSizeFail)                                     | 风险   | 卷   | 错误  |
| WAFL卷自动调整大小完成<br>*(wafVolAutoSizeDone)                                  | 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   | 批判的 |
| 卷存储效率异常<br>(ocumVolumeAbnormalStorageEfficiencyWarning)                 | 风险   | 卷   | 警告  |
| 卷快照预留未充分利用<br>(volumeSnapshotReserveUnderutilizedWarning)               | 事件   | 卷   | 警告  |
| 卷快照预留未充分利用<br>(volumeSnapshotReserveUnderutilizedCleared)               | 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  |

| 事件名称（陷阱名称） | 影响级别 | 源类型 | 严重性 |
|------------|------|-----|-----|
| 已发现卷（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 |
|---------------------------------------------------------------|------|-----|-----|
| QoS 卷最大 IOPS 警告阈值超出<br>(ocumQosVolumeMaxIopsWarning)          | 风险   | 卷   | 警告  |
| QoS 卷最大 MB/s 警告阈值超出<br>(ocumQosVolumeMaxMbpsWarning)          | 风险   | 卷   | 警告  |
| QoS 卷最大 IOPS/TB 警告阈值已超出<br>(ocumQosVolumeMaxIopsPerTbWarning) | 风险   | 卷   | 警告  |
| 工作负载卷延迟阈值超出性能服务级别策略所定义的范围<br>(ocumConformanceLatencyWarning)  | 风险   | 卷   | 警告  |
| 卷 IOPS 临界阈值被突破<br>(ocumVolumeIopsIncident)                    | 意外事件 | 卷   | 批判的 |
| 卷 IOPS 警告阈值超出<br>(ocumVolumeIopsWarning)                      | 风险   | 卷   | 警告  |
| 卷 MB/s 临界阈值突破<br>(ocumVolumeMbpsIncident)                     | 意外事件 | 卷   | 批判的 |
| 超出卷 MB/s 警告阈值<br>(ocumVolumeMbpsWarning)                      | 风险   | 卷   | 警告  |



| 事件名称（陷阱名称）                                                                  | 影响级别 | 源类型 | 严重性 |
|-----------------------------------------------------------------------------|------|-----|-----|
| 突破卷延迟临界阈值<br>(ocumVolumeLatencyIncident)                                    | 意外事件 | 卷   | 批判的 |
| 超出卷延迟警告阈值<br>(ocumVolumeLatencyWarning)                                     | 风险   | 卷   | 警告  |
| 卷缓存未命中率临界阈值被突破<br>(ocumVolumeCacheMissRatioIncident)                        | 意外事件 | 卷   | 批判的 |
| 卷缓存未命中率警告阈值已超出<br>(ocumVolumeCacheMissRatioWarning)                         | 风险   | 卷   | 警告  |
| 卷延迟和 IOPS 临界阈值被突破<br>(ocumVolumeLatencyIopsIncident)                        | 意外事件 | 卷   | 批判的 |
| 卷延迟和 IOPS 警告阈值超出<br>(ocumVolumeLatencyIopsWarning)                          | 风险   | 卷   | 警告  |
| 卷延迟和 MB/s 临界阈值被突破<br>(ocumVolumeLatencyMbpsIncident)                        | 意外事件 | 卷   | 批判的 |
| 超出卷延迟和 MB/s 警告阈值<br>(ocumVolumeLatencyMbpsWarning)                          | 风险   | 卷   | 警告  |
| 卷延迟和聚合性能容量使用临界阈值被突破<br>(ocumVolumeLatencyAggregatePerfCapacityUsedIncident) | 意外事件 | 卷   | 批判的 |

| 事件名称（陷阱名称）                                                                                | 影响级别 | 源类型 | 严重性 |
|-------------------------------------------------------------------------------------------|------|-----|-----|
| 卷延迟和聚合性能容量使用警告阈值已突破<br>(ocumVolumeLatencyAggregatePerfCapacityUsedWarning)                | 风险   | 卷   | 警告  |
| 卷延迟和聚合利用率临界阈值被突破<br>(ocumVolumeLatencyAggregateUtilizationIncident)                       | 意外事件 | 卷   | 批判的 |
| 卷延迟和聚合利用率警告阈值超出<br>(ocumVolumeLatencyAggregateUtilizationWarning)                         | 风险   | 卷   | 警告  |
| 卷延迟和节点性能容量使用临界阈值突破<br>(ocumVolumeLatencyNodePerfCapacityUsedIncident)                     | 意外事件 | 卷   | 批判的 |
| 卷延迟和节点性能容量使用警告阈值已突破<br>(ocumVolumeLatencyNodePerfCapacityUsedWarning)                     | 风险   | 卷   | 警告  |
| 已使用的卷延迟和节点性能容量 - 超出接管临界阈值<br>(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident) | 意外事件 | 卷   | 批判的 |
| 卷延迟和节点性能容量使用情况 - 超出接管警告阈值<br>(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)  | 风险   | 卷   | 警告  |
| 卷延迟和节点利用率临界阈值被突破<br>(ocumVolumeLatencyNodeUtilizationIncident)                            | 意外事件 | 卷   | 批判的 |

| 事件名称（陷阱名称）                                                       | 影响级别 | 源类型 | 严重性 |
|------------------------------------------------------------------|------|-----|-----|
| 卷延迟和节点利用率警告<br>阈值超出<br>(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 |
|---------------------------------------------------------------|------|-----|-----|
| 容量反勒索软件监控已启用（主动模式）<br>(antiRansomwareVolumeStateEnabled)      | 事件   | 卷   | 信息  |
| 批量反勒索软件监控已禁用<br>(antiRansomwareVolumeStateDisabled)           | 风险   | 卷   | 警告  |
| 容量反勒索软件监控已启用（学习模式）<br>(antiRansomwareVolumeStateDryrun)       | 事件   | 卷   | 信息  |
| 批量反勒索软件监控已暂停（学习模式）<br>(antiRansomwareVolumeStateDryrunPaused) | 风险   | 卷   | 警告  |
| 批量反勒索软件监控已暂停（活动模式）<br>(antiRansomwareVolumeStateEnablePaused) | 风险   | 卷   | 警告  |
| 批量反勒索软件监控正在禁用<br>(antiRansomwareVolumeStateDisableInProgress) | 风险   | 卷   | 警告  |
| 发现勒索软件活动<br>(callHomeRansomwareActivitySeen)                  | 意外事件 | 卷   | 批判的 |

| 事件名称（陷阱名称）                                                              | 影响级别 | 源类型 | 严重性 |
|-------------------------------------------------------------------------|------|-----|-----|
| 适合反勒索软件监控的卷（学习模式）<br>(ocumEvtVolumeArwCandidate)                        | 事件   | 卷   | 信息  |
| 适合反勒索软件监控的卷（主动模式）<br>(ocumVolumeSuitedForActiveAntiRansomwareDetection) | 风险   | 卷   | 警告  |
| 音量显示嘈杂的反勒索软件警报<br>(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<br>(volumeLacksLocalProtectionWarning) | 风险   | 卷   | 警告  |
| 卷的本地快照保护不足<br>(volumeLacksLocalProtectionCleared) | 风险   | 卷   | 警告  |

## 卷移动状态事件

卷移动状态事件会告诉您卷移动的状态，以便您可以监控潜在问题。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。

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（不适用）                         | 事件   | 卷   | 信息  |
| 卷移动状态 - 失败<br>(ocumEvtVolumeMoveFailed) | 风险   | 卷   | 错误  |
| 卷移动状态：已完成（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 |
|--------------------------------------------------|------|-----|-----|
| 卷移动 - 切换延迟<br>(ocumEvtVolumeMoveCutoverDeferred) | 风险   | 卷   | 警告  |

## 事件窗口和对话框说明

事件会通知您环境中的任何问题。您可以使用事件管理库存页面和事件详细信息页面来监控所有事件。您可以使用通知设置选项对话框来配置通知。您可以使用事件设置页面来禁用或启用事件。

### 通知页面

您可以配置 Unified Manager 服务器，使其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

此区域使您能够配置以下警报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。共享时，此值还可用作报告的发件人地址。如果发件人地址预先填写了“[ActiveIQUnifiedManager@localhost.com](mailto:ActiveIQUnifiedManager@localhost.com)”，您应该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成功送达。

### SMTP 服务器

此区域使您能够配置以下 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，用于将警报通知发送给指定的收件人。

- 用户名

指定 SMTP 用户名。仅当 SMTP 服务器中启用 SMTPAUTH 时才需要 SMTP 用户名。

- 密码

指定 SMTP 密码。仅当 SMTP 服务器中启用 SMTPAUTH 时才需要 SMTP 用户名。

- 港口

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**

选中此框可使用 TLS/SSL 协议（也称为 start\_tls 和 StartTLS）在 SMTP 服务器和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

此区域使您能够配置以下 SNMP 陷阱设置：

- 版本

根据您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、带身份验证的版本 3 和带身份验证和加密的版本 3。默认值为版本 1。

- 陷阱目标主机

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）。要指定多个陷阱目标，请用逗号分隔每个主机。



列表中所有主机的所有其他 SNMP 设置（例如“版本”和“出站端口”）必须相同。

- 出站陷阱端口

指定 SNMP 服务器通过其接收管理服务器发送的陷阱的端口。

默认值为 162。

- 社区

访问主机的社区字符串。

- 引擎ID

指定 SNMP 代理的唯一标识符，由管理服务器自动生成。引擎 ID 适用于 SNMP 版本 3、带身份验证的 SNMP 版本 3 以及带身份验证和加密的 SNMP 版本 3。

- 用户名

指定 SNMP 用户名。用户名适用于 SNMP 版本 3、带身份验证的 SNMP 版本 3 以及带身份验证和加密的 SNMP 版本 3。

- 身份验证协议

指定用于验证用户的协议。协议选项包括 MD5 和 SHA。MD5 是默认值。身份验证协议适用于具有身份验证的 SNMP 版本 3 和具有身份验证和加密的 SNMP 版本 3。

- 认证密码

指定验证用户时使用的密码。带有身份验证的 SNMP 版本 3 和带有身份验证和加密的 SNMP 版本 3 均提供身份验证密码。

- 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。带有身份验证和加密功能的 SNMP 版本 3 提供隐私协议。

- 隐私密码

指定使用隐私协议时的密码。带有身份验证和加密功能的 SNMP 版本 3 提供隐私密码。

有关 SNMP 对象和陷阱的更多信息，您可以下载["Active IQ Unified ManagerMIB"](#)来自NetApp支持站点。

## 活动管理库存页面

事件管理库存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。

### 过滤器组件

使您能够自定义事件列表中显示的信息。您可以使用以下组件优化显示的事件列表：

- 查看菜单以从预定义的过滤器选择列表中进行选择。

这包括所有活动（新的和已确认的）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时段内生成的所有事件。

- 搜索窗格可通过输入完整或部分术语来优化事件列表。
- 过滤按钮可启动过滤器窗格，以便您可以从每个可用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

使您能够选择分配事件的用户。当您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，您可以通过该对话框将事件分配或重新分配给其他用户。您还可以通过将所有权字段留空来取消分配事件。

- 承认

确认选定的事件。

当您确认某个事件时，您的用户名和确认该事件的时间将添加到所选事件的事件列表中。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。

当您解决某个事件时，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，您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，您可以在此时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到逗号分隔值 (.csv) 文件或 PDF 文档。

- 显示/隐藏列选择器

使您能够选择页面上显示的列并选择它们的显示顺序。

## 事件列表

按触发时间排序显示所有事件的详细信息。

默认情况下，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

事件生成的时间。

- 严重性

事件严重性：严重 (❌)，错误 (⚠️)，警告 (⚠️) 和信息 (i)。

- 状态

事件状态：新的、已确认的、已解决的或已过时的。

- 影响程度

事件影响级别：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。

- 姓名

事件名称。您可以选择名称来显示该事件的事件详细信息页面。

- 来源

发生事件的对象的名称。您可以选择名称来显示该对象的健康状况或性能详细信息页面。

当发生共享 QoS 策略违规时，此字段中仅显示消耗最多 IOPS 或 MB/s 的工作负载对象。使用此策略的其他工作负载显示在事件详细信息页面中。

- 来源类型

与事件关联的对象类型（例如，存储虚拟机、卷或 Qtree）。

- 分配给

分配了事件的用户的姓名。

- 事件起源

事件是否源自“Active IQ门户”或直接源自“Active IQ Unified Manager”。

- 注释名称

分配给存储对象的注释的名称。

- 笔记

为事件添加的注释数。

- 未结清天数

自事件最初生成以来的天数。

- 指定时间

自事件分配给用户以来已经过去的时间。如果时间超过一周，则会显示将事件分配给用户的时间戳。

- 致谢

确认该事件的用户的姓名。如果事件未被确认，则该字段为空白。

- 确认时间

自事件被确认以来已经过去的时间。如果时间超过一周，则会显示确认事件的时间戳。

- 已解决

解决该事件的用户的姓名。如果事件尚未解决，则该字段为空白。

- 解决时间

自事件解决以来已经过去的时间。如果时间超过一周，则会显示事件解决的时间戳。

- 过时的时间

事件状态变为过时的时间。

## 事件详细信息页面

在事件详情页面中，您可以查看所选事件的详细信息，例如事件严重性、影响级别、影响区域和事件来源。您还可以查看有关解决问题的可能补救措施的其他信息。

- 活动名称

事件的名称以及最后看到该事件的时间。

对于非绩效事件，当事件处于“新”或“已确认”状态时，最后看到的信息是未知的，因此是隐藏的。

- 活动描述

事件的简要描述。

在某些情况下，事件描述中会提供触发事件的原因。

- 有争议的组件

对于动态性能事件，此部分显示代表集群的逻辑和物理组件的图标。如果某个组件存在争用，其图标将被圈出并以红色突出显示。

有关此处显示的组件的描述，请参阅\_集群组件以及它们为何会发生争用\_。

事件信息、系统诊断和建议的操作部分在其他主题中描述。

## 命令按钮

这些命令按钮可用来执行下列任务：

- 注释图标

使您能够添加或更新有关事件的注释，并查看其他用户留下的所有注释。

## 操作菜单

- 分配给我

将事件分配给您。

- 分配给其他人

打开“分配所有者”对话框，您可以将事件分配或重新分配给其他用户。

当您分配事件给用户时，用户的姓名和分配事件的时间将添加到所选事件的事件列表中。

您可以通过将所有权字段留空来取消分配事件。

- 承认

确认选定的事件，以便您不会继续收到重复的警报通知。

当您确认某个事件时，您的用户名和确认该事件的时间将添加到所选事件的事件列表（确认人）中。当您确认某个事件时，您就承担起管理该事件的责任。

- 标记为已解决

使您能够将事件状态更改为“已解决”。

当您解决某个事件时，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，您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，您可以在这里为选定事件添加警报。

#### Event Information 部分显示的内容

您可以使用“事件详细信息”页面上的“事件信息”部分查看有关选定事件的详细信息，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

事件生成的时间。

- 状态

事件状态：新的、已确认的、已解决的或已过时的。

- 过时的原因

导致事件过时的操作，例如问题已修复。

- 活动时长

对于活动（新的和已确认的）事件，这是检测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。

所有性能事件都会显示此字段，其他事件类型只有在解决或淘汰后才会显示。

- 最后露面

事件最后处于活跃状态的日期和时间。

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，因此该字段被隐藏。

- 严重性

事件严重性：严重 (❌)， 错误 (❗)， 警告 (⚠️) 和信息 (ℹ️)。

- 影响程度

事件影响级别：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。

- 来源

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，此字段中最多列出三个消耗最多 IOPS 或 MBps 的工作负载对象。

您可以单击源名称链接来显示该对象的健康状况或性能详细信息页面。

- 来源注释

显示与事件关联的对象的注释名称和值。

仅针对集群、SVM 和卷上的运行状况事件显示此字段。

- 源组

显示受影响对象所属的所有组的名称。

仅针对集群、SVM 和卷上的运行状况事件显示此字段。

- 来源类型

与事件关联的对象类型（例如，SVM、卷或 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健康状况或性能详细信息页面。

- 受影响对象数量

受事件影响的对象的数量。

您可以单击对象链接来显示库存页面，其中填充了当前受此事件影响的对象。

仅针对性能事件显示此字段。

- 受影响的卷

受此事件影响的卷的数量。

仅针对节点或聚合上的性能事件显示此字段。

- 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（分配空间或使用空间）。

仅针对性能事件显示此字段。

- 规则 ID

对于Active IQ平台事件，这是触发生成事件的规则的编号。

- 感谢

确认事件的人员的姓名以及确认事件的时间。

- 已解决

解决事件的人员的姓名以及解决事件的时间。

- 分配给

被指派负责该活动的人员的姓名。

- 警报设置

显示有关警报的以下信息：

- 如果没有与所选事件相关的警报，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。

- 如果有一个警报与选定事件关联，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。

- 如果有多个警报与选定事件关联，则会显示警报的数量。

您可以通过单击链接打开“警报设置”页面来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。

- 最后通知已发送

发送最新警报通知的日期和时间。

- 发送者

用于发送警报通知的机制：电子邮件或 SNMP 陷阱。

- 上一个脚本运行

生成警报时执行的脚本的名称。

#### 建议的操作部分显示的内容

事件详细信息页面的建议操作部分提供了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该事件。建议的操作是根据事件类型或已突破的阈值类型定制的。

此区域仅针对某些类型的事件显示。

在某些情况下，页面上会提供\*帮助\*链接，其中引用了许多建议操作的附加信息，包括执行特定操作的说明。某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。当可用时，这些分辨率将显示一个“修复”按钮。单击此按钮可让 Unified Manager 修复导致该事件的问题。

对于Active IQ平台事件，本部分可能包含指向NetApp知识库文章（如果有）的链接，其中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 会在本地打开；该 PDF 是您手动下载到 Unified Manager 实例的规则文件的一部分。

#### 系统诊断部分显示的内容

事件详细信息页面的系统诊断部分提供的信息可以帮助您诊断可能导致该事件的问题。

此区域仅针对某些事件显示。

一些性能事件提供与已触发的特定事件相关的图表。通常这包括 IOPS 或 MBps 图表和前十天的延迟图表。通过这种方式排列，您可以看到当事件处于活动状态时，哪些存储组件对延迟的影响最大，或者受延迟的影响。

对于动态性能事件，显示以下图表：

- 工作负载延迟 - 显示争用组件中排名靠前的受害者、欺凌者或鲨鱼工作负载的延迟历史记录。
- 工作负载活动 - 显示有关争用中的集群组件的工作负载使用情况的详细信息。
- 资源活动 - 显示争用的集群组件的历史性能统计数据。

当某些集群组件存在争用时，会显示其他图表。

其他事件简要描述了系统对存储对象执行的分析类型。在某些情况下，将会有一行或多行；每个已分析的组件都有一行，用于分析多个性能计数器的系统定义的性能策略。在这种情况下，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问题。

## 活动设置页面

事件设置页面显示已禁用的事件列表，并提供相关对象类型和事件严重性等信息。您还可以执行全局禁用或启用事件等任务。

只有具有应用程序管理员或存储管理员角色才可以访问此页面。

### 命令按钮

命令按钮使您能够针对选定的事件执行以下任务：

- 禁用

启动“禁用事件”对话框，您可以使用该对话框来禁用事件。

- 使能够

启用您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。这些规则针对集群AutoSupport消息运行，以生成Active IQ平台定义的系统配置、布线、最佳实践和可用性事件。

- 订阅 **EMS** 活动

启动“订阅 EMS 事件”对话框，该对话框使您能够订阅从您正在监控的集群接收特定的事件管理系统 (EMS) 事件。EMS 收集有关集群上发生的事件的信息。当收到订阅的 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

列表视图显示（以表格形式）有关已禁用事件的信息。您可以使用列过滤器来自定义显示的数据。

- 事件

显示已禁用事件的名称。

- 严重性

显示事件的严重级别。严重性可以是“严重”、“错误”、“警告”或“信息”。

- 来源类型

显示生成事件的源类型。

### 禁用事件对话框

“禁用事件”对话框显示您可以禁用事件的事件类型列表。您可以根据特定的严重性或一组事件禁用某种事件类型的事件。

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：

- 事件严重性

使您能够根据严重性类型选择事件，严重性类型可以是“严重”、“错误”、“警告”或“信息”。

- 事件名称包含

使您能够过滤名称包含指定字符的事件。

- 匹配事件

显示与您指定的事件严重性类型和文本字符串匹配的事件列表。

- 禁用事件

显示您选择禁用的事件列表。

事件的严重性也会与事件名称一起显示。

#### 命令按钮

命令按钮使您能够针对选定的事件执行以下任务：

- 保存并关闭

禁用事件类型并关闭对话框。

- 取消

放弃更改并关闭对话框。

## 管理警报

您可以配置警报，以便在发生特定事件或特定严重性类型的事件时自动发送通知。您还可以将警报与触发警报时执行的脚本关联。

### 什么是警报

虽然事件会连续发生，但只有当事件满足指定的过滤条件时，Unified Manager 才会生成警报。您可以选择应生成警报的事件 - 例如，当超过空间阈值或对象离线时。您还可以将警报与触发警报时执行的脚本关联。

过滤条件包括对象类别、名称或事件严重性。



## 警报电子邮件中包含哪些信息

Unified Manager 警报电子邮件提供事件类型、事件严重性、导致事件发生的策略或阈值的名称以及事件描述。电子邮件还为每个事件提供了超链接，使您可以在 UI 中查看该事件的详细信息页面。

警报电子邮件将发送给所有已订阅接收警报的用户。

如果性能计数器或容量值在收集期间发生较大变化，则可能导致针对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，您可能会收到一封针对警告事件的电子邮件和一封针对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

您可以配置警报，以便在生成特定事件时通知您。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。您可以指定接收通知的频率并将脚本与警报关联。

### 开始之前

- 您必须配置通知设置，例如用户电子邮件地址、SMTP 服务器和 SNMP 陷阱主机，以便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 and 事件，以及要通知的用户的用户名或电子邮件地址。

- 如果您希望根据事件执行脚本，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”，然后输入警报的名称和描述。
4. 单击“资源”，然后选择要包含在警报中或从警报中排除的资源。

您可以通过在\*名称包含\*字段中指定文本字符串来设置过滤器，以选择一组资源。根据您的指定的文本字符串，可用资源列表仅显示符合过滤规则的资源。您指定的文本字符串区分大小写。

如果资源同时符合您指定的包含规则和排除规则，则排除规则优先于包含规则，并且不会针对与排除的资源相关的事件生成警报。

5. 单击“事件”，然后根据事件名称或事件严重性类型选择要触发警报的事件。



要选择多个事件，请在选择时按住 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，并分配在生成警报时执行的脚本。



如果您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，如果您从“用户”页面修改了所选用户的电子邮件地址，则所选用户的修改后的电子邮件地址不会更新。

您还可以选择通过 SNMP 陷阱通知用户。

7. 单击“保存”。

#### 添加警报的示例

此示例显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，并排除名称包含“xyz”的所有卷
- 事件：包括所有重大健康事件
- 操作：包括“[sample@domain.com](mailto:sample@domain.com)”和“测试”脚本，并且每 15 分钟通知一次用户

在“添加警报”对话框中执行以下步骤：

1. 单击\*姓名\*，然后输入\*HealthTest\* 在 警报名称 字段中。
2. 单击“资源”，然后在“包含”选项卡中，从下拉列表中选择“卷”。
  - a. 进入\*abc\* 在“名称包含”字段中显示名称中包含“abc”的卷。

- b. 选择 **+ [All Volumes whose name contains 'abc'] +** 从可用资源区域，并将其移动到选定资源区域。
  - c. 单击“排除”，然后输入 `*xyz*` 在 名称包含 字段中，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. 从匹配事件区域选择“所有关键事件”，并将其移动到选定事件区域。
  5. 单击“操作”，然后输入 `*sample@domain.com*` 在“提醒这些用户”字段中。
  6. 选择 `*每 15 分钟提醒一次*`，每 15 分钟通知一次用户。

您可以配置警报以在指定时间内重复向收件人发送通知。您应该确定事件通知对于警报生效的时间。

7. 在选择要执行的脚本菜单中，选择 `*测试*脚本`。
8. 单击“保存”。

### 添加警报的准则

您可以根据资源（例如集群、节点、聚合或卷）以及特定严重性类型的事件添加警报。作为最佳实践，您可以在添加对象所属的集群之后为任何关键对象添加警报。

您可以根据以下指南和注意事项来创建警报，以有效地管理您的系统：

- 警报描述

您应该提供警报的描述，以便帮助您有效地跟踪警报。

- 资源

您应该决定哪些物理或逻辑资源需要警报。您可以根据需要包含或排除资源。例如，如果您想通过配置警报来密切监视您的聚合，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] +**，那么您将收到该类别中所有对象的警报。



选择集群作为资源并不会自动选择该集群内的存储对象。例如，如果您为所有集群的所有关键事件创建警报，那么您将只收到集群关键事件的警报。您将不会收到有关节点、聚合等的关键事件的警报。

- 事件严重性

您应该决定指定严重性类型（严重、错误、警告）的事件是否应触发警报，如果是，则应决定触发哪种严重性类型。

- 选定事件

如果您根据生成的事件类型添加警报，则应该决定哪些事件需要警报。

如果您选择事件严重性，但不选择任何单个事件（如果您将“选定事件”列留空），那么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。您还可以指定 SNMP 陷阱作为通知模式。您可以将脚本与警报关联，以便在生成警报时执行它们。

- 通知频率

您可以配置警报以在指定时间内重复向收件人发送通知。您应该确定事件通知对于警报生效的时间。如果您希望重复事件通知直到事件被确认，您应该确定希望重复通知的频率。

- 执行脚本

您可以将脚本与警报关联起来。当警报生成时，您的脚本就会执行。

## 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 收到的任何其他事件一样。此外，如果您希望平等对待所有性能事件并将电子邮件发送给同一个人，您可以创建一个警报，以便在触发任何关键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。

下面的示例展示了如何为所有关键延迟、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中选择事件，以及所有警告事件。

### 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”，然后输入警报的名称和描述。
4. 不要在“资源”页面上选择任何资源。

由于未选择任何资源，因此警报将应用于收到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. 在事件严重性列表中，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\* 然后单击箭头选择所有匹配的事件。
6. 单击“操作”，然后在“警告这些用户”字段中选择将接收警报电子邮件的用户的姓名。
7. 配置此页面上的任何其他选项以发出 SNMP 陷阱和执行脚本。
8. 单击“保存”。

## 测试警报

您可以测试警报以验证您是否已正确配置它。当触发事件时，会生成警报，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您的脚本是否已执行。

开始之前

- 您必须配置通知设置，例如收件人的电子邮件地址、SMTP 服务器和 SNMP 陷阱。
- 当生成事件时，Unified Manager 服务器可以使用这些设置向用户发送通知。
- 您必须分配一个脚本并将该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。

启用和禁用已解决和已过时事件的警报

对于您已配置为发送警报的所有事件，当这些事件转变至所有可用状态时都会发送警报消息：新建、已确认、已解决和已过时。如果您不想在事件进入“已解决”和“过时”状态时收到警报，您可以配置全局设置来抑制这些警报。

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，当事件进入“已解决”和“过时”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“已解决和过时事件的警报”项旁边的滑块控件执行以下操作之一：

| 目的                | 操作        |
|-------------------|-----------|
| 当事件得到解决或过时时停止发送警报 | 将滑块控件向左移动 |
| 当事件得到解决或过时时开始发送警报 | 将滑块控件向右移动 |

排除灾难恢复目标卷生成警报

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，因此您将收到这两个卷的警报。

开始之前

您必须具有应用程序管理员或存储管理员角色。

您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。这是可能的，因为卷事件的标识符包含 SVM 名称和卷名称，格式为“<svm\_name>:/<volume\_name>”。

下面的示例显示了如何在主 SVM“vs1”上为卷“vol1”创建警报，但排除在 SVM“vs1-dr”上同名卷上生成警报。

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\*Volume\*，然后输入\*vol1\* 在“名称包含”字段中显示名称中包含“vol1”的卷。
  - b. 选择 **+ [All Volumes whose name contains 'vol1'] +** 从\*可用资源\*区域，并将其移动到\*选定资源\*区域。
3. 选择\*Exclude\*选项卡，选择\*Volume\*，输入\*vs1-dr\* 在 名称包含 字段中，然后单击 添加。

这将排除针对 SVM“vs1-dr”上的卷“vol1”生成的警报。

4. 单击“事件”并选择要应用于卷的一个或多个事件。
5. 单击“操作”，然后在“警告这些用户”字段中选择将接收警报电子邮件的用户的姓名。
6. 配置此页面上的任何其他选项以发出 SNMP 陷阱和执行脚本，然后单击\*保存\*。

## 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。您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。

## 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警报相关的脚本。

4. 单击“保存”。

## 删除警报

当不再需要警报时，您可以删除它。例如，当某个资源不再受 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描述

您应该使用“添加警报”对话框配置警报以接收有关事件的通知。您还可以从警报设置页面查看警报列表。

### 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“添加警报”对话框，您可以在其中添加新警报。

- 编辑

显示“编辑警报”对话框，您可以借此编辑选定的警报。

- 删除

删除选定的警报。

- 使能够

启用选定的警报来发送通知。

- 禁用

当您想要暂时停止发送通知时，禁用所选警报。

- 测试

测试选定的警报以验证其添加或编辑后的配置。

- 已解决和过时事件的警报

允许您在事件移至“已解决”或“过时”状态时启用或禁用发送警报。这可以帮助用户避免接收不必要的通知。

## 列表视图

列表视图以表格形式显示有关所创建的警报的信息。您可以使用列过滤器来自定义显示的数据。您还可以选择一个警报以在详细信息区域中查看有关它的更多信息。

- 地位

指定是否启用警报 (  ) 或禁用 (  ) 。

- 警报

显示警报的名称。

- 描述

显示警报的描述。

- 通知方式

显示为警报选择的 notification 方法。您可以通过电子邮件或 SNMP 陷阱通知用户。

- 通知频率

指定管理服务器持续发送通知的频率（以分钟为单位），直到事件被确认、解决或移至过时状态。

## 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。

- 警报描述

显示警报的描述。



- 活动

显示您想要触发警报的事件。

- 资源

显示您想要触发警报的资源。

- 包括

显示您想要触发警报的资源组。

- 不包括

显示您不想触发警报的资源组。

- 通知方式

显示警报的通知方法。

- 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、解决或移至过时状态。

- 脚本名称

显示与所选警报关联的脚本的名称。当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。

## 添加警报对话框

您可以创建警报，在生成特定事件时通知您，以便您可以快速解决问题并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

此区域使您能够指定警报的名称和描述：

- 警报名称

使您能够指定警报名称。

- 警报描述

使您能够指定警报的描述。

## 资源

该区域使您能够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。\_动态规则\_是根据您指定的文本字符串过滤的资源集。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来显示特定资源。

如果您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

使您能够包含想要触发警报的资源。您可以指定一个文本字符串来对与该字符串匹配的资源进行分组，并选择该组包含在警报中。例如，您可以对名称包含“abc”字符串的所有卷进行分组。

- 排除

使您能够排除不想触发警报的资源。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>>或者<<All Volumes whose name contains 'xyz'>>。

如果资源同时符合您指定的包含规则和排除规则，则排除规则优先于包含规则，并且不会为事件生成警报。

## 事件

此区域使您能够选择要为其创建警报的事件。您可以根据特定严重性或一组事件创建事件警报。

要选择多个事件，您应该在选择时按住 Ctrl 键。

- 事件严重性

使您能够根据严重性类型选择事件，严重性类型可以是“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

此区域使您能够指定在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

使您能够指定接收通知的用户的电子邮件地址或用户名。

如果您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，如果您从“用户”页面修改了所选用户的电子邮件地址，则所选用户的修改后的电子邮件地址不会更新。

- 通知频率

使您能够指定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式：

- 仅通知一次
- 按指定频率通知
- 在指定时间范围内按指定频率通知

- 发出 **SNMP** 陷阱

选择此框可让您指定是否应将 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中。当生成警报时执行此脚本。



如果您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

- 节省

创建警报并关闭对话框。

- 取消

放弃更改并关闭对话框。

#### 编辑警报对话框

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

此区域使您能够编辑警报的名称和描述。

- 警报名称

使您能够编辑警报名称。

- 警报描述

使您能够指定警报的描述。

- 警戒状态

使您能够启用或禁用警报。

##### 资源

该区域使您能够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来显示特定资源。

- 包括

使您能够包含想要触发警报的资源。您可以指定一个文本字符串来对与该字符串匹配的资源进行分组，并选择该组包含在警报中。例如，您可以对名称包含“vol0”字符串的所有卷进行分组。

- 排除

使您能够排除不想触发警报的资源。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'] +。

## 事件

此区域使您能够选择想要触发警报的事件。您可以根据特定严重性或一组事件触发事件警报。

- 事件严重性

使您能够根据严重性类型选择事件，严重性类型可以是“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

此区域使您能够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，或者指定新的电子邮件地址或用户名来接收通知。

- 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式：

- 仅通知一次
- 按指定频率通知
- 在指定时间范围内按指定频率通知

- 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关联。当生成警报时执行此脚本。

命令按钮

- 节省

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

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。当事件触发警报时，脚本就会执行。您可以上传自定义脚本并在生成警报时测试其执行情况。

默认情况下，将脚本上传到 Unified Manager 并运行它们的功能是启用的。如果您的组织由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"](#)

### 脚本如何与警报结合使用

您可以将警报与脚本关联，以便在 Unified Manager 中针对某个事件发出警报时执行该脚本。您可以使用脚本来解决存储对象的问题，或者标识哪些存储对象正在生成事件。

当 Unified Manager 中某个事件生成警报时，会向指定的收件人发送警报电子邮件。如果您已将警报与脚本关联，则系统将执行该脚本。您可以从警报电子邮件中获取传递给脚本的参数详细信息。



如果您创建了自定义脚本并将其与特定事件类型的警报关联，则会根据该事件类型的自定义脚本采取操作，并且“管理操作”页面或 Unified Manager 仪表板上默认不提供“修复”操作。

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`
```

添加脚本

您可以在 Unified Manager 中添加脚本，并将脚本与警报关联。生成警报时，系统将自动执行这些脚本，使您能够获得有关生成事件的存储对象的信息。

开始之前

- 您必须已创建并保存要添加到 Unified Manager 服务器的脚本。
- 脚本支持的文件格式包括 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，而脚本仅支持 Perl 5 支持的功能。如果在 Unified Manager 之后安装了 Perl，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来跟踪警报脚本进度，则必须确保日志文件不会在 Unified Manager 安装文件夹内的任何位置创建。

- 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。



如果您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“添加”。

相关信息

["启用和禁用上传脚本的功能"](#)

删除脚本

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。
- 该脚本不得与警报关联。

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。

测试脚本执行

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传到 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 | <div>a. 单击“添加”。</div> <div>b. 在“操作”部分，将警报与您的测试脚本关联。</div> |

| 目的   | 操作                                              |
|------|-------------------------------------------------|
| 编辑警报 | a. 选择一个警报，然后单击“编辑”。<br>b. 在“操作”部分，将警报与您的测试脚本关联。 |

- 单击“保存”。
- 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\*。

该脚本使用“-test”参数执行，并将通知警报发送到创建警报时指定的电子邮件地址。

## 支持的 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，对集群、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的脚本中使用 CLI 命令，或者在触发警报时执行的脚本。

所有命令必须以命令开头 `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                                                                         | 描述                                                                                               | 输出                                            |
|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------|
| <code>um cli login -u &lt;username&gt; [-p &lt;password&gt;]</code>            | 登录到 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在历史记录或进程表中。会话在登录后三小时过期，之后用户必须再次登录。 | 显示相应的消息。                                      |
| <code>um cli logout</code>                                                     | 退出 CLI。                                                                                          | 显示相应的消息。                                      |
| <code>um help</code>                                                           | 显示所有第一级子命令。                                                                                      | 显示所有第一级子命令。                                   |
| <code>um run cmd [ -t &lt;timeout&gt; ] &lt;cluster&gt; &lt;command&gt;</code> | 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获取或执行 ONTAP 上的操作。可选的超时参数设置在客户端完成命令的最大时间限制（以秒为单位）。默认值为 0（永远等待）。      | 从 ONTAP 收到。                                   |
| <code>um run query &lt;sql command&gt;</code>                                  | 执行 SQL 查询。只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                                                                                                                                          | 描述                                                                                                                                                                              | 输出                                                                                                                                                           |
|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| um datasource add -u<br><username> -P <password> [<br>-t <protocol> ] [ -p<br><port> ] <hostname-or-ip>                                         | 将数据源添加到托管存储系统列表中。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 [<br><datasource-id>]                                                                                                        | 显示托管存储系统的数据源。                                                                                                                                                                   | 以表格形式显示以下值：ID<br>Address Port, Protocol<br>Acquisition Status,<br>Analysis Status,<br>Communication status,<br>Acquisition Message, and<br>Analysis Message。 |
| um datasource modify [ -h<br><hostname-or-ip> ] [ -u<br><username> ] [ -P<br><password> ] [ -t<br><protocol> ] [ -p <port> ]<br><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<br><datasource-id>                                                                                                         | 从 Unified Manager 中删除数据源（集群）。                                                                                                                                                   | 显示相应的消息。                                                                                                                                                     |
| um option list [ <option><br>.. ]                                                                                                               | 列出可以使用 set 命令配置的所有选项。                                                                                                                                                           | 以表格形式显示以下值：Name,<br>Value, Default Value, and<br>Requires Restart.                                                                                           |
| um option set <option-<br>name>=<option-value> [<br><option-name>=<option-<br>value> ... ]                                                      | 设置一个或多个选项。该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                                       | 描述                                                                                                                                                                                                                              | 输出                                  |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| um lun list [-q] [-ObjectType <object-id>]   | <p>列出按指定对象过滤后的 LUN。-q 适用于所有命令，不显示标题。ObjectType 可以是 lun、qtree、cluster、volume、quota 或 svm。</p> <p>例如：</p> <p><b>um lun list -cluster 1</b></p> <p>在这个例子中，“-cluster”是 objectType，“1”是 objectId。该命令列出了集群内 ID 为 1 的所有 LUN。</p>       | 以表格形式显示以下值：ID and LUN path.         |
| um svm list [-q] [-ObjectType <object-id>]   | <p>按指定对象过滤后列出存储虚拟机。ObjectType 可以是 lun、qtree、cluster、volume、quota 或 svm。</p> <p>例如：</p> <p><b>um svm list -cluster 1</b></p> <p>在这个例子中，“-cluster”是 objectType，“1”是 objectId。该命令列出了集群内 ID 为 1 的所有存储虚拟机。</p>                       | 以表格形式显示以下值：Name and Cluster ID.     |
| um qtree list [-q] [-ObjectType <object-id>] | <p>列出按指定对象过滤后的 qtree。-q 适用于所有命令，不显示标题。ObjectType 可以是 lun、qtree、cluster、volume、quota 或 svm。</p> <p>例如：</p> <p><b>um qtree list -cluster 1</b></p> <p>在这个例子中，“-cluster”是 objectType，“1”是 objectId。该命令列出了集群内 ID 为 1 的所有 qtree。</p> | 以表格形式显示以下值：Qtree ID and Qtree Name. |

| CLI 命令                                              | 描述                                                                                                                                                                                               | 输出                                                                                             |
|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| um disk list [-q] [-ObjectType <object-id>]         | <p>列出按指定对象过滤后的磁盘。ObjectType 可以是磁盘、聚合、节点或集群。</p> <p>例如：</p> <p><b>um disk list -cluster 1</b></p> <p>在这个例子中，“-cluster”是 objectType，“1”是 objectId。该命令列出了集群内 ID 为 1 的所有磁盘。</p>                      | 以表格形式显示以下值<br>ObjectType and object-id。                                                        |
| um cluster list [-q] [-ObjectType <object-id>]      | <p>列出根据指定对象进行过滤后的集群。ObjectType 可以是磁盘、aggr、节点、集群、lun、qtree、卷、配额或 svm。</p> <p>例如：</p> <p><b>um cluster list -aggr 1</b></p> <p>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。</p> | 以表格形式显示以下值：Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key。 |
| um cluster node list [-q] [-ObjectType <object-id>] | <p>根据指定对象进行过滤后列出集群节点。ObjectType 可以是磁盘、聚合、节点或集群。</p> <p>例如：</p> <p><b>um cluster node list -cluster 1</b></p> <p>在这个例子中，“-cluster”是 objectType，“1”是 objectId。该命令列出了集群内 ID 为 1 的所有节点。</p>          | 以表格形式显示以下值 Name and Cluster ID。                                                                |

| CLI 命令                                                               | 描述                                                                                                                                                                                                              | 输出                                    |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| <code>um volume list [-q] [-ObjectType &lt;object-id&gt;]</code>     | <p>列出按指定对象过滤后的卷。ObjectType 可以是 lun、mtree、cluster、volume、quota、svm 或 aggregate。</p> <p>例如：</p> <p><b>um volume list -cluster 1</b></p> <p>在这个例子中，“-cluster”是 objectType，“1”是 objectId。该命令列出了集群内 ID 为 1 的所有卷。</p> | 以表格形式显示以下值 Volume ID and Volume Name。 |
| <code>um quota user list [-q] [-ObjectType &lt;object-id&gt;]</code> | <p>列出按指定对象过滤后的配额用户。ObjectType 可以是 mtree、cluster、volume、quota 或 svm。</p> <p>例如：</p> <p><b>um quota user list -cluster 1</b></p> <p>在这个例子中，“-cluster”是 objectType，“1”是 objectId。该命令列出了集群内 ID 为 1 的所有配额用户。</p>     | 以表格形式显示以下值 ID, Name, SID and Email。   |
| <code>um aggr list [-q] [-ObjectType &lt;object-id&gt;]</code>       | <p>列出按指定对象过滤后的聚合。ObjectType 可以是磁盘、聚合、节点、集群或卷。</p> <p>例如：</p> <p><b>um aggr list -cluster 1</b></p> <p>在这个例子中，“-cluster”是 objectType，“1”是 objectId。该命令列出了集群中 ID 为 1 的所有聚合。</p>                                   | 以表格形式显示以下值 Aggr ID, and Aggr Name。    |
| <code>um event ack &lt;event-ids&gt;</code>                          | 确认一个或多个事件。                                                                                                                                                                                                      | 显示相应的消息。                              |
| <code>um event resolve &lt;event-ids&gt;</code>                      | 解决一个或多个事件。                                                                                                                                                                                                      | 显示相应的消息。                              |
| <code>um event assign -u &lt;username&gt; &lt;event-id&gt;</code>    | 将事件分配给用户。                                                                                                                                                                                                       | 显示相应的消息。                              |

| CLI 命令                                                                                                            | 描述                             | 输出                                                                         |
|-------------------------------------------------------------------------------------------------------------------|--------------------------------|----------------------------------------------------------------------------|
| <code>um event list [ -s &lt;source&gt; ] [ -S &lt;event-state-filter-list&gt;.. ] [ &lt;event-id&gt; .. ]</code> | 列出系统或用户生成的事件。根据来源、状态和 ID 过滤事件。 | 以表格形式显示以下值 Source, Source type, Name, Severity, State, User and Timestamp。 |
| <code>um backup restore -f &lt;backup_file_path_and_name&gt;</code>                                               | 使用 .7z 文件恢复 MySQL 数据库备份。       | 显示相应的消息。                                                                   |

## 脚本窗口和对话框的描述

脚本页面允许您将脚本添加到 Unified Manager。

### 脚本页面

通过“脚本”页面，您可以将自定义脚本添加到 Unified Manager。您可以将这些脚本与警报关联起来，以实现存储对象的自动重新配置。

脚本页面允许您从 Unified Manager 添加或删除脚本。

#### 命令按钮

- 添加

显示“添加脚本”对话框，您可以在其中添加脚本。

- 删除

删除选定的脚本。

#### 列表视图

列表视图以表格形式显示您添加到 Unified Manager 的脚本。

- 姓名

显示脚本的名称。

- 描述

显示脚本的描述。

#### 添加脚本对话框

通过“添加脚本”对话框，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

使您能够选择警报的脚本。

- 描述

使您能够指定脚本的描述。

# 监控和管理集群性能

## Active IQ Unified Manager性能监控简介

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，您还可以指定某些性能计数器的最大值，以便在超过阈值时生成事件。Unified Manager 会向您发出有关这些性能事件的警报，以便您采取纠正措施，并使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 监控两种类型工作负载的性能：

- 用户定义的工作负载

这些工作负载包括您在集群中创建的FlexVol卷和FlexGroup卷。

- 系统定义的工作负载

这些工作负载由内部系统活动组成。

### Unified Manager 性能监控功能

Unified Manager 收集并分析运行ONTAP软件的系统的性能统计数据。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。

响应时间（延迟）较长表明存储对象（例如卷）的执行速度比正常情况慢。此问题还表明使用该卷的客户端应用程序的性能有所下降。Unified Manager 可识别存在性能问题的存储组件，并提供可采取的解决性能问题的建议操作列表。

Unified Manager 包括以下功能：

- 监控并分析运行ONTAP软件的系统的工作负载性能统计数据。
- 跟踪集群、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。
- 显示绘制工作负载活动随时间变化的详细图表；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，当阈值被突破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了解您的工作负载活动，以识别性能问题并向您发出警报。
- 识别应用于您的卷和 LUN 的服务质量 (QoS) 策略和性能服务级别策略 (PSL)。
- 清楚地识别存在争用的集群组件。
- 识别过度使用集群组件的工作负载以及性能受到活动增加影响的工作负载。

## 用于管理存储系统性能的 **Unified Manager** 界面

这些部分包含有关Active IQ Unified Manager提供的两个用户界面的信息，用于解决数据存储容量、可用性和保护问题。这两个 UI 是 Unified Manager Web UI 和维护控制台。

如果您想使用 Unified Manager 中的保护功能，您还必须安装和配置OnCommand Workflow Automation (WFA)。

### **Unified Manager Web UI**

Unified Manager Web UI 使管理员能够监控和排除与数据存储容量、可用性和保护相关的集群问题。

这些部分介绍了管理员可以遵循的一些常见工作流程，以解决 Unified Manager Web UI 中显示的存储容量、数据可用性或保护问题。

### 维护控制台

Unified Manager 维护控制台使管理员能够监控、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。

## 集群配置和性能数据收集活动

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。对集群进行更改时也适用此间隔。

例如，如果您向集群中的 SVM 添加两个新卷，您将在下一个轮询间隔（最长可达 15 分钟）后在 UI 中看到这些新对象。

Unified Manager 每五分钟从所有受监控的集群收集一次当前性能统计数据。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。这使您可以查看当前月份的非常详细的性能详情以及长达一年的总体性能趋势。

收集轮询会偏移几分钟，以便每个集群的数据不会同时发送，这可能会影响性能。

下表描述了 Unified Manager 执行的收集活动：

| 活动     | 时间间隔 | 描述             |
|--------|------|----------------|
| 绩效统计调查 | 每5分钟 | 从每个集群收集实时性能数据。 |



| 活动        | 时间间隔        | 描述                                                                                                                         |
|-----------|-------------|----------------------------------------------------------------------------------------------------------------------------|
| 统计分析      | 每5分钟        | <p>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。</p> <p>如果超出任何性能阈值，Unified Manager 会生成事件并向指定用户发送电子邮件（如果配置为这样做）。</p> |
| 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         | <p>将最近 12 个五分钟性能数据集合汇总为每小时平均值。</p> <p>部分UI页面采用每小时平均值，并保留180天。</p>                                                          |
| 预测分析和数据修剪 | 每天午夜后       | <p>分析集群数据以建立未来 24 小时的卷延迟和 IOPS 的动态阈值。</p> <p>从数据库中删除任何超过 30 天的五分钟性能数据。</p>                                                 |
| 数据修剪      | 每天凌晨 2 点后   | 从数据库中删除任何超过 180 天的事件以及超过 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。                                                                                                 |

## 什么是数据连续性收集周期

数据连续性收集周期检索实时集群性能收集周期之外的性能数据，默认情况下，实时集群性能收集周期每五分钟运行一次。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白。

当发生以下事件时，Unified Manager 会对历史性能数据执行数据连续性收集轮询：

- 集群最初添加到 Unified Manager。

Unified Manager 收集前 15 天的历史性能数据。这使您可以在添加集群后的几个小时内查看该集群两周的历史性能信息。

此外，如果存在的话，还会报告前一时期的系统定义阈值事件。

- 当前性能数据收集周期未按时完成。

如果实时性能轮询超出了五分钟的收集时间，则会启动数据连续性收集周期来收集缺失的信息。如果没有数据连续性收集，则跳过下一个收集期。

- Unified Manager 在一段时间内无法访问，然后又重新上线，如以下情况：
  - 它已重新启动。
  - 它在软件升级或创建备份文件时被关闭。
  - 网络中断已修复。
- 集群在一段时间内无法访问，然后又重新上线，例如以下情况：
  - 网络中断已修复。
  - 广域网连接速度慢延迟了性能数据的正常收集。

一个数据连续性采集周期最多可以采集24小时的历史数据。如果 Unified Manager 停机超过 24 小时，UI 页面上的性能数据就会出现差距。

数据连续性收集周期和实时数据收集周期不能同时运行。数据连续性收集周期必须在启动实时性能数据收集之前完成。当数据连续性收集需要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。

## 时间戳在收集的数据和事件中意味着什么

收集的健康和性能数据中出现的时间戳，或作为事件检测时间出现的时间戳，基于ONTAP集群时间，并根据 Web 浏览器上设置的时区进行调整。

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集群和 Web 浏览器上的时间。



如果您发现某个特定集群的时间戳不正确，您可能需要检查集群时间是否设置正确。

## 在 Unified Manager GUI 中导航性能工作流程

Unified Manager 界面提供了许多页面用于收集和显示性能信息。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来查看和配置信息。

您可以使用以下所有页面来监视和排除集群性能信息故障：

- 仪表板页面
- 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
- 活动页面

## 登录用户界面

您可以使用受支持的 Web 浏览器登录 Unified Manager UI。

## 开始之前

- 网络浏览器必须满足最低要求。

请参阅互操作性矩阵 "[mysupport.netapp.com/matrix](https://mysupport.netapp.com/matrix)" 以获取受支持的浏览器版本的完整列表。

- 您必须拥有 Unified Manager 服务器的 IP 地址或 URL。

如果您 1 小时没有活动，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. 在您的 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，表明该证书不受信任。您可以承认风险并继续访问，或者安装证书颁发机构 (CA) 签名的数字证书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 身份验证保护登录 Unified Manager 用户界面，您将在身份提供商 (IdP) 登录页面而不是 Unified Manager 登录页面中输入您的凭据。

将显示“仪表板”页面。



如果 Unified Manager 服务器未初始化，则新的浏览器窗口将显示首次体验向导。您必须输入将向其发送电子邮件警报的初始电子邮件收件人、将处理电子邮件通信的 SMTP 服务器，以及是否启用 AutoSupport 以将有关 Unified Manager 安装的信息发送给技术支持。完成此信息后，将出现 Unified Manager UI。

## 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。

### 监控集群对象导航

您可以监控 Unified Manager 管理的任何集群中所有对象的性能。监控您的存储对象可以让您概览集群和对象的性能，并包括性能事件监控。您可以从高层次查看性能和事件，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，然后单击条形图导航到该集群的节点列表。
2. 确定具有最高性能容量使用值的节点并单击该节点。
3. 在节点/性能资源管理器页面中，单击查看和比较菜单中的\*此节点上的聚合\*。
4. 确定使用最多性能容量的聚合并单击该聚合。

5. 在“聚合/性能资源管理器”页面上，单击“查看和比较”菜单中的“此聚合上的卷”。
6. 确定使用最多 IOPS 的卷。

您应该调查这些卷，看看是否应该应用 QoS 策略或性能服务级别策略，或者更改策略设置，以便这些卷不会在集群上使用如此大比例的 IOPS。

**Dashboard** All Clusters

**Management Actions**

- Enable takeover on panic (2)
- Disable telnet (2)
- Enable volume autogrow (9)

**Capacity**

31 events (No new in past 24 hours)

| CLUSTER         | USED    | DAYS TO FULL | REDUCTION |
|-----------------|---------|--------------|-----------|
| opm-sl...licity | 40.5 TB | < 1 month    | 13.0:1    |
| umeng...1-02    | 83.6 TB | 51 days      | 8.0:1     |
| sysmgr...0-1-8  | 33 TB   | 149 days     | 6.3:1     |

**Performance Capacity**

No new events

| CLUSTER            | USED | DAYS TO FULL |
|--------------------|------|--------------|
| umeng-aff220-01-02 | 83%  | < 1 month    |
| sysmgr-fas8060-1-8 | 49%  | < 1 month    |
| fas8040-206-21     | 46%  | 77 days      |

**Nodes**

Last updated: Nov 15, 2019, 10:48 AM

VIEW Nodes on umeng-aff220-01-02 Search Nodes Filter Hardware Inventory Report

Assign Performance Threshold Policy Clear Performance Threshold Policy Scheduled Reports Show/Hide

| Status | Node            | Latency    | IOPS        | MB/s     | Performance Capacity Used | Utilization | Fr  |
|--------|-----------------|------------|-------------|----------|---------------------------|-------------|-----|
| ✖      | umeng-aff220-01 | 21.7 ms/op | 27,333 IOPS | 221 MB/s | 73%                       | 50%         | 3.1 |
| ✖      | umeng-aff220-02 | 8.33 ms/op | 83.4 IOPS   | 102 MB/s | 53%                       | 42%         | 6.1 |

**Node / Performance : umeng-aff220-01**

Summary Explorer Failover Planning Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Aggregates on this Node Filter

| Aggregate  | Latency  | IOPS      | MB/s     | Perf... |
|------------|----------|-----------|----------|---------|
| NSLM12_002 | 12.4 ... | 47.51 ... | 5.8 M... | 8 %     |
| NSLM12_001 | 11.4 ... | 216 L...  | 4.33 ... | 5 %     |

**Aggregate / Performance : NSLM12\_002**

Summary Explorer Information

Compare the performance of associated objects and display detailed charts

VIEW AND COMPARE Volumes on this Aggregate Filter

| Volume               | Latency    | IOPS       | MB/s      |
|----------------------|------------|------------|-----------|
| suchita_vmware_d...  | 6.38 ms... | 76.8 IOPS  | 2.55 MB/s |
| suchita_vmware_d...  | 3.82 ms... | 4,775 L... | 18.7 MB/s |
| aiqum_scale_do_no... | 0.114 m... | < 1 IOPS   | < 1 MB/s  |

## 监控集群性能导航

您可以监控 Unified Manager 管理的所有集群的性能。监控集群可为您提供集群和对象性能的概览，并包括性能事件监控。您可以从高层次查看性能和事件，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. 要查看有关这些聚合的性能的信息，请选择“性能：所有聚合”视图。
3. 确定您要调查的聚合，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. 或者，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出现在计数器图表中以供比较。

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”以查看有关该聚合的性能历史记录的信息。

## 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 

| <input type="checkbox"/> | Status                                                                            | Aggregate    | Type | Latency    | IOPS      | MB/s      | Performance Capacity Used | Utilization |
|--------------------------|-----------------------------------------------------------------------------------|--------------|------|------------|-----------|-----------|---------------------------|-------------|
| <input type="checkbox"/> |  | aggr_evt     | SSD  | 0.29 ms/op | 3.79 IOPS | < 1 MB/s  | < 1%                      | < 1%        |
| <input type="checkbox"/> |  | <b>aggr4</b> | HDD  | 5.74 ms/op | 14.4 IOPS | 1.31 MB/s | 6%                        | 5%          |
| <input type="checkbox"/> |  | aggr3        | HDD  | 5.06 ms/op | 3.06 IOPS | < 1 MB/s  | 6%                        | 5%          |
| <input type="checkbox"/> |  | meg_aggr2    | HDD  | 10.4 ms/op | 52.9 IOPS | 7.28 MB/s | 3%                        | 2%          |

## Aggregate / Performance : aggr4

Switch to Health View Last updated: Nov 15, 2019, 1:20 PM 

Summary Explorer **Information**

Compare the performance of associated objects and display detailed charts 

TIME RANGE  Last 72 Hours

VIEW AND COMPARE **Aggregates on same Node** 

Filter

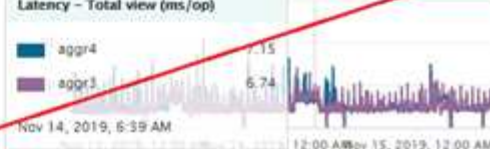
| Aggregate       | Latency  | IOPS     | MB/s     | Perf... |
|-----------------|----------|----------|----------|---------|
| aggr3           | 5.06 ... | 3.06 ... | < 1 M... | 6%      |
| <b>aggr_evt</b> | 0.29 ... | 3.79 ... | < 1 M... | < 1%    |
| aggr_automation | 0.27...  | 6.35 ... | < 1 M... | < 1%    |

**Comparing**  
1 Additional Object  


-  aggr4
-  aggr3

CHOOSE CHARTS 7 Charts Selected 

Events for Aggregate: aggr4  
     
No data to display

Latency  Total  **Zoom View**  
Latency - Total view (ms/op)  
  
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

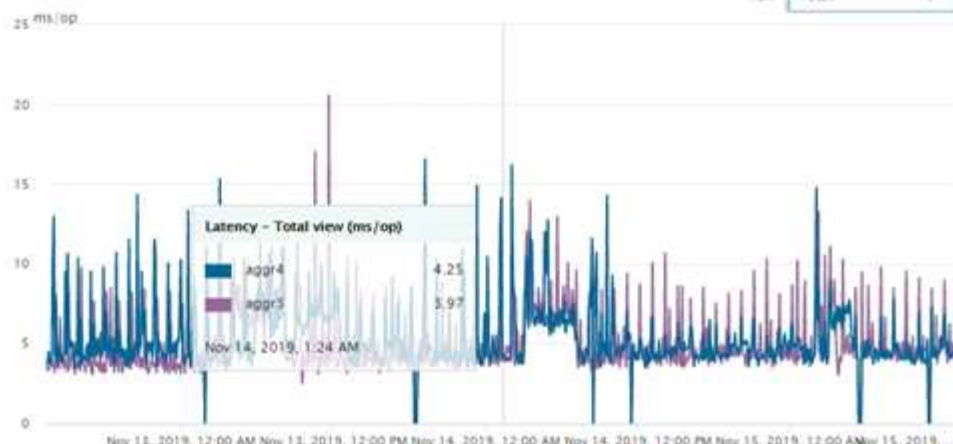
 Critical Events  
 Error Events  
 Warning Events  
 Information Events

     
No data to display

Comparing Objects

 aggr4

 aggr3



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、排除故障和微调系统性能时非常有用。

根据性能事件的类型，您可能会看到以下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例子。

1. 在左侧导航窗格中，单击“事件管理”。
2. 从“查看”菜单中，单击“活动性能事件”。
3. 单击要调查的事件的名称，将显示事件详细信息页面。
4. 查看事件描述并查看建议的操作（如果有）以查看有关该事件的更多详细信息，这可能有助于您解决问题。您可以单击“分析工作负载”按钮来显示详细的性能图表，以帮助进一步分析问题。



## Event Management

Last updated: Nov 15, 2019, 11:23 AM

VIEW

Active performance events

Search Events

Filter +

Assign To

Acknowledge

Mark as Resolved

Add Alert

Show / Hide

| Triggered Time         | Severity | State | Impact Lev | Impact Area | Name                                          | Source                        | Source Ty |
|------------------------|----------|-------|------------|-------------|-----------------------------------------------|-------------------------------|-----------|
| Nov 14, 2019, 11:39 AM |          | New   | Risk       | Performance | QoS Volume Peak IOP... Threshold Breached     | vs2:/julia_feb12_vol3         | Volume    |
| Nov 14, 2019, 11:39 AM |          | New   | Risk       | Performance | QoS Volume Peak IOP... Threshold Breached     | vs7:/julia_non_shared_3       | Volume    |
| Nov 15, 2019, 5:04 AM  |          | New   | Risk       | Performance | QoS Volume Peak IOP... Threshold Breached     | suchita_vmwar...nt_delete_01  | Volume    |
| Nov 15, 2019, 10:39 AM |          | New   | Risk       | Performance | Workload LUN Latency ... Service Level Policy | iscsi_boot/ia.../ocum-c220-01 | LUN       |
| Nov 15, 2019, 10:39 AM |          | New   | Risk       | Performance | Workload LUN Latency ... Service Level Policy | iscsi_boot/ia.../ocum-c220-07 | LUN       |

### Event: QoS Volume Peak IOPS/TB Warning Threshold Breached

(Last Seen: Nov 15, 2019, 11:19 AM)

IOPS value of 570 IOPS on policy group NSLM\_vs7\_Performance\_2\_0 has triggered a WARNING event to identify performance problems for the workloads in this policy group.



Actions

#### Suggested Actions to Fix The Issue

##### Troubleshoot

Analyze Workload

##### Take Action

This is an Adaptive QoS Policy that might be used by other workloads in the system.

If it is acceptable that changes you make to the QoS setting will be applied to other workloads that are using this policy,

- Increase the threshold to 4950 IOPS/TB for this Adaptive QoS Policy.

If you are satisfied with the current limitation on workload throughput,

- Leave the QoS configuration setting as it is.

#### Event Information

|                        |              |                            |
|------------------------|--------------|----------------------------|
| EVENT TRIGGER TIME     | SEVERITY     | SOURCE                     |
| Nov 14, 2019, 11:39 AM | Warning      | vs7:/julia_non_shared_3    |
| STATE                  | IMPACT LEVEL | SOURCE TYPE                |
| New                    | Risk         | Volume                     |
| EVENT DURATION         | IMPACT AREA  | ION CLUSTER                |
| 1 day 40 minutes       | Performance  | ocum-mobility-01-02        |
| LAST SEEN              |              | AFFECTED OBJECTS COUNT     |
| Nov 15, 2019, 11:19 AM |              | 1                          |
|                        |              | TRIGGERED POLICY           |
|                        |              | QoS Peak IOPS/TB threshold |

## 搜索存储对象

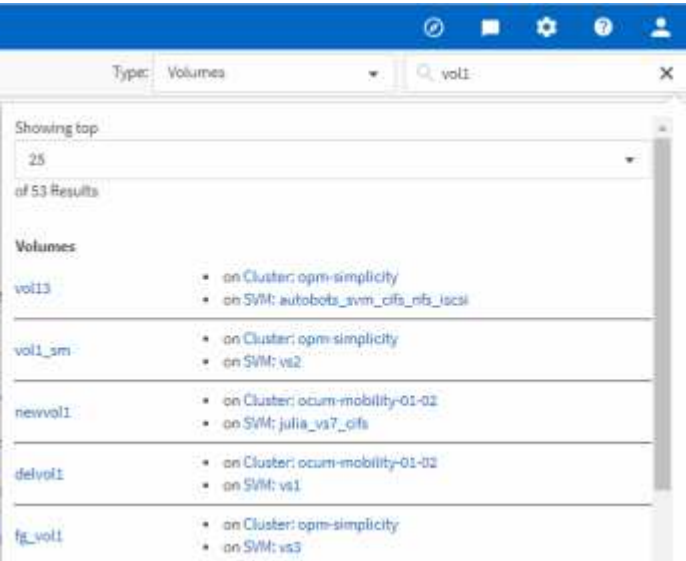
要快速访问特定对象，您可以使用菜单栏顶部的“搜索所有存储对象”字段。这种对所有对象进行全局搜索的方法使您能够按类型快速定位特定对象。搜索结果按存储对象类型排序，您可以使用下拉菜单进行过滤。有效搜索必须至少包含三个字符。

全局搜索显示结果总数，但只能访问前 25 个搜索结果。因此，如果您知道想要快速找到的项目，则可以将全局搜索功能视为查找特定项目的快捷工具。要获得完整的搜索结果，您可以使用对象库存页面中的搜索及其相关的过滤功能。



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”字段中输入对象或事件名称的至少三个字符，然后按“Enter”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：卷名称
- LUN：LUN 路径



 无法在全球搜索栏中搜索 LIF 和端口。

在此示例中，下拉框已选择卷对象类型。在“搜索所有存储对象”字段中输入“vol”将显示名称中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。

### 过滤库存页面内容

您可以在 Unified Manager 中过滤库存页面数据，以便根据特定条件快速定位数据。您可以使用过滤功能来缩小 Unified Manager 页面的内容范围，以仅显示您感兴趣的结果。这是一种非常高效的方法，它可以仅显示您感兴趣的数据。

使用\*过滤\*根据您的喜好自定义网格视图。可用的过滤选项基于网格中查看的对象类型。如果当前应用了过滤器，则已应用的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参数。

| 参数      | 验证                             |
|---------|--------------------------------|
| 字符串（文本） | 运算符包括*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 <b>is</b> 和 <b>is not</b> 。 |

每个过滤器都需要列、运算符和值字段；可用的过滤器反映当前页面上可过滤的列。您最多可以应用四个过滤器。过滤结果基于组合过滤参数。过滤结果适用于过滤搜索中的所有页面，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“过滤器”按钮。显示过滤面板。
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. 要添加另一个过滤器，请单击“+添加过滤器”。一个额外的筛选字段即会显示。使用上述步骤中所述的过程完成此筛选器。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”。过滤选项应用于网格，过滤器的数量显示在过滤器按钮的右侧。
7. 使用过滤面板通过单击要删除的过滤器右侧的垃圾桶图标来删除单个过滤器。
8. 要删除所有过滤器，请单击过滤面板底部的“重置”。

### 筛选示例

该图显示了带有三个过滤器的过滤面板。当您拥有的过滤器少于四个时，将显示“+添加过滤器”按钮。

The screenshot shows a filter panel with three rows of filters. Each row has a dropdown for the field, a dropdown for the operator, and a text input for the value. To the right of each row is a trash icon for deletion. At the bottom left is a '+ Add Filter' button. At the bottom right are 'Cancel' and 'Apply Filter' buttons. The filters are: 1. MBps greater than 5 MBps; 2. Node name starts with test; 3. Type is FCP Port.

单击“应用过滤器”后，“过滤”面板将关闭，应用过滤器，并显示已应用的过滤器数量（ 3 ）。

## 从仪表板监控集群性能

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性能状态。它使您能够评估托管集群的整体性能，并快速记录、定位或分配解决任何已识别的特定事件。

## 了解仪表板上的性能面板

Unified Manager 仪表板提供了一些面板，显示环境中正在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的活跃事件数以及过去 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库存页面的链接，该页面经过筛选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

在查看所有集群时，此面板会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之前的天数（基于每日增长率）。单击条形图将转到该集群的节点清单页面。请注意，节点库存页面显示过去 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

当启用工作负载主动管理并查看单个集群时，此面板显示当前在一定 IOPS 范围内运行的工作负载总数。

- 工作负载性能面板

启用工作负载主动管理后，此面板显示分配给每个定义的性能服务级别的符合和不符合的工作负载总数。单击条形图可转到“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，您可以选择按最高 IOPS 或吞吐量（MB/s）排序查看集群。

查看单个集群时，您可以选择按最高 IOPS 或吞吐量（MB/s）排序查看该集群上的工作负载。

## 性能横幅消息和说明

Unified Manager 可能会在通知页面上显示横幅消息（来自通知铃），以提醒您特定集群的状态问题。

| 横幅消息                                                                                                                     | 描述                                      | 解决方法                                             |
|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------|
| No performance data is being collected from cluster <i>cluster_name</i> . 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性能数据。 | 重新启动 Unified Manager 以解决此问题。如果此方法无法解决问题，请联系技术支持。 |

| 横幅消息                                                                                                                                                                     | 描述                                    | 解决方法                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|-----------------------------------------------------------------------------------------------|
| More than x hour(s) of historical data is being collected from cluster <i>cluster_name</i> . Current data collections will start after all historical data is collected. | 数据连续性收集周期目前正在运行，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。数据连续性收集周期完成后，将收集当前性能数据。<br><br>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。 |

## 修改性能统计收集间隔

性能统计信息的默认收集间隔为5分钟。如果您发现大型集群的收集未在默认时间内完成，则可以将此间隔更改为 10 或 15 分钟。此设置会影响此 Unified Manager 实例所监控的所有集群的统计信息收集。

开始之前

您必须拥有授权登录 Unified Manager 服务器维护控制台的用户 ID 和密码。

横幅消息指出了性能统计数据收集未按时完成的问题 Unable to consistently collect from cluster *<cluster\_name>* 或者 `Data collection is taking too long on cluster *<cluster\_name>*。

仅当由于统计信息收集问题而需要时才应更改收集间隔。请勿因任何其他原因更改此设置。



将此值从默认设置 5 分钟更改为其他值可能会影响 Unified Manager 报告的性能事件的数量和频率。例如，当超过策略 30 分钟时，系统定义的性能阈值会触发事件。当使用 5 分钟收集时，必须超过该政策连续六次收集。对于 15 分钟的收集，政策必须仅超出两个收集期。

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 以维护用户身份登录 Unified Manager 主机。

显示 Unified Manager 维护控制台提示。

2. 键入标有“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字，然后按 Enter。

如果您将 Unified Manager 收集间隔更改为 10 或 15 分钟，并且您当前已连接到外部数据提供商（例如 Graphite），则必须更改数据提供商传输间隔，使其等于或大于 Unified Manager 收集间隔。

## 使用工作负载分析器排除工作负载故障

工作负载分析器提供了一种在单个页面上查看单个工作负载的重要健康和性能标准的方法，以协助进行故障排除。通过查看工作负载的所有当前和过去事件，您可以更好地了解工

作负载现在可能存在性能或容量问题的原因。

使用此工具还可以帮助您确定存储是否是导致应用程序性能问题的原因，或者该问题是否是由网络或其他相关问题引起的。

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”选择
- 在事件详细信息页面中单击“分析工作负载”按钮
- 在任何工作负载清单页面（卷、LUN、工作负载、NFS 共享或 SMB/CIFS 共享）中，单击更多图标 ，然后\*分析工作负载\*
- 在虚拟机页面上，单击任意数据存储对象上的“分析工作负载”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，并选择要排除故障的时间范围。当您从任何工作负载或虚拟机清单页面启动该工具时，工作负载的名称将自动填写，并且工作负载的数据将以默认的 2 小时时间范围显示。从事件详情页面启动该工具时，会自动填写工作负载的名称，并显示 10 天的数据。

## 工作负载分析器显示哪些数据

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、可能修复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の图表。

在页面顶部，您可以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，您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 的工作负载图表不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。

### • 活动摘要区

显示一段时间内发生的事件的数量和类型的简要概述。当有来自不同影响领域（例如性能和容量）的事件时，会显示此信息，以便您可以选择感兴趣的事件类型的详细信息。单击事件类型以查看事件名称列表。

如果该时间范围内只有一个事件，则会针对某些事件列出修复该问题的建议列表。

### • 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即可查看事件名称。

如果您通过单击事件详细信息页面上的“分析工作负载”按钮到达此页面，则所选事件的图标将会变得更大，以便您识别该事件。

### • 性能图表区域

根据您选择的时间范围显示延迟、吞吐量（IOPS 和 MB/s）和利用率（节点和聚合）的图表。如果您想进行进一步的分析，可以单击“查看性能详细信息”链接来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。该图表有三种视图，您可以查看：

- \*总\*延迟
- \*细分\*延迟（按读取、写入和其他过程细分）
- \*集群组件\*延迟（按集群组件细分）

看[“集群组件及其争用的原因”](#)有关此处显示的集群组件的描述。吞吐量\*显示所选时间范围内工作负载的 IOPS 和 MB/s 吞吐量。该图表有四种视图，可让您查看：总\*吞吐量 细分\*吞吐量（按读取、写入和其他过程细分）云吞吐量（用于将数据写入云和从云读取数据的 MB/s；适用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计的上限和下限 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），因此您可以看到系统可能在何处使用 QoS 策略有意限制吞吐量。\*利用率\*显示在选定时间范围内运行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

显示过去一个月工作负载的数据容量和快照容量图表。

对于卷，您可以单击查看容量详细信息链接来显示工作负载的运行状况详细信息页面，以便进行进一步的分析。LUN 不提供此链接，因为没有 LUN 的“健康详情”页面。

- \*容量视图\*显示分配给工作负载的总可用空间和逻辑使用空间（经过所有NetApp优化后）。
- **Snapshot View** 显示为 Snapshot 副本保留的总空间以及当前正在使用的空间量。请注意，LUN 不提供快照视图。
- \*云层视图\*显示本地性能层中正在使用的容量以及云层中正在使用的容量。这些图表包括对该工作负载容量满之前的剩余时间的估计。此信息基于历史使用情况，需要至少 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”。

## 我什么时候应该使用工作负载分析器

您通常会使用工作负载分析器来排除用户报告的延迟问题，更彻底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。

如果用户联系您并告知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，以查看存储是否是导致性能问题的原因。您也可以使用容量图表来查看容量是否较低，因为ONTAP系统的容量使用率超过 85% 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网络或其他相关问题引起的。

如果 Unified Manager 生成了性能事件，并且您想要更彻底地检查问题的原因，则可以从事件详细信息页面启动工作负载分析器，方法是单击 **分析工作负载** 按钮来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）时发现工作负载运行异常，您可以单击“更多”图标 ，然后\*分析工作负载\*打开工作负载分析页面，进一步检查工作负载。

## 使用工作负载分析器

有多种方法可以从用户界面启动工作负载分析器。这里我们描述如何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”。
- 将显示“工作负载分析”页面。
2. 如果您知道工作负载名称，请输入该名称。如果您不确定全名，请输入至少 3 个字符，系统将显示与该字符串匹配的工作负载列表。
3. 如果您想查看超过默认 2 小时的统计数据，请选择时间范围，然后单击“应用”。
4. 查看摘要区域以了解该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。

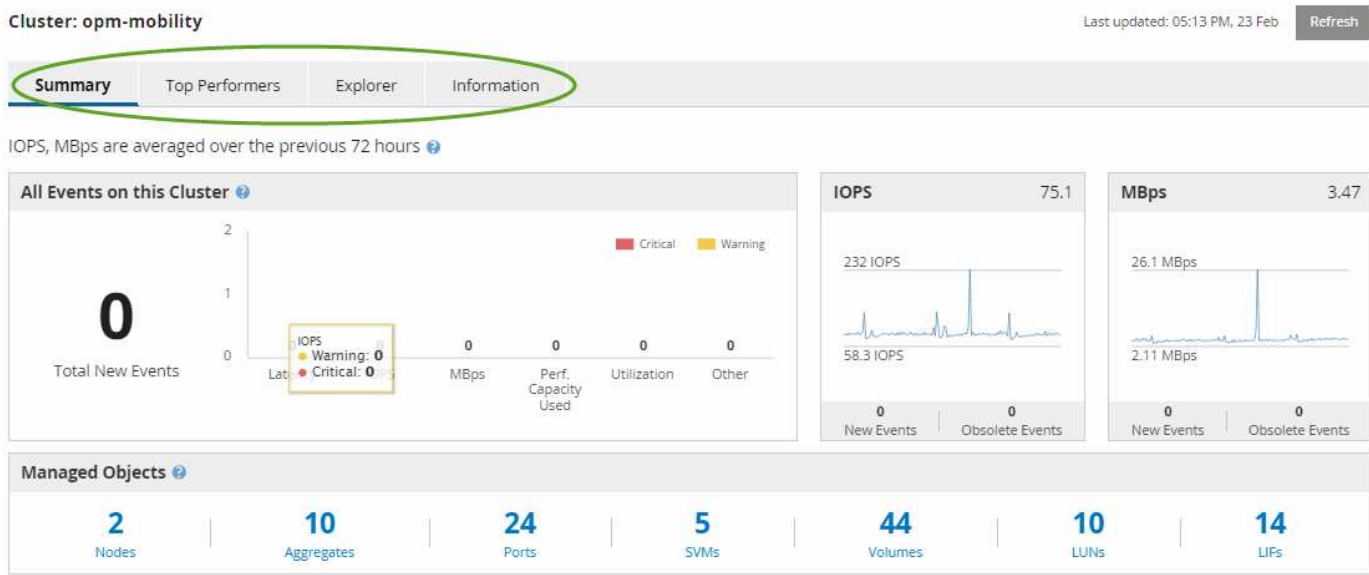
## 从性能集群登录页面监控集群性能

性能集群登录页面显示由 Unified Manager 实例监控的选定集群的高级性能状态。此页面使您能够评估特定集群的整体性能，并快速记录、定位或分配已识别的任何特定于集群的事件以供解决。

### 了解性能集群登陆页面

性能集群登录页面提供了所选集群的高级性能概述，重点关注集群内前 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，并使您能够监控和排除集群故障。下图显示了名为 opm-mobility 的集群的性能集群登录页面的示例：



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”栏中分别显示一个事件，而当违反组合策略时，“性能事件清单”页面仅显示一个事件。



如果集群已从 Unified Manager 的管理中删除，则状态 已删除 将显示在页面顶部的集群名称右侧。

## 性能集群登陆页面

性能集群登录页面显示所选集群的高级性能状态。通过该页面，您可以访问所选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含四个选项卡，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
  - 管理对象窗格
- 最佳表演者页面
- 资源管理器页面
- 信息页面

### 性能集群摘要页面

性能集群摘要页面提供集群的活动事件、IOPS 性能和 MB/s 性能的摘要。此页面还包括集群中存储对象的总数。

#### 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数据 and 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最有用。

#### 此群集窗格上的所有事件

此集群上的所有事件窗格显示前 72 小时内所有活动的集群性能事件。最左侧显示“总活动事件”；此数字代表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“总活动事件”链接导航到“事件清单”页面，该页面经过过滤以显示这些事件。

集群的总活动事件条形图显示活动严重事件和警告事件的总数：

- 延迟（节点、聚合、SVM、卷、LUN 和命名空间的总延迟）
- IOPS（集群、节点、聚合、SVM、卷、LUN 和命名空间的总数）
- MB/s（集群、节点、聚合、SVM、卷、LUN、命名空间、端口和 LIF 的总数）
- 已使用的性能容量（节点和聚合的总容量）
- 利用率（节点、聚合和端口的总数）
- 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。

图表数据（垂直计数器条）显示为红色 (■) 表示关键事件，黄色 (■) 表示警告事件。将光标放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“刷新”来更新计数器面板数据。



您可以通过单击图例中的“严重”和“警告”图标来显示或隐藏“总活动事件”性能图中的严重事件和警告事件。如果隐藏某些事件类型，图例图标将显示为灰色。

## 柜台面板

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，以每秒输入/输出操作数表示。该计数器面板提供了过去 72 小时内集群 IOPS 健康状况的高级概述。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 表示每秒有多少数据以兆字节为单位传输到集群和从集群传输出去。该计数器面板提供了过去 72 小时内集群 MB/s 健康状况的高级概览。您可以将光标放在图形趋势线上以查看特定时间的 MB/s 值。

图表右上角灰色条中的数字是过去 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 小时内活动事件（新事件和已确认事件）和过时事件的数量。

计数器面板包含两种类型的事件：

- 积极的

表示性能事件当前处于活动状态（新的或已确认）。导致该事件的问题尚未自行纠正或尚未解决。存储对象的性能计数器仍然高于性能阈值。

- 过时的

表示该事件不再有效。导致该事件的问题已自行纠正或已解决。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，您可以将光标放在事件图标上，然后单击事件编号以链接到相应的事件详细信息页面。如果有多个事件，您可以单击“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。

## 管理对象窗格

“性能摘要”选项卡中的“管理对象”窗格提供了集群的存储对象类型和数量的顶级概览。此窗格使您能够跟踪每个集群中对象的状态。

管理对象计数是截至上一个收集期的时间点数据。每隔 15 分钟就会发现新物体。

单击任何对象类型的链接数字将显示该对象类型的对象性能清单页面。对象清单页面经过过滤，仅显示此集群上的对象。

管理对象有：

- 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，可以作为单个单元进行管理以进行保护和配置。

- 端口

节点上的物理连接点，用于连接网络上的其他设备。

- 存储虚拟机

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余部分分开管理。

- 卷

通过一个或多个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；但不包括FlexGroup组成部分。

- 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

代表节点的网络接入点的逻辑网络接口。该计数包括所有接口类型。

## 最佳表演者页面

根据您选择的性能计数器，“最佳性能者”页面显示具有最高性能或最低性能的存储对象。例如，在存储虚拟机类别中，您可以显示具有最高 IOPS、最高延迟或最低 MB/s 的 SVM。此页面还显示任何表现最佳者是否有任何活跃的表现事件（新的或已确认的）。

“最佳表现者”页面最多显示每个对象的 10 个。请注意，Volume 对象包括FlexVol卷和FlexGroup卷。

- 时间范围

您可以选择一个时间范围来查看表现最佳的对象；所选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
- 过去 72 小时（默认）
- 过去 7 天

- 公制

单击“**Metric**”菜单以选择不同的计数器。计数器选项对于对象类型来说是唯一的。例如，**Volumes** 对象的可用计数器有 **Latency**、**IOPS** 和 **MB/s**。更改计数器会根据所选计数器重新加载具有最佳表现者的面板数据。

可用计数器：

- 延迟

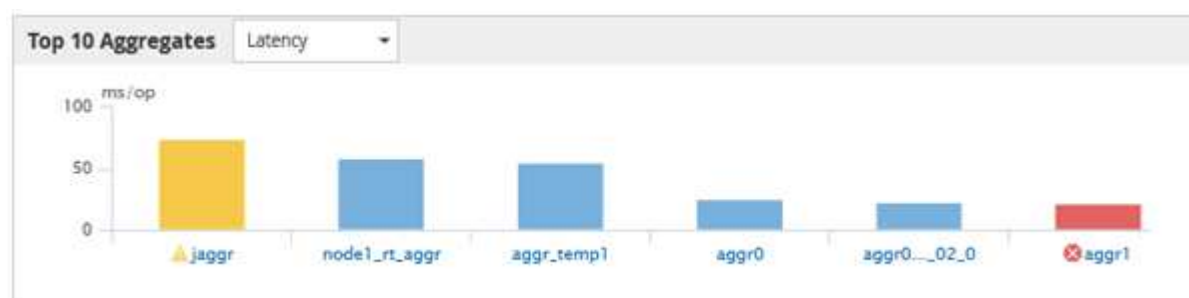
- IOPS
- MB/秒
- 已使用的性能容量（针对节点和聚合）
- 利用率（针对节点和聚合）

- 种类

单击“排序”菜单可为选定的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\*。这些选项使您能够查看性能最高或性能最低的对象。

- 柜台酒吧

图表中的计数器条显示每个对象的性能统计数据，以该项目的条形表示。条形图采用颜色编码。如果计数器未突破性能阈值，则计数器条显示为蓝色。如果阈值突破处于活动状态（新事件或已确认事件），则条形图将以该事件的颜色显示：警告事件以黄色显示（），关键事件显示为红色（）。阈值违规进一步通过警告和严重事件的严重性事件指示图标来指示。



对于每个图表，X 轴显示所选对象类型的最佳表现。Y 轴显示适用于所选计数器的单位。单击每个垂直条形图元素下方的对象名称链接可导航至所选对象的性能登录页面。

- 严重程度事件指示器

严重性事件\*指示图标显示在活动严重事件的对象名称左侧（）或警告（）顶级表演者图表中的事件。单击“\*严重性事件”指示器图标可查看：

- 一项活动

导航至该事件的事件详细信息页面。

- 两个或更多事件

导航到事件清单页面，该页面经过过滤以显示所选对象的所有事件。

- 导出按钮

创建一个`.csv`包含计数器栏中显示的数据的文件。您可以选择为您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

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。

这为您提供了集群内每个对象（例如所有节点或所有卷）性能状态的概览。

对象库存性能页面提供了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、排序和过滤来优化对象库存页面的内容。这在监控和管理对象性能时非常有用，因为它使您能够快速找到具有性能问题的对象并开始故障排除过程。

Nodes - Performance / All Nodes

Last updated: Jan 17, 2019, 7:54 AM

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

View

All Nodes

Search Nodes

| Assign Performance Threshold Policy |        | Clear Performance Threshold Policy |             | Schedule Report |           |                   |                     |             |               |                |                     |
|-------------------------------------|--------|------------------------------------|-------------|-----------------|-----------|-------------------|---------------------|-------------|---------------|----------------|---------------------|
|                                     | Status | Node                               | Latency     | IOPS            | MBps      | Flash Cache Reads | Perf. Capacity Used | Utilization | Free Capacity | Total Capacity | Cluster             |
| <input type="checkbox"/>            |        | ocum-mobility-02                   | 10.2 ms/op  | 18,884 IOPS     | 156 MBps  | N/A               | 81%                 | 35%         | 16.6 TB       | 23.2 TB        | ocum-mobility-01-02 |
| <input checked="" type="checkbox"/> |        | opm-simplicity-01                  | 2.01 ms/op  | 39,358 IOPS     | 153 MBps  | < 1%              | 119%                | 88%         | 4.88 TB       | 18.3 TB        | opm-simplicity      |
| <input type="checkbox"/>            |        | ocum-mobility-01                   | 0.018 ms/op | < 1 IOPS        | 18.2 MBps | N/A               | 23%                 | 18%         | 8.69 TB       | 15.7 TB        | ocum-mobility-01-02 |
| <input type="checkbox"/>            |        | opm-simplicity-02                  | 17 ms/op    | 14,627 IOPS     | 124 MBps  | < 1%              | 29%                 | 20%         | 212 GB        | 5.88 TB        | opm-simplicity      |

默认情况下，性能清单页面上的对象根据对象性能关键性进行排序。具有新的关键性能事件的对象列在最前面，具有警告事件的对象列在后面。这提供了必须解决的问题的直接视觉指示。所有性能数据均基于 72 小时平均值。

您可以通过单击对象名称列中的对象名称，轻松地从对象库存绩效页面导航到对象详细信息页面。例如，在性能/所有节点库存页面上，您可以单击\*节点\*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信息，包括活动事件的并排比较。

查看所有存储对象的性能清单页面

您可以使用性能清单页面查看有关每个可用存储对象（例如集群、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来查看特定对象的详细信息。

默认情况下，视图页面中的对象根据事件严重性进行排序。发生严重事件的对象列在最前面，发生警告事件的对象列在后面。这提供了必须解决的问题的直接视觉指示。

您可以将这些数据从这些页面导出为逗号分隔的值(.csv) 文件、Microsoft Excel 文件(.xlsx) ， 或者(.pdf) 文档，然后使用导出的数据构建报告。此外，您可以自定义页面，然后使用“计划报告”按钮安排定期创建和通过电子邮件发送报告。

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。一些字段链接到相关页面，以便提供更详细的视图。

性能：所有集群视图

性能：所有集群视图显示由 Unified Manager 实例监控的每个集群的性能事件、数据和配置信息概览。此页面使您能够监控集群的性能，并解决性能问题和阈值事件。

您可以使用\*分配性能阈值策略\*和\*清除性能阈值策略\*按钮为对象库存页面上的任何对象分配性能阈值策略或清除阈值策略。

以下是“性能：所有集群”视图中的一些重要字段。

- 集群 FQDN：集群的完全限定域名 (FQDN)。

- IOPS：集群每秒的输入/输出操作数。
- MB/s：集群上的吞吐量，以每秒 MiB 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软件版本。



如果集群中的节点上安装了不同版本的ONTAP软件，则列出最低版本号。您可以从“性能：所有节点”视图查看每个节点上安装的ONTAP版本。

- 阈值策略：在此存储对象上有效的用户定义的性能阈值策略或策略。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已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。

## 性能：所有卷视图

性能：所有卷视图显示由 Unified Manager 实例监控的每个FlexVol volume和FlexGroup卷的性能事件、计数器数据和配置信息概览。这使您能够快速监控卷的性能，并解决性能问题和阈值事件。

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\*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。如果您拥有系统管理器的有效凭证，则可以查看系统管理器上的详细信息。



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。

以下是“性能：所有卷”视图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表示。对于FlexGroup卷，这是所有组成卷的平均延迟。
- IOPS/TB：基于工作负载所消耗的总空间，每秒处理的输入/输出操作数（以 TB 为单位）。该计数器测量给定的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 的总和。
- MB/s：对于FlexVol卷，这是卷上的吞吐量，以每秒兆字节为单位。对于FlexGroup卷，这是所有组成卷的 MB/s 的总和。
- 容量字段：可用容量和总容量（以 GiB 为单位）。

请参阅以下链接以了解更多信息：

- ["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"](#)
- ["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 Unified Manager 将数据分层到云的建议"](#)
- ["查看性能图表以比较同一 QoS 策略组中的卷或 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、数据和配置信息概览。此页面使您能够监控聚合的性能，并解决性能问题和阈值事件。

以下是“性能：所有聚合”视图中的一些重要字段。

- 类型：聚合的类型：
  - HDD
  - 杂交种。结合了 HDD 和 SSD，但尚未启用 Flash Pool。
  - 混合（Flash Pool）。结合了 HDD 和 SSD，并且已启用 Flash Pool。
  - SSD
  - SSD（FabricPool）。结合 SSD 和云层
  - HDD（FabricPool）。结合 HDD 和云层
  - VM磁盘（SDS）。虚拟机内的虚拟磁盘
  - VMDisk（FabricPool）。结合虚拟磁盘和云层
  - LUN (FlexArray)
- 非活动数据报告：此聚合上是否启用或禁用非活动数据报告功能。启用后，此聚合上的卷将在“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：在此存储对象上有效的用户定义的性能阈值策略或策略。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已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。请参阅以下链接以了解更多信息：
- ["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 Unified Manager 实例所监控的每个节点的性能事件、数据和配置信息概览。通过此页面，您可以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的读取操作的百分比，而不是从磁盘返回的。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。

在“报告”菜单中，当 Unified Manager 及其管理的集群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，其中包含集群和节点信息的完整列表；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\*按钮为对象库存页面上的任何对象分配性能阈值策略或清除阈值策略。

请参阅以下链接以了解更多信息：

- ["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签合同"](#)

## 性能：所有存储虚拟机视图

性能：所有存储虚拟机视图显示由 Unified Manager 实例监控的每个存储虚拟机 (SVM) 的性能事件、数据和配置信息概览。这使您能够快速监控 SVM 的性能，并解决性能问题和阈值事件。此页面上的“延迟”字段报告所有 I/O 请求的平均响应时间，以每次操作的毫秒数表示。



此页面上列出的 SVM 仅包括数据 SVM 和集群 SVM。Unified Manager 不使用或显示管理员或节点 SVM。

请参阅以下链接以了解更多信息：

- ["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 视图显示由 Unified Manager 实例监控的每个 LUN 的性能事件、数据和配置信息概览。这使您能够快速监控 LUN 的性能，并排除性能问题和阈值事件的故障。

如果要分析特定对象的延迟和吞吐量，请点击更多图标 ，然后\*分析工作负载\*，您可以在\*工作负载分析\*页面查看性能和容量图表。

请参阅以下链接以了解更多信息：

- ["监控一致性组关系中的 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 预配 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 实例监控的每个 NVMe 命名空间的性能事件、数据和配置信息概览。这使您能够快速监控命名空间的性能和健康状况，并解决问题和阈值事件。

报告的信息包括：命名空间的当前状态。\* 离线 - 不允许对命名空间进行读或写访问。\* 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 - 命名空间已耗尽空间。

请参阅以下链接以了解更多信息：

- ["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此 Unified Manager 实例监控的每个网络接口 (LIF) 的性能事件、数据和配置信息



概览。此页面使您能够快速监控接口的性能，并解决性能问题和阈值事件。以下是“性能：所有网络接口”视图中的的一些重要字段。

- IOPS：每秒的输入/输出操作数。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表示。延迟不适用于 NFS LIF 和 CIFS LIF，并且对于这些类型显示为 N/A。
- 主位置：接口的主位置，显示为节点名称和端口名称，以冒号 (:) 分隔。如果位置显示有省略号 (...), 您可以将光标放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，以冒号 (:) 分隔。如果位置显示有省略号 (...), 您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 Unified Manager 实例正在监控的每个端口的性能事件、数据和配置信息概览。这使您能够快速监控端口的性能，并排除性能问题和阈值事件的故障。对于端口角色，显示网络端口功能，即数据或集群。FCP 端口不能拥有角色，角色显示为 N/A。



仅显示物理端口的性能计数器值。不显示 VLAN 或接口组的计数器值。

请参阅以下链接以了解更多信息：

- ["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 正在监控的集群上可用的 QoS 策略组。这包括传统的 QoS 策略、自适应 QoS 策略和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 策略组：QoS 策略组的名称。对于已导入 Unified Manager 9.7 或更高版本的 NetApp 服务级别管理器 (NSLM) 1.3 策略，此处显示的名称包括 SVM 名称以及在 NSLM 中定义性能服务级别时名称中没有的其他信息。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“性能”PSL 策略，预期延迟为“2 ms/op”。
- SVM：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来导航到该存储虚拟机的详细信息页面。请注意，如果已在管理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代表集群。
- 最小吞吐量：策略组保证提供的最小吞吐量（以 IOPS 为单位）。对于自适应策略，这是根据存储对象分配的大小分配给卷或 LUN 的每 TB 的最小预期 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，表示 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，基于存储对象分配的大小或存储对象使用的大小。



- 绝对最小 IOPS：对于自适应策略，这是绝对最小 IOPS 值，当预期 IOPS 小于此值时，用作覆盖。
- 块大小：为 QoS 自适应策略指定的块大小。
- 最小分配：使用“分配空间”还是“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：对于传统的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量。您可以点击展开按钮（）来查看有关该策略组的更多详细信息。
- 分配容量：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量，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。

更多信息请参阅以下主题["使用 QoS 策略组信息管理性能"](#)。

优化绩效清单页面内容

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，使您能够快速轻松地找到特定数据。

性能对象库存页面中包含的信息可能非常广泛，通常跨越多个页面。这种综合数据非常适合监控、跟踪和提高性能；但是，定位特定数据需要工具来使您能够快速找到您正在寻找的数据。因此，性能对象库存页面包含搜索、排序和过滤功能。此外，搜索和过滤可以协同工作以进一步缩小搜索结果。

在对象库存性能页面上搜索

您可以在对象清单性能页面上搜索字符串。使用位于页面右上角的“搜索”字段可以根据对象名称或策略名称快速定位数据。这使您能够快速找到特定对象及其关联数据，或者快速找到策略并查看关联的策略对象数据。

步骤

1. 根据您的搜索要求，执行以下选项之一：

| 要找到这个...    | 输入此...                                         |
|-------------|------------------------------------------------|
| 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 | 将全部或部分政策名称输入到*搜索*字段中，然后单击*搜索*。将显示分配给您搜索的策略的对象。 |

在对象清单性能页面上排序

您可以按任意列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库存数据，这在检查性能或开始故障排除过程时很有帮助。

选定的要排序的列由突出显示的列标题名称和指示名称右侧排序方向的箭头图标表示。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\*（事件严重性）降序排列，最关键的性能事件列在最前面。

步骤

1. 您可以单击列名来切换列的排序顺序（升序或降序）。

根据所选列，对象清单性能页面内容按升序或降序排序。

过滤对象清单性能页面中的数据

您可以过滤对象清单性能页面中的数据，以便根据特定条件快速找到数据。您可以使用过滤来缩小对象清单性能页面的内容，以仅显示您指定的结果。这提供了一种非常有效的方法，可以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喜好自定义网格视图。可用的过滤选项基于网格中查看的对象类型。如果当前应用了过滤器，则已应用的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参数。

| 参数      | 验证                               |
|---------|----------------------------------|
| 字符串（文本） | 运算符包括*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 <b>is</b> 和 <b>is not</b> 。 |

每个过滤器都需要列、运算符和值字段；可用的过滤器反映当前页面上可过滤的列。您最多可以应用四个过滤器。过滤结果基于组合过滤参数。过滤结果适用于过滤搜索中的所有页面，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“过滤器”按钮。显示过滤面板。
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. 要添加另一个过滤器，请单击“+添加过滤器”。一个额外的筛选字段即会显示。使用上述步骤中所述的过程完成此筛选器。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”。过滤选项应用于网格，过滤器的数量显示在过滤器按钮的右侧。
7. 使用过滤面板通过单击要删除的过滤器右侧的垃圾桶图标来删除单个过滤器。
8. 要删除所有过滤器，请单击过滤面板底部的“重置”。

筛选示例

该图显示了带有三个过滤器的过滤面板。当您拥有的过滤器少于四个时，将显示“+添加过滤器”按钮。

|              |                  |          |      |                                           |
|--------------|------------------|----------|------|-------------------------------------------|
| MBps         | greater than     | 5        | MBps |                                           |
| Node         | name starts with | test     |      |                                           |
| Type         | is               | FCP Port |      |                                           |
| + Add Filter |                  |          |      |                                           |
|              |                  |          |      | <div>Cancel</div> <div>Apply Filter</div> |

单击“应用过滤器”后，“过滤”面板将关闭，应用过滤器，并显示已应用的过滤器数量（ 3 ）。

## 了解 Unified Manager 将数据分层到云的建议

性能：所有卷视图显示与非活动（冷）卷上存储的用户数据大小相关的信息。在某些情况下，Unified Manager 会识别某些卷，这些卷可以通过将非活动数据分层到启用FabricPool的聚合的云层（云提供商或StorageGRID）而受益。



FabricPool是在ONTAP 9.2 中引入的，因此如果您使用的是 9.2 之前的ONTAP软件版本，则 Unified Manager 对分层数据的建议需要升级您的ONTAP软件。此外， **auto** ONTAP 9.4 中引入了分层策略，并且 **all** 分层策略是在ONTAP 9.6 中引入的，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空间的信息。

- 分层政策

分层策略决定卷上的数据是否保留在性能层，或者是否将部分数据从性能层移动到云层。

此字段中的值表示在卷上设置的分层策略，即使该卷当前不驻留在FabricPool聚合上。仅当卷位于FabricPool聚合上时，分层策略才会生效。

- 冷数据

冷数据显示非活动（冷）卷上存储的用户数据的大小。

仅当使用ONTAP 9.4 或更高版本的软件时，此处才会显示值，因为它要求部署卷的聚合具有 **inactive data reporting parameter** 设置为 **enabled**，并且已达到最低冷却天数阈值（对于使用 **snapshot-only** 或者 **auto** 分层策略）。否则，该值将被列为“N/A”。

- 云推荐

在捕获有关卷上的数据活动的足够信息后，Unified Manager 可能会确定不需要采取任何行动，或者您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。



冷数据字段每 15 分钟更新一次，但对卷执行冷数据分析时云推荐字段每 7 天更新一次。因此，不同领域的冷数据的具体数量可能有所不同。云推荐字段显示运行分析的日期。

启用非活动数据报告后，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 将使用性能统计数据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。

您将看到的云建议是：

- 学习。未收集足够的数据以提供建议。
- 等级。分析已确定该卷包含非活动（冷）数据，并且您应该配置该卷以将该数据移动到云层。在某些情况下，这可能要求您首先将卷移动到启用FabricPool的聚合。在其他情况下，如果卷已经位于FabricPool聚合上，您只需更改分层策略。
- 无动作。该卷具有非常少的非活动数据，该卷已设置为FabricPool聚合上的“自动”分层策略，或者该卷是数据保护卷。当卷处于脱机状态或在MetroCluster配置中使用，也会显示此值。

要移动卷、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。

如果您以应用程序管理员或存储管理员角色登录到 Unified Manager，则将光标悬停在单词 **Tier** 上时，云推荐中会出现 **Configure Volume** 链接。单击此按钮可打开系统管理器中的卷页面以进行建议的更改。

## 使用性能资源管理器页面监视性能

性能资源管理器页面显示有关集群中每个对象的性能的详细信息。该页面提供了所有集群对象性能的详细视图，使您可以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。

### 了解根对象

根对象是与其他对象进行比较的基线。这使您能够查看和比较来自其他对象的数据与根对象的数据，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。附加对象显示在根对象下方。尽管可以添加到比较窗格的附加对象的数量没有限制，但只允许一个根对象。根对象的数据会自动显示在计数器图表窗格中的图表中。

您无法更改根对象；它始终设置为您正在查看的对象页面。例如，如果您打开 Volume1 的 Volume Performance Explorer 页面，则 Volume1 是根对象，无法更改。如果您想与不同的根对象进行比较，那么您必须单击对象的链接并打开其登录页面。



仅显示根对象的事件和阈值。

### 应用过滤来减少网格中相关对象的列表

通过过滤，您可以在网格中显示更小、定义更明确的对象子集。例如，如果网格中有 25 个卷，则通过过滤，您可以仅查看吞吐量小于 90 MBps 或延迟大于 1 ms/op 的卷。

### 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

间范围可优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有效的方法，可以仅显示您感兴趣的性能数据。您可以选择预定义的时间范围或指定自定义时间范围。默认时间范围是前 72 小时。

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集中数据输出的快速有效方法。选择预定义的时间范围时，可以使用长达 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”。

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。

您可以选择一小时到 390 天之间的时间范围。13 个月等于 390 天，因为每个月算 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的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可以更详细地显示性能事件周围的数据。使用\*时间范围\*控件选择预定义的日期和时间范围，或指定您自己的自定义日期和时间范围（最长 390 天）。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”选项或指定超过 30 天的自定义日期范围将显示一个对话框，提醒您超过 30 天的时间段内显示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，可能会出现时间线视觉粒度的损失。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，不会出现该消息。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。超过 30 天的时间范围基于一小时间隔的数据样本。

From

< April 2015 >

| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|-----|-----|-----|-----|-----|-----|-----|
| 29  | 30  | 31  | 01  | 02  | 03  | 04  |
| 05  | 06  | 07  | 08  | 09  | 10  | 11  |
| 12  | 13  | 14  | 15  | 16  | 17  | 18  |
| 19  | 20  | 21  | 22  | 23  | 24  | 25  |
| 26  | 27  | 28  | 29  | 30  | 01  | 02  |
| 03  | 04  | 05  | 06  | 07  | 08  | 09  |

Time: 6:00 am

< April 2015 >

| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|-----|-----|-----|-----|-----|-----|-----|
| 29  | 30  | 31  | 01  | 02  | 03  | 04  |
| 05  | 06  | 07  | 08  | 09  | 10  | 11  |
| 12  | 13  | 14  | 15  | 16  | 17  | 18  |
| 19  | 20  | 21  | 22  | 23  | 24  | 25  |
| 26  | 27  | 28  | 29  | 30  | 01  | 02  |
| 03  | 04  | 05  | 06  | 07  | 08  | 09  |

Time: 6:00 am

Last Hour

Last 24 Hours

Last 72 Hours

Last 7 Days

Last 30 Days

Last 13 Months

Custom Range

Cancel

Apply Range

- 1. 单击“时间范围”下拉框，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，可以使用长达 13 个月的数据。选定的预定义时间范围按钮会突出显示，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“从”日历中的开始日期。单击 < 或 > 可在日历中向前或向后导航。要指定结束日期，请单击右侧“至”日历中的日期。请注意，除非指定其他结束日期，否则默认结束日期是今天。时间范围面板右侧的“自定义范围”按钮突出显示，表明您已选择自定义日期范围。
- 4. 要选择自定义时间范围，请单击“从”日历下方的“时间”控件并选择开始时间。要指定结束时间，请单击右侧“至”日历下方的“时间”控件，然后选择结束时间。时间范围面板右侧的“自定义范围”按钮突出显示，表示您已选择自定义时间范围。
- 5. 或者，也可以在选择预定义的日期范围时指定开始时间和结束时间。如前所述选择预定义的日期范围，然后如前所述选择开始时间和结束时间。选定的日期在日历中突出显示，您指定的开始和结束时间显示在\*时间\*控件中，并且\*自定义范围\*按钮突出显示。
- 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数据显示在图表和事件时间线中。

定义用于比较图表的相关对象列表

您可以在计数器图表窗格中定义相关对象的列表，以进行数据和性能比较。例如，如果您的存储虚拟机 (SVM) 遇到性能问题，您可以比较 SVM 中的所有卷以确定哪个卷可能导致该问题。

您可以将相关对象网格中的任何对象添加到比较和计数器图表窗格。这使您可以查看和比较多个对象以及根对象的数据。您可以在相关对象网格中添加和删除对象；但是，比较窗格中的根对象是不可删除的。



向比较窗格添加许多对象可能会对性能产生负面影响。为了保持性能，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。  
  
\*添加\*按钮变为灰色，并且该对象被添加到比较窗格中的附加对象列表中。对象的数据被添加到计数器图表窗格中的图表中。对象的眼睛图标的颜色 (  ) 与图表中对象数据趋势线的颜色相匹配。
- 2. \*可选：\*隐藏或显示选定对象的数据：

| 要做到这一点... | 采取此行动...                                                                                                                               |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------|
| 隐藏选定的对象   | 单击所选对象的眼睛图标 (  ) 在比较窗格中。该对象的数据被隐藏，并且该对象的眼睛图标变为灰色。 |
| 显示隐藏的对象   | 单击比较窗格中所选对象的灰色眼睛图标。<br><br>眼睛图标恢复其原始颜色，并且对象数据被重新添加至计数器图表窗格中的图表中。                                                                       |

- 3. \*可选：\*从\*比较\*窗格中删除选定的对象：



| 要做到这一点... | 采取此行动...                                                                       |
|-----------|--------------------------------------------------------------------------------|
| 移除选定的对象   | 将鼠标悬停在比较窗格中选定对象的名称上以显示删除对象按钮（ <b>X</b> ），然后单击该按钮。该对象将从比较窗格中删除，并且其数据将从计数器图表中清除。 |
| 移除所有选定的对象 | 单击比较窗格顶部的删除所有对象的按钮（ <b>X</b> ）。所有选定的对象及其数据都将被删除，只留下根对象。                        |

## 了解计数器图表

计数器图表窗格中的图表使您能够查看和比较根对象和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是事件、延迟、IOPS 和 MBps。您可以选择显示的可选图表包括利用率、已用性能容量、可用 IOPS、IOPS/TB 和缓存未命中率。此外，您还可以选择查看延迟、IOPS、MBps 和已用性能容量图表的总值或细分值。

性能资源管理器默认显示某些计数器图表；无论存储对象是否全部支持它们。当计数器不受支持时，计数器图表为空，并且消息 `Not applicable for <object>` 将显示。

图表显示根对象和您在比较窗格中选择的所有对象的性能趋势。各图表数据排列如下：

- **X轴**

显示指定的时间段。如果您未指定时间范围，则默认为前 72 小时。

- **Y轴**

显示选定对象或对象独有的计数器单位。

趋势线颜色与比较窗格中显示的对象名称颜色相匹配。您可以将光标放在任何趋势线上的某个点上，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，可以使用以下方法之一：

- 使用 < 按钮展开计数器图表窗格以跨越页面宽度。
- 使用光标（当它变为放大镜时）选择图表中时间范围的一部分来聚焦和放大该区域。您可以单击“重置图表缩放”将图表恢复到默认时间范围。
- 使用“缩放视图”按钮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。



有时，趋势线会出现缺口。差距意味着 Unified Manager 无法从存储系统收集性能数据，或者 Unified Manager 可能已关闭。

## 性能计数器图表的类型

有标准性能图表显示所选存储对象的计数器值。每个细分计数器图表显示分为读取、写入

和其他类别的总值。此外，当图表以缩放视图显示时，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      | 图表描述                                                                                                                                                                                                                                                 |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 事件        | 显示与根对象的统计图表相关的严重、错误、警告和信息事件。除了性能事件之外，还显示健康事件，以提供性能可能受到影响的原因的完整情况。                                                                                                                                                                                    |
| 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   | “延迟总计”中显示相同的信息，但性能数据分为读取、写入和其他延迟。仅当选定的对象是 SVM、节点、聚合、卷、LUN 或命名空间时，此图表选项才适用。                                                                                                                                                                           |
| 延迟 - 集群组件 | “延迟总计”中显示相同的信息，但性能数据按集群组件分为延迟。此图表选项仅当选定对象为体积时才适用。                                                                                                                                                                                                    |
| IOPS - 总计 | 每秒处理的输入/输出操作数。当显示某个节点时，选择“总计”将显示通过此节点移动的数据的 IOPS，这些数据可能驻留在本地或远程节点上，而选择“总计（本地）”将显示仅驻留在当前节点上的数据的 IOPS。                                                                                                                                                 |
| IOPS - 细分 | <p>IOPS Total 中显示相同的信息，但性能数据分为读取、写入和其他 IOPS。仅当选定的对象是 SVM、节点、聚合、卷、LUN 或命名空间时，此图表选项才适用。</p> <p>当在缩放视图中显示时，卷图表会显示 QoS 最小和最大吞吐量值（如果在 ONTAP 中配置）。</p> <p>当显示某个节点时，选择“细分”将显示通过此节点移动的数据的 IOPS 细分，这些数据可能驻留在本地或远程节点上，而选择“细分（本地）”将显示仅驻留在当前节点上的数据的 IOPS 细分。</p> |
| IOPS - 协议 | IOPS Total 中显示相同的信息，但性能数据分为 CIFS、NFS、FCP、NVMe 和 iSCSI 协议流量的单独图表。此图表选项仅当选定的对象是 SVM 时才适用。                                                                                                                                                              |



| 可用图表         | 图表描述                                                                                                                                                                                                                                                                                                           |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IOPS/TB - 总计 | <p>根据工作负载所占用的总空间，每秒处理的输入/输出操作数（以 TB 为单位）。该计数器也称为 I/O 密度，用于衡量给定存储容量可以提供多少性能。如果在 ONTAP 中配置，则在缩放视图中显示卷图表会显示 QoS 预期值和峰值吞吐量值。</p> <p>此图表选项仅当选定对象为体积时才适用。</p>                                                                                                                                                        |
| MB/秒 - 总计    | 每秒传输到对象和从对象传输的数据（兆字节数）。                                                                                                                                                                                                                                                                                        |
| MB/秒 - 细分    | <p>MB/s 图表中显示相同的信息，但吞吐量数据分为磁盘读取、闪存读取、写入和其他。当在缩放视图中显示时，卷图表会显示 QoS 最大吞吐量值（如果在 ONTAP 中配置）。</p> <p>仅当选定的对象是 SVM、节点、聚合、卷、LUN 或命名空间时，此图表选项才适用。</p> <div>  <p>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。</p> </div> |
| 已用性能容量 - 总计  | 节点或聚合所消耗的性能容量百分比。                                                                                                                                                                                                                                                                                              |
| 已用性能容量 - 细分  | 性能容量使用的数据分为用户协议和系统后台进程。此外，还显示了可用的性能容量。                                                                                                                                                                                                                                                                         |
| 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 计算的对象可以执行的总 IOPS 中减去当前使用的 IOPS 的结果。仅当选定的对象是节点或聚合时，此图表选项才适用。                                                                                                                                                                                                      |
| 利用率 - 总计     | 正在使用的对象的可用资源百分比。利用率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。此图表选项仅当选定的对象是节点、聚合或端口时才适用。                                                                                                                                                                                                                                     |
| 缓存未命中率 - 总计  | 来自客户端应用程序的读取请求中从磁盘返回而不是从缓存返回的百分比。此图表选项仅当选定对象为体积时才适用。                                                                                                                                                                                                                                                           |

## 选择要显示的性能图表

通过“选择图表”下拉列表，您可以选择要在“计数器图表”窗格中显示的性能计数器图表的类型。这使您能够根据性能要求查看特定的数据和计数器。

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 |
| 添加所有图表    | 点击“全选”            |
| 删除所有图表    | 点击*取消全选*          |

您选择的图表将显示在计数器图表窗格中。请注意，当您添加图表时，新图表将插入到“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的顺序。选择其他图表可能需要额外滚动。

展开计数器图表窗格

您可以展开计数器图表窗格，以便图表更大且更易读。

定义计数器的比较对象和时间范围后，您可以查看更大的计数器图表窗格。您可以使用性能资源管理器窗口中间的 < 按钮来展开窗格。

步骤

- 1. 展开或缩小\*计数器图表\*窗格。

| 目的                 | 操作      |
|--------------------|---------|
| 扩展计数器图表窗格以适合页面宽度   | 点击 < 按钮 |
| 将计数器图表窗格缩小到页面的右半部分 | 点击 > 按钮 |

将计数器图表焦点更改为较短的时间段

您可以使用鼠标缩小时间范围，以在计数器图表窗格或计数器图表缩放视图窗口中关注特定时间段。这使您能够更细致、更微观地查看性能数据、事件和阈值的时间线的任何部分。

开始之前

光标必须变为放大镜才能表明此功能处于活动状态。



当使用此功能时，它会改变时间线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变化。

步骤

- 1. 要放大特定时间段，请使用放大镜单击并拖动鼠标以突出显示您想要详细查看的区域。

您选择的时间段内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。

### 在事件时间线中查看事件详细信息

您可以在性能资源管理器的事件时间线窗格中查看所有事件及其相关详细信息。这是一种快速有效的方法，可以查看指定时间范围内根对象上发生的所有健康和性能事件，这在解决性能问题时很有帮助。

事件时间线窗格显示在选定时间范围内在根对象上发生的关键、错误、警告和信息事件。每个事件严重程度都有其自己的时间表。单个事件和多个事件由时间线上的事件点表示。您可以将光标放在事件点上以查看事件详细信息。为了增加多个事件的视觉粒度，您可以减小时间范围。这会将多个事件分散为单个事件，使您能够单独查看和调查每个事件。

事件时间线上的每个性能事件点与事件时间线下方显示的计数器图表趋势线中的相应峰值垂直排列。这提供了事件和整体表现之间的直接视觉关联。健康事件也会显示在时间线上，但这些类型的事件不一定与性能图表之一的峰值一致。

#### 步骤

- 1. 在“事件时间线”窗格上，将光标放在时间线上的事件点上，以查看该事件点的事件摘要。

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情：

| 要做到这一点...   | 单击此处...                                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 查看单个事件的详细信息 | 在弹出对话框中*查看事件详情*。                                                                                                                                   |
| 查看多个事件的详细信息 | <div><div></div><div>单击多个事件对话框中的单个事件将显示相应的事件详细信息页面。</div></div> |

### 计数器图表缩放视图

计数器图表提供缩放视图，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，这在解决性能问题时非常有用。

当以缩放视图显示时，某些细分图表会提供比图表未以缩放视图显示时显示的信息更多的信息。例如，如果已在ONTAP中设置了卷和 LUN 的 QoS 策略值，则 IOPS、IOPS/TB 和 MBps 细分图表缩放视图页面将显示这些值。



对于系统定义的性能阈值策略，\*策略\*列表中只有“节点资源过度利用”和“QoS 吞吐量限制突破”策略可用。其他系统定义的阈值策略目前不可用。

显示计数器图表缩放视图

计数器图表缩放视图为所选计数器图表及其相关时间线提供了更精细的细节。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根本原因。

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”，细分图表将以缩放视图显示。如果您想更改视图选项，可以在“缩放视图”中选择“总计”。

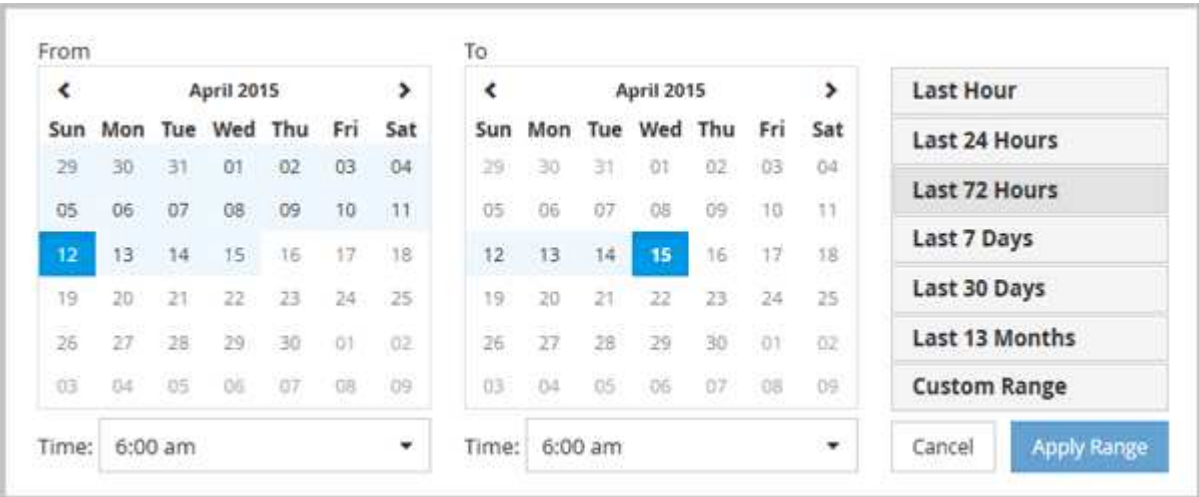
在缩放视图中指定时间范围

计数器图表缩放视图窗口中的“时间范围”控件使您能够为所选图表指定日期和时间范围。这使您能够根据预设的时间范围或您自己的自定义时间范围快速找到特定数据。

您可以选择一小时到 390 天之间的时间范围。13 个月等于 390 天，因为每个月算 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的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可以更详细地显示性能事件周围的数据。使用\*时间范围\*控件选择预定义的日期和时间范围，或指定您自己的自定义日期和时间范围（最长 390 天）。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”选项或指定超过 30 天的自定义日期范围将显示一个对话框，提醒您超过 30 天的时间段内显示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，可能会出现时间线视觉粒度的损失。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，不会出现该消息。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。超过 30 天的时间范围基于一小时间隔的数据样本。



- 1. 单击“时间范围”下拉框，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，可以使用长达 13 个月的数据。选定的预定义时间范围按钮会突出显示，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“从”日历中的开始日期。单击 < 或 > 可在日历中向前或向后导航。要指定结束日期，请单击右侧“至”日历中的日期。请注意，除非指定其他结束日期，否则默认结束日期是今天。时间范围面板右侧的“自定义范围”按钮突出显示，表明您已选择自定义日期范围。
4. 要选择自定义时间范围，请单击“从”日历下方的“时间”控件并选择开始时间。要指定结束时间，请单击右侧“至”日历下方的“时间”控件，然后选择结束时间。时间范围面板右侧的“自定义范围”按钮突出显示，表示您已选择自定义时间范围。
5. 或者，也可以在选择预定义的日期范围时指定开始时间和结束时间。如前所述选择预定义的日期范围，然后如前所述选择开始时间和结束时间。选定的日期在日历中突出显示，您指定的开始和结束时间显示在\*时间\*控件中，并且\*自定义范围\*按钮突出显示。
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数据显示在图表和事件时间线中。

在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进行故障排除时很有帮助。

在计数器图表缩放视图中选择阈值使您能够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的\*策略\*区域下出现的任何阈值。

每次只能将一个策略应用于计数器图表缩放视图中的对象。

步骤

1. 选择或取消选择  与政策相关的。

所选阈值将应用于计数器图表缩放视图。临界阈值显示为红线；警告阈值显示为黄线。

## 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。延迟 - 总计数器图表显示卷上的总延迟，延迟 - 细分计数器图表有助于确定读写延迟对卷的影响。

此外，“延迟 - 集群组件”图表显示了每个集群组件的延迟的详细比较，以帮助确定每个组件对卷的总延迟的贡献。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. 在您选择的卷的“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”。

显示延迟 - 集群组件图表。

2. 要查看图表的较大版本，请选择“缩放视图”。

显示集群组件比较图。您可以通过取消选择或选择  与每个集群组件相关联的。

3. 要查看具体值，请将光标移到图表区域以查看弹出窗口。

### 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 - 细分计数器图表有助于确定读取、写入和其他 IOPS 对 SVM 的影响。

此外，IOPS - 协议图表显示了 SVM 上使用的每种协议的 IOPS 流量的详细比较。可以使用以下协议：

- CIFS
- NFS
- FCP
- iSCSI
- NVMe光纤通道

#### 步骤

1. 在您选择的 SVM 的“性能/SVM 资源管理器”页面中，从 IOPS 图表的下拉菜单中选择“协议”。

显示 IOPS - 协议图表。

2. 要查看图表的较大版本，请选择“缩放视图”。

显示IOPS高级协议对比图。您可以通过取消选择或选择  与协议相关。

3. 要查看具体值，请将光标移到任一图表的图表区域以查看弹出窗口。

### 查看卷和 LUN 延迟图表以验证性能保证

您可以查看已订阅“性能保证”计划的卷和 LUN，以验证延迟是否未超过您所保证的水平。

延迟性能保证是每次操作一毫秒的值，不应超过该值。它基于每小时平均值，而不是默认的五分钟性能收集期。

#### 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 查看统计信息 选择器中选择 每小时平均值。

随着五分钟收集的数据被每小时平均值取代，延迟图表中的水平线将显示更平滑的线。

3. 如果同一聚合上还有其他卷处于性能保证之下，则可以添加这些卷以在同一图表中查看其延迟值。

## 查看所有 SAN 阵列集群的性能

您可以使用性能：所有集群视图来显示所有 SAN 阵列集群的性能状态。

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”视图中查看所有 SAN 阵列集群的概述信息，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“个性”列显示在\*健康：所有集群\*视图中，或使用\*显示/隐藏\*控件添加它。

此列显示您的所有 SAN 阵列集群的“所有 SAN 阵列”。

3. 要查看有关这些集群的性能信息，请选择“性能：所有集群”视图。

查看全 SAN 阵列群集的性能信息。

4. 要查看有关这些集群的性能的详细信息，请单击所有 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数据，以确保两个节点上的负载几乎相同。如果两个节点之间存在很大差异，您可以将第二个节点添加到图表中，并比较较长时间范围内的值以识别任何配置问题。

## 根据仅驻留在本地节点上的工作负载查看节点 IOPS

节点 IOPS 计数器图表可以突出显示操作仅通过本地节点使用网络 LIF 对远程节点上的卷执行读/写操作的位置。IOPS - “总计（本地）”和“细分（本地）”图表显示仅驻留在当前节点上的本地卷中的数据的 IOPS。

这些计数器图表的“本地”版本与性能容量和利用率率的节点图表类似，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“本地”版本与这些计数器图表的常规总版本进行比较，您可以看到是否有大量流量通过本地节点移动以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，可能表现为节点利用率高。在这些情况下，您可能希望将卷移动到本地节点，或者在远程节点上创建 LIF，以便可以连接访问该卷的主机的流量。

步骤

1. 在所选节点的“性能/节点资源管理器”页面中，从 IOPS 图表的下拉菜单中选择“总计”。



显示 IOPS - 总计图表。

- 2. 单击“缩放视图”可在新浏览器选项卡中显示图表的较大版本。
- 3. 返回“性能/节点资源管理器”页面，从 IOPS 图表的下拉菜单中选择“总计（本地）”。

显示 IOPS - 总计（本地）图表。

- 4. 单击“缩放视图”可在新浏览器选项卡中显示图表的较大版本。
- 5. 查看两个图表并排查看，并确定 IOPS 值看起来差异很大的区域。
- 6. 将光标移到这些区域上，以比较特定时间点的本地和总 IOPS。

对象登陆页面的组件

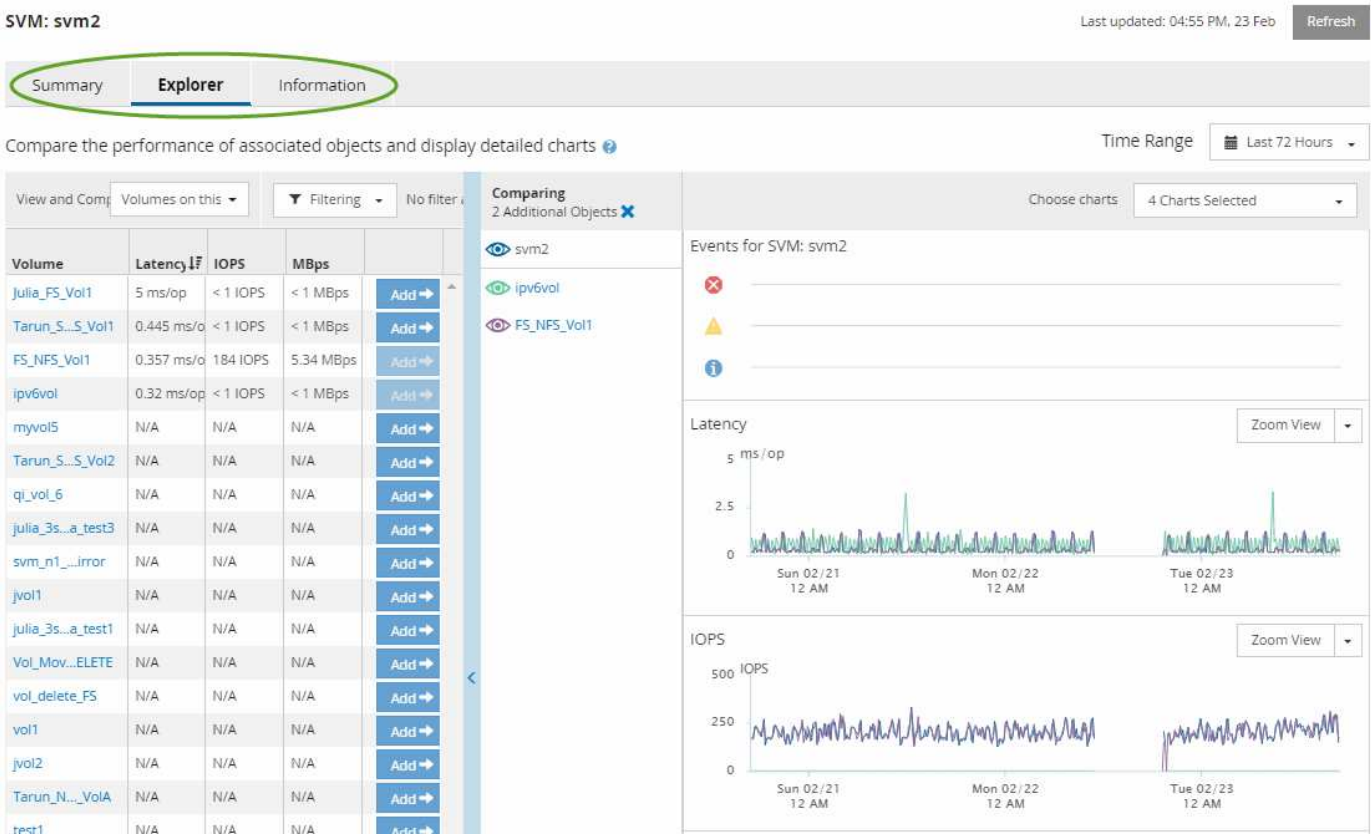
对象登陆页面提供有关所有关键、警告和信息事件的详细信息。它们提供了所有集群对象性能的详细视图，使您能够选择和比较不同时间段内的单个对象。

对象登录页面使您能够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，对象登录页面可以包含以下选项卡，提供有关该对象的性能数据：



- 摘要

显示三个或四个计数器图表，其中包含前 72 小时内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。此选项卡包含最多 11 个计数器图表和一个时间范围选择器，可让您执行各种比较。

- 信息

显示有关存储对象的非性能配置属性的值，包括已安装的ONTAP软件版本、HA 合作伙伴名称以及端口和 LIF 的数量。

- 性能最佳的对象

对于集群：根据您选择的性能计数器，显示具有最高性能或最低性能的存储对象。

- 故障转移规划

对于节点：显示如果节点的 HA 伙伴发生故障，对节点性能造成的影响的估计。

- 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卷和 FlexGroups 的组成部分。

## 摘要页面

摘要页面显示计数器图表，其中包含前 72 小时内每个对象的事件和性能的详细信息。该数据不会自动刷新，但截至上次页面加载时是最新数据。摘要页面中的图表回答了“我需要进一步了解吗？”这个问题

### 图表和计数器统计

摘要图表提供了过去 72 小时内的快速、高级概览，并帮助您识别可能需要进一步调查的问题。

摘要页面计数器统计信息以图表形式显示。

您可以将光标放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前 72 小时内的活动严重和警告事件的总数：

- 延迟

所有 I/O 请求的平均响应时间；以每次操作的毫秒数表示。

显示所有对象类型。

- 每秒输入/输出次数

平均运行速度；以每秒的输入/输出操作表示。

显示所有对象类型。

• **MB/秒**

平均吞吐量；以每秒兆字节表示。

显示所有对象类型。

• **已使用的性能容量**

节点或聚合所消耗的性能容量百分比。

仅对节点和聚合显示。

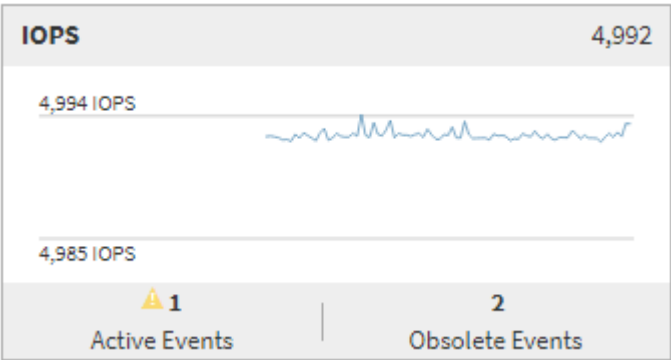
• **利用率**

节点和聚合的对象利用率百分比，或端口的带宽利用率。

仅显示节点、聚合和端口。

将光标定位在活动事件的事件计数上会显示事件的类型和数量。关键事件以红色显示 (■)，警告事件显示为黄色 (■)。

图表右上角灰色条中的数字是过去 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 小时内活动事件（新事件和已确认事件）和过时事件的数量。



• **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览。延迟是指所有 I/O 请求的平均响应时间；（以每操作毫秒数为单位表示）相关集群存储组件中数据包或块经历的服务时间和（或）等待时间。

\*顶部（计数器值）：\*标题中的数字显示前 72 小时的平均值。

\*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。将光标置于图形趋势线上方可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，导航至“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 健康状况的高级概览。IOPS 表示存储系统的速度，以每秒输入/输出操作数为单位。

\*顶部（计数器值）：\*标题中的数字显示前 72 小时的平均值。

\*中间（性能图）：\*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。将光标置于图形趋势线上方可查看特定时间的 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，导航至“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 MB/s 性能，并指示每秒有多少数据以兆字节为单位传输到对象和从对象传输出去。MB/s 计数器图表提供了前 72 小时内对象 MB/s 健康状况的高级概览。

\*顶部（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 小时内最高的 MB/s 数。将光标置于此图形趋势线上方可查看特定时刻的 MB/秒数值。

\*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，导航至“事件清单”页面以查看完整的事件详细信息。

- **性能容量已用计数器图表**

已用性能容量计数器图表显示对象所消耗的性能容量百分比。

\*顶部（计数器值）：\*标题中的数字显示前 72 小时内平均使用的性能容量。

\*中间（性能图）：\*图表底部的值显示最低使用的性能容量百分比，图表顶部的值显示前 72 小时内最高的使用的性能容量百分比。将光标置于图形趋势线上方可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，导航至“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高级概览。

\*顶部（计数器值）：\*标题中的数字显示前 72 小时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。将光标置于图形趋势线上方可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，导航至“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。单击事件名称可在“事件详细信息”页面上显示该事件的详细信息。

通过“性能资源管理器”页面，您可以比较集群中类似对象的性能 - 例如，集群中的所有卷。这在排除性能事件故障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线。

您可以单击“切换到健康视图”按钮来显示此对象的健康详细信息页面。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，这可能有助于解决问题。

性能资源管理器页面显示集群对象及其性能数据的列表。此页面以表格形式显示同一类型的所有集群对象（例如，卷及其特定于对象的性能统计信息）。此视图提供了集群对象性能的有效概览。



如果表格中的任何单元格中出现“N/A”，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

使您能够选择对象数据的时间范围。

您可以选择预定义的范围，或指定您自己的自定义时间范围。

- 查看并比较

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。

- 过滤

使您能够根据自己的喜好缩小接收的数据量。

您可以创建适用于对象数据的过滤器 - 例如，IOPS 大于 4。您最多可以同时添加四个过滤器。

- 比较

显示您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。

- 查看统计数据

对于卷和 LUN，您可以选择是否在每个收集周期（默认 5 分钟）后显示统计信息，或者是否以每小时平均值的形式显示统计信息。此功能使您能够查看支持 NetApp “性能保证”计划的延迟图表。

- 反图表

显示每个对象性能类别的图形数据。

通常，默认仅显示三到四个图表。选择图表组件使您能够显示其他图表或隐藏特定图表。您还可以选择显示

或隐藏事件时间线。

- 事件时间表

显示您在时间范围组件中选择的时间线上发生的性能和健康事件。

## 使用 QoS 策略组信息管理性能

Unified Manager 使您能够查看您正在监控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（系统管理器或 ONTAP CLI）或 Unified Manager 性能服务级别策略定义。Unified Manager 还显示哪些卷和 LUN 分配了 QoS 策略组。

有关调整 QoS 设置的更多信息，请参阅 ["绩效管理概述"](#)

### 存储 QoS 如何控制工作负载吞吐量

您可以创建服务质量 (QoS) 策略组来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（例如默认策略组）中，或者设置的限制不能满足您的需求，您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，工作负载可以使用全部吞吐量限制。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，分配给三个工作负载的 QoS 限制为 9,000 IOPS，这将限制合并后的 IOPS 不能超过 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，从而随着卷大小的变化保持 IOPS 与 TB 的比率。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 卷的最大吞吐量将为 50,000 IOPS。如果稍后将卷大小调整为 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。当工作负载使用非常大的块大小并最终使用大量吞吐量时，这可以有效地将策略从 IOPS/TB 阈值转换为 MB/s 阈值。

对于共享组 QoS 策略，当策略组中所有工作负载的 IOPS 或 MB/s 超过设定的限制时，策略组会限制工作负载以限制其活动，这会降低策略组中所有工作负载的性能。如果动态性能事件是由策略组限制生成的，则事件描述会显示所涉及的策略组的名称。

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，可能导致该事件。在性能/卷资源管理器页面中，您可以选择其他卷或卷上的 LUN，以与受影响的工作负载 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，策略组可以限制工作负载以限制其活动，从而减少该节点上资源的使用。但是，如果您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
- 将工作负载移动到不同的聚合和/或节点

## 查看所有集群上可用的所有 QoS 策略组

您可以显示 Unified Manager 正在监控的集群上可用的所有 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”。

默认情况下显示“性能：传统 QoS 策略组”视图。

2. 查看每个可用的传统 QoS 策略组的详细配置设置。
3. 单击展开按钮 (▼) 来查看有关该策略组的更多详细信息。
4. 在“查看”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。

## 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“共享”的传统 QoS 策略组，这有助于查看某些卷是否过度使用了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，这有助于查看使用策略组的所有卷或 LUN，以便您可以看到如果更改 QoS 策略的配置设置，哪些对象会受到影响。

### 步骤

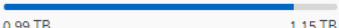
1. 在左侧导航窗格中，单击“存储”>“QoS 策略组”。

默认情况下显示“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，选择其中一个附加查看选项以显示所有自适应 QoS 策略组或由 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，单击展开按钮 (▼) 来查看更多详细信息。

View Adaptive QoS Policy Groups Search Quality of Service

Schedule Report

| QoS Policy Group                                                                                                                                                                                    | Cluster             | SVM               | Min Through...  | Max Through...  | Absolute Min... | Block Size | Asso |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|-------------------|-----------------|-----------------|-----------------|------------|------|
| ▼ julia_vs2_cifs_Performance                                                                                                                                                                        | opm-simplicity      | julia_vs2_cifs    | 2048.0 IOPS/TB  | 4096.0 IOPS/TB  | 500IOPS         |            | 1    |
| ▲ julia_vs1_nfs_Performance                                                                                                                                                                         | opm-simplicity      | julia_vs1_nfs     | 2048.0 IOPS/TB  | 4096.0 IOPS/TB  | 500IOPS         |            | 2    |
| <b>Details</b><br>Allocated Capacity  0.99 TB 1.15 TB<br>Associated Objects <b>2 Volumes</b> 0 LUNs<br>Events None |                     |                   |                 |                 |                 |            |      |
| ▼ julia_nfs_extreme_Extreme_Performance                                                                                                                                                             | ocum-mobility-01-02 | julia_nfs_extreme | 6144.0 IOPS/TB  | 12288.0 IOPS/TB | 1000IOPS        | any        | 1    |
| ▼ julia_extreme_jan16_aqos                                                                                                                                                                          | ocum-mobility-01-02 | julia_nfs_extreme | 10000.0 IOPS/TB | 12000.0 IOPS/TB | 1000IOPS        | any        | 1    |

4. 单击卷或 LUN 链接以查看使用此 QoS 策略的对象。

卷或 LUN 的性能清单页面显示使用 QoS 策略的对象的排序列表。

## 查看应用于特定卷或 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，并且可以链接到性能/QoS 策略组视图以显示每个 QoS 策略的详细配置设置。

查看应用于卷的 QoS 策略的步骤如下所示。查看 LUN 的此信息的步骤类似。

### 步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。

默认情况下显示“健康状况：所有卷”视图。

2. 在“查看”菜单中，选择“性能：QoS 策略组中的卷”。

3. 找到您要查看的卷并向右滚动直到看到\*QoS 策略组\*列。

4. 单击 QoS 策略组名称。

根据传统 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，将显示相应的服务质量页面。

5. 查看 QoS 策略组的详细配置设置。

6. 单击展开按钮 (▼) 来查看有关该策略组的更多详细信息。

## 查看性能图表以比较同一 QoS 策略组中的卷或 LUN

您可以查看同一 QoS 策略组中的卷和 LUN，然后比较单个 IOPS、MB/s 或 IOPS/TB 图表上的性能以识别任何问题。

比较同一 QoS 策略组中卷的性能的步骤如下所示。查看 LUN 的此信息的步骤类似。

步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。

默认情况下显示“健康状况：所有卷”视图。

2. 在“查看”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。

将显示该卷的性能资源管理器页面。

4. 在查看和比较菜单中，选择\*相同 QoS 策略组中的卷\*。

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除默认的 72 小时之外的不同时间间隔内的性能。

不同类型的 QoS 策略如何在吞吐量图表中显示

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。图表中显示的信息根据应用于工作负载的 QoS 策略的类型而不同。

吞吐量最大值（或“峰值”）设置定义了工作负载可以消耗的最大吞吐量，从而限制了对系统资源竞争工作负载的影响。吞吐量最小值（或“预期”）设置定义了工作负载必须具备的最小吞吐量，以便关键工作负载能够满足最小吞吐量目标，而不管竞争工作负载的需求如何。

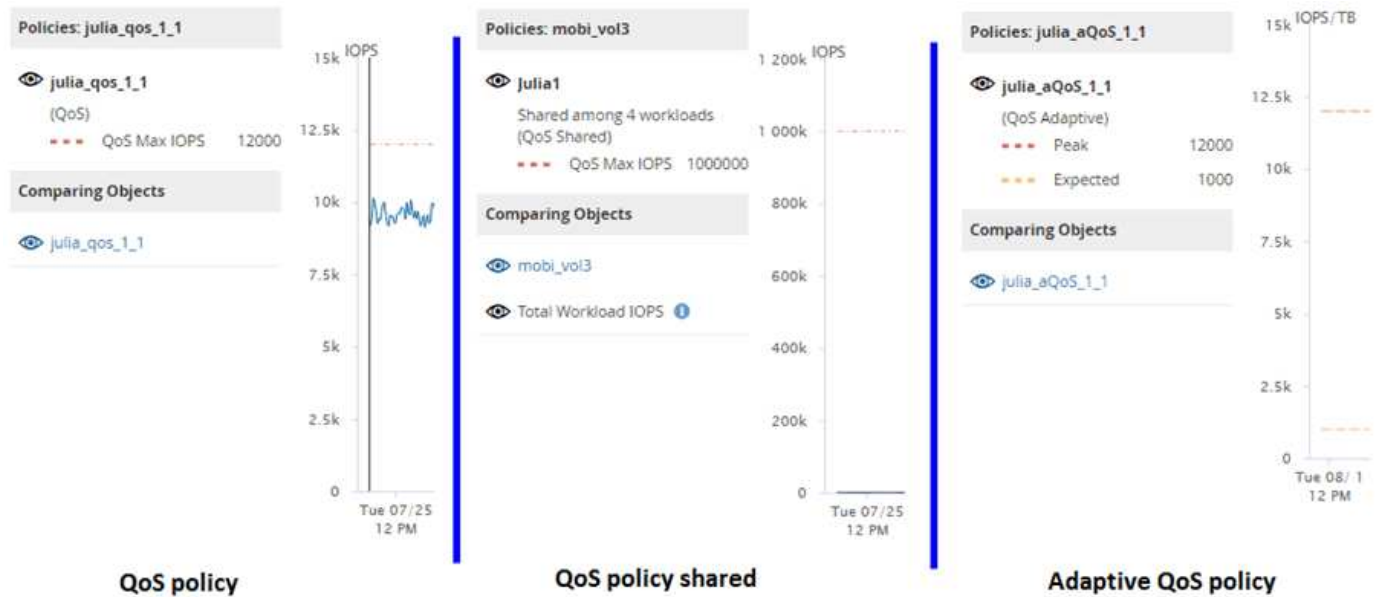
IOPS 和 MB/s 的共享和非共享 QoS 策略使用术语“最小值”和“最大值”来定义下限和上限。 ONTAP 9.3 中引入的 IOPS/TB 自适应 QoS 策略使用术语“预期”和“峰值”来定义下限和上限。

虽然ONTAP允许您创建这两种类型的 QoS 策略，但根据它们如何应用于工作负载，QoS 策略将以三种方式显示在性能图表中。

| 政策类型                                             | 功能                 | Unicum Manager 界面中的指示器 |
|--------------------------------------------------|--------------------|------------------------|
| 分配给单个工作负载的 QoS 共享策略，或分配给单个工作负载或多个工作负载的 QoS 非共享策略 | 每个工作负载可以使用指定的吞吐量设置 | 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 共享）”           |
| 分配给单个工作负载或多个工作负载的自适应 QoS 策略                      | 每个工作负载可以使用指定的吞吐量设置 | 显示“（QoS 自适应）”          |



下图显示了计数器图表中三个选项的显示方式的示例。



当已在 IOPS 中定义的正常 QoS 策略出现在工作负载的 IOPS/TB 图表中时，ONTAP 会将 IOPS 值转换为 IOPS/TB 值，并且 Unified Manager 会在 IOPS/TB 图表中显示该策略以及文本“QoS，在 IOPS 中定义”。

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，并且 Unified Manager 会在 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。当分配设置为“allocated-space”时，峰值 IOPS 是根据卷的大小计算的。当分配设置为“已用空间”时，峰值 IOPS 是根据卷中存储的数据量计算的，同时考虑存储效率。



IOPS/TB 图表仅当卷使用的逻辑容量大于或等于 128 GB 时才显示性能数据。当所选时间范围内已用容量低于 128 GB 时，图表中会显示缺口。

## 在性能资源管理器中查看工作负载 QoS 最小和最大设置

您可以在性能资源管理器图表中查看卷或 LUN 上 ONTAP 定义的服务质量 (QoS) 策略设置。吞吐量最大设置限制了竞争工作负载对系统资源的影响。吞吐量最小设置可确保关键工作负载满足最低吞吐量目标，而不管竞争工作负载的需求如何。

仅当在 ONTAP 中配置了 QoS 吞吐量“最小”和“最大”IOPS 和 MB/s 设置时，它们才会显示在计数器图表中。吞吐量最小设置仅在运行 ONTAP 9.2 或更高版本软件的系统上可用，仅在 AFF 系统上可用，并且目前只能为 IOPS 设置。

自适应 QoS 策略从 ONTAP 9.3 开始可用，并使用 IOPS/TB 而不是 IOPS 来表示。这些策略会根据每个工作负载的卷大小自动调整 QoS 策略值，从而随着卷大小的变化保持 IOPS 与 TB 的比率。您只能将自适应 QoS 策略组应用于卷。QoS 术语“预期”和“峰值”用于自适应 QoS 策略，而不是最小值和最大值。

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“平均”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尚未超过图表中显示的策略阈值。

### 步骤

1. 在所选卷或 LUN 的“性能资源管理器”页面中，执行以下操作来查看 QoS 上限和下限设置：

| 目的                     | 操作                         |
|------------------------|----------------------------|
| 查看 IOPS 上限（QoS 最大值）    | 在 IOPS 总计或细分图表中，单击“缩放视图”。  |
| 查看 MB/s 上限（QoS 最大值）    | 在 MB/s 总计或细分图表中，单击 缩放视图。   |
| 查看 IOPS 下限（QoS 最小值）    | 在 IOPS 总计或细分图表中，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 底线（预期的 QoS） | 对于卷，在 IOPS/TB 图表中，单击 缩放视图。 |

虚线水平线表示ONTAP中设置的最大或最小吞吐量值。您还可以查看 QoS 值更改的实施时间。

2. 要查看与 QoS 设置相比的特定 IOPS 和 MB/s 值，请将光标移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 并且正在给系统资源带来压力，则可以使用 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 设置的更多信息，请参阅 ["绩效管理概述"](#)

## 使用性能容量和可用 IOPS 信息管理性能

性能容量 表示在不超过资源有用性能的情况下，您可以从资源中获得多少吞吐量。当使用现有的性能计数器查看时，性能容量是在延迟成为问题之前从节点或聚合获得最大利用率的点。

Unified Manager 从每个集群中的节点和聚合收集性能容量统计信息。已使用的性能容量是当前正在使用的性能容量的百分比，可用性能容量是仍然可用的性能容量的百分比。

虽然性能容量可用提供了仍然可用的资源百分比，但 可用 IOPS 告诉您在达到最大性能容量之前可以添加到资源的 IOPS 数量。通过使用此指标，您可以确保可以向资源添加预定数量的 IOPS 的工作负载。

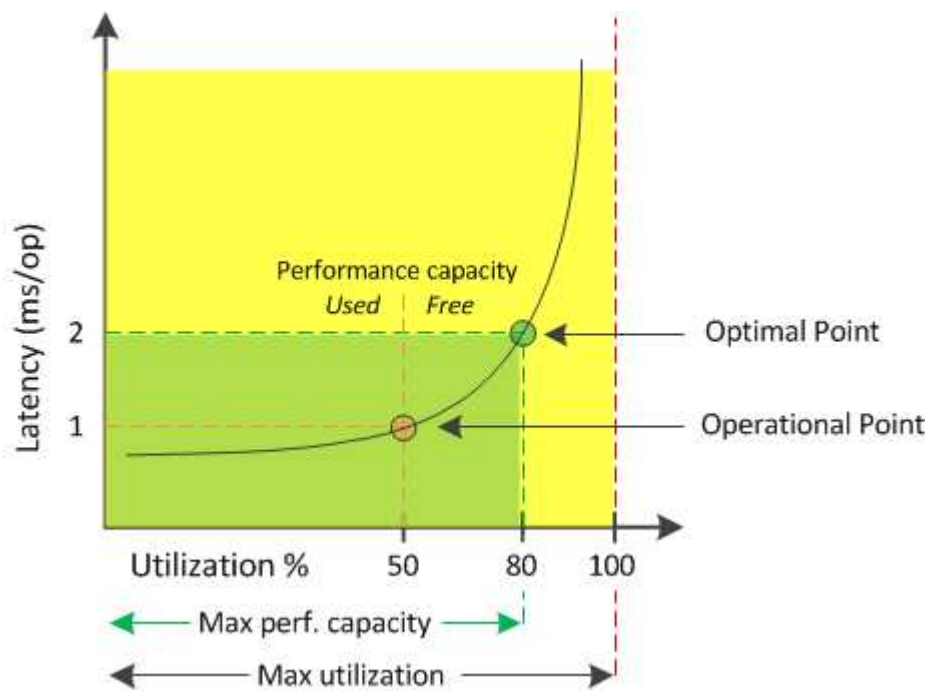
监控性能容量信息有以下好处：

- 协助工作流程配置和平衡。
- 帮助您防止节点过载或将其资源推到最佳点之外，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。

### 所用性能容量

性能容量使用计数器可帮助您确定节点或聚合的性能是否已达到工作负载增加时性能可能下降的程度。它还可以显示在特定时间段内某个节点或聚合是否被过度使用。使用的性能容量与利用率类似，但前者提供了有关特定工作负载的物理资源可用性能能力的更多见解。

最佳使用性能容量是节点或聚合具有最佳利用率和延迟（响应时间）并得到有效利用的点。下图显示了聚合的延迟与利用率曲线示例。



在此示例中，\_操作点\_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 确定此聚合是否有额外的性能容量可用。在这个例子中，\_最佳点\_被确定为聚合利用率为 80% 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，以便更高效地利用您的系统。

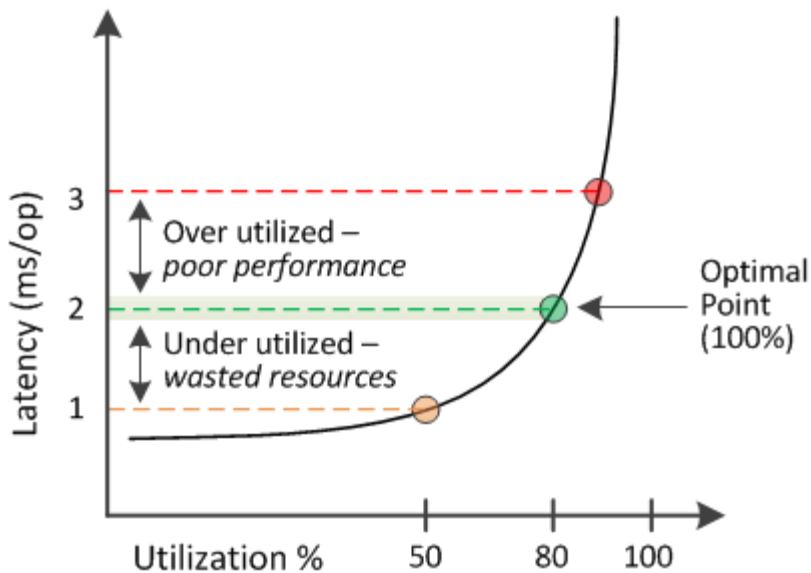
性能容量使用计数器预计会比“利用率”计数器更大，因为性能容量会增加对延迟的影响。例如，如果节点或聚合的使用率为 70%，则性能容量值可能在 80% 到 100% 范围内，具体取决于延迟值。

然而，在某些情况下，仪表板页面上的利用率计数器可能会更高。这是正常现象，因为仪表板会在每个收集周期刷新当前计数器值；它不像 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。性能容量使用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瞬时使用情况。

### 性能容量使用值的含义

性能容量使用值可帮助您识别当前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，并用彩色点标识了当前操作点可能所在的三个区域。



- 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。

- 性能容量使用百分比高于 100 表示节点或聚合体利用率过高，并且工作负载的性能不佳。

不应向资源添加任何新的工作负载，并且可能需要重新分配现有的工作负载。

- 性能容量使用百分比低于 100 表示节点或聚合未得到充分利用，并且资源未得到有效利用。

可以向资源添加更多工作负载。



与利用率不同，性能容量使用百分比可以高于 100%。没有最大百分比，但当资源过度利用时，其百分比通常会在 110% 到 140% 的范围内。百分比越高，表明资源存在严重问题。

## 可用的 IOPS 是什么

可用 IOPS 计数器标识在资源达到其限制之前可以添加到节点或聚合的剩余 IOPS 数。

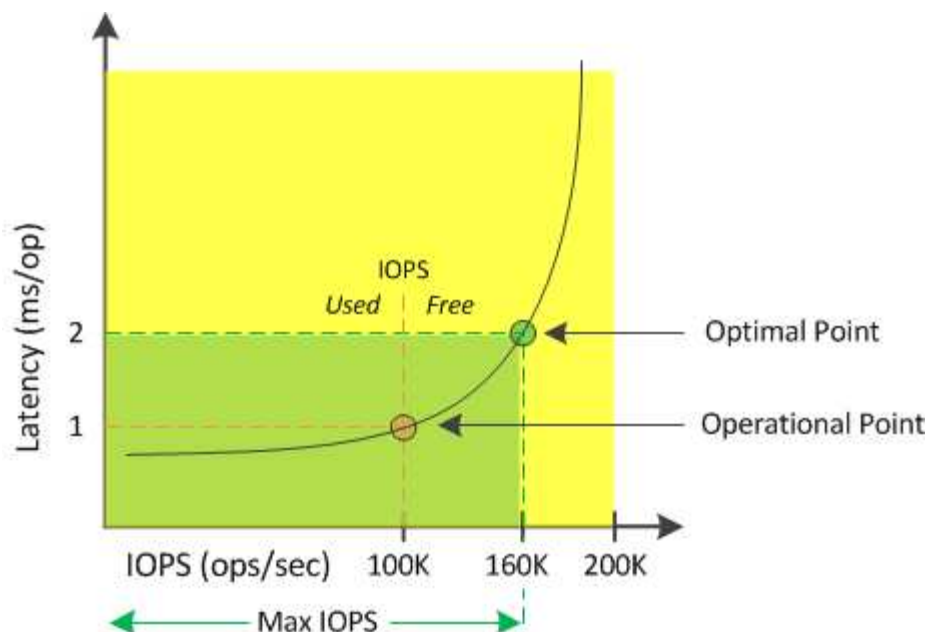
节点可以提供的总 IOPS 取决于节点的物理特性 - 例如 CPU 数量、CPU 速度和 RAM 数量。聚合可以提供的总 IOPS 取决于磁盘的物理属性 - 例如 SATA、SAS 或 SSD 磁盘。

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 IOP 的总和与聚合 IOP 不匹配?"](#)

虽然性能容量可用计数器提供了仍然可用的资源百分比，但可用 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的确切 IOPS（工作负载）数量。

例如，如果您使用一对 FAS2520 和 FAS8060 存储系统，则性能容量可用值为 30% 意味着您有一些可用的性能容量。但是，该值无法显示您可以向这些节点部署多少工作负载。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。

下图显示了节点的延迟与 IOPS 曲线示例。



资源所能提供的最大IOPS数是性能容量使用计数器为100%（最优值）时的IOPS数。操作点表明该节点当前以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 确定该节点的最大 IOPS 为 160K，这意味着有 60K 空闲或可用的 IOPS。因此，您可以向该节点添加更多工作负载，以便更高效地使用您的系统。



当资源中的用户活动最少时，可用的 IOPS 值是根据每个 CPU 核心大约 4,500 IOPS 的通用工作负载来计算的。这是因为 Unified Manager 缺乏数据来准确估计所服务的工作负载的特征。

### 查看节点和聚合性能容量使用值

您可以监控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。

性能容量使用值显示在仪表板、性能清单页面、最佳表现页面、创建阈值策略页面、性能资源管理器页面和详细图表中。例如，“性能：所有聚合”页面提供了“已用性能容量”列，用于查看所有聚合的性能容量已用值。

Aggregates ⓘ

Last updated: 04:11 PM, 08 Feb Refresh

Latency, IOPS, MBps, Utilization are based on hourly samples averaged over the previous 72 hours

Filtering ▾

No filter applied

Assign Threshold Policy

Clear Threshold Policy

Search Aggregates Data

Search

| <input type="checkbox"/> | Status | Aggregate        | Latency    | IOPS     | MBps      | Perf. Capacity Used | Utilization | Free Capacity | Total Capacity | Cluster       | Node           | Policy    |
|--------------------------|--------|------------------|------------|----------|-----------|---------------------|-------------|---------------|----------------|---------------|----------------|-----------|
| <input type="checkbox"/> | ✓      | opm_mo...agg0    | 16.3 ms/op | 124 IOPS | < 1 MBps  | 45%                 | 9%          | 154 GB        | 3,179 GB       | opm-mobility  | opm-m...-02    |           |
| <input type="checkbox"/> | ✓      | rt_aggr2         | 19.8 ms/op | 290 IOPS | < 1 MBps  | 45%                 | 15%         | 6,692 GB      | 6,693 GB       | opm-mobility  | opm-m...-02    |           |
| <input type="checkbox"/> | ✓      | aggr_snap_mirror | 13.9 ms/op | 267 IOPS | < 1 MBps  | 38%                 | 12%         | 6,692 GB      | 6,693 GB       | opm-mobility  | opm-m...-02    |           |
| <input type="checkbox"/> | ✓      | sdot_aggr        | 17.3 ms/op | 745 IOPS | < 1 MBps  | 24%                 | 11%         | 26,621 GB     | 26,774 GB      | opm-mobility  | opm-m...-02    |           |
| <input type="checkbox"/> | ✓      | aggr1            | 15.5 ms/op | 434 IOPS | < 1 MBps  | 16%                 | 6%          | 4,390 GB      | 20,080 GB      | opm-mobility  | opm-m...-01    |           |
| <input type="checkbox"/> | ✓      | rt_aggr1         | 22.3 ms/op | 267 IOPS | < 1 MBps  | 11%                 | 6%          | 6,691 GB      | 6,693 GB       | opm-mobility  | opm-m...-01    |           |
| <input type="checkbox"/> | ✓      | aggr2            | 15.6 ms/op | 259 IOPS | 1.03 MBps | 11%                 | 5%          | 18,472 GB     | 20,080 GB      | opm-mobility  | opm-m...-02    |           |
| <input type="checkbox"/> | ✓      | aggr2            | 9.52 ms/op | 87 IOPS  | 20.8 MBps | Not Supported       | 5%          | 847 GB        | 984 GB         | opm-io...vity | opm-io...ty-01 | aggr_IOPS |
| <input type="checkbox"/> | ⚠      | RTaggr           | 7.62 ms/op | 199 IOPS | 34.7 MBps | Not Supported       | 6%          | 1,292 GB      | 1,477 GB       | opm-io...vity | opm-io...ty-01 | aggr_IOPS |



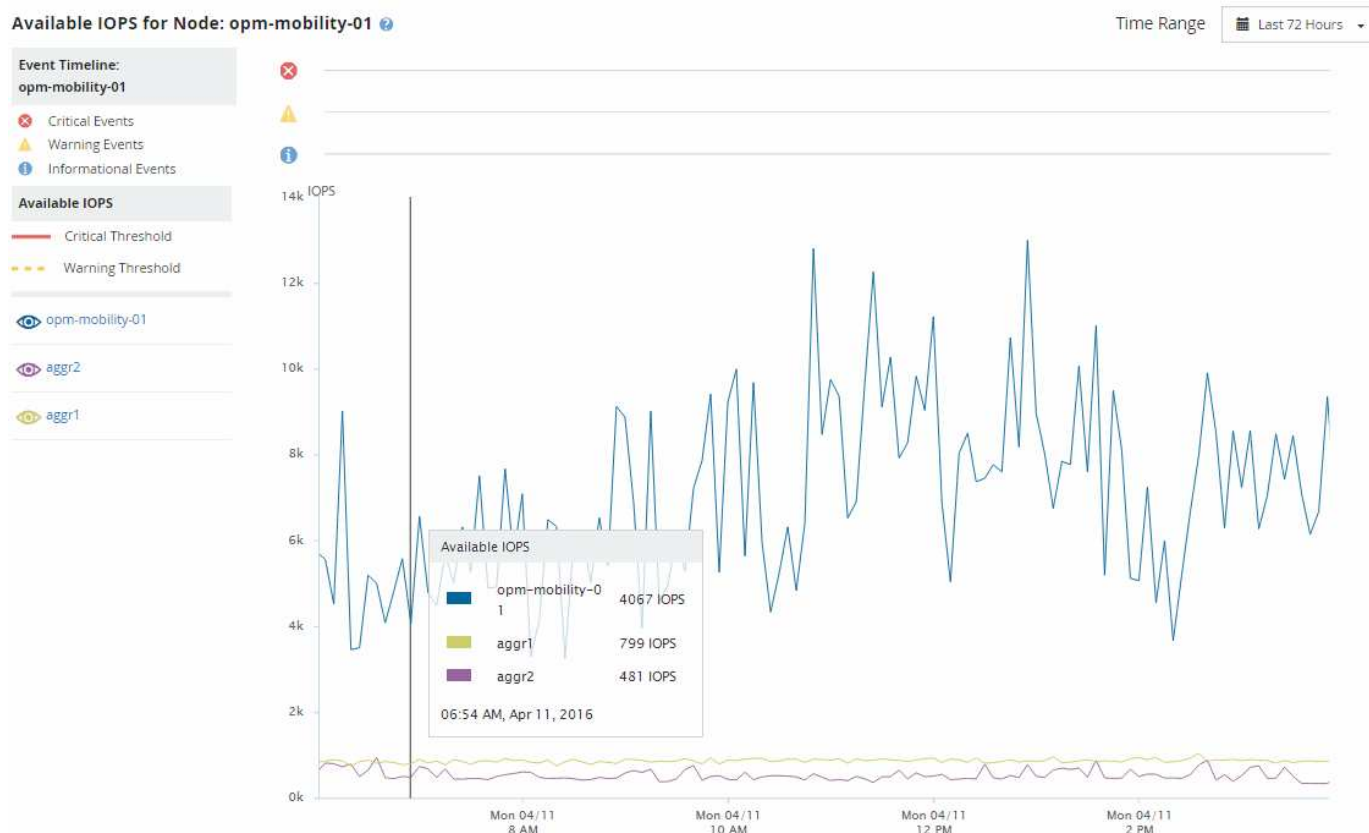
监视性能容量使用计数器可让您识别以下内容：

- 任何集群上的任何节点或聚合是否具有高性能容量使用值
- 任何集群上的任何节点或聚合是否有活动的性能容量使用事件
- 集群中性能容量使用值最高和最低的节点和聚合
- 延迟和利用率计数器值与具有高性能容量使用值的节点或聚合结合使用
- 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受到怎样的影响
- 具有高性能容量使用值的聚合上最繁忙的卷和 LUN

## 查看节点并聚合可用 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和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，以便比较该节点和该节点上的多个聚合的可用 IOPS 值。



监控可用的 IOPS 计数器可让您识别：

- 具有最大可用 IOPS 值的节点或聚合有助于确定未来工作负载的部署位置。
- 具有最小可用 IOPS 值的节点或聚合，用于确定您应该监控的潜在未来性能问题的资源。
- 聚合上可用 IOPS 值较小的最繁忙的卷和 LUN。

## 查看性能容量计数器图表以识别问题

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所选节点或聚合的性能容量使用值。细分计数器图表显示根据用户协议与后台系统进程划分的根对象的总性能容量值。此外，还显示了可用的性能容量。

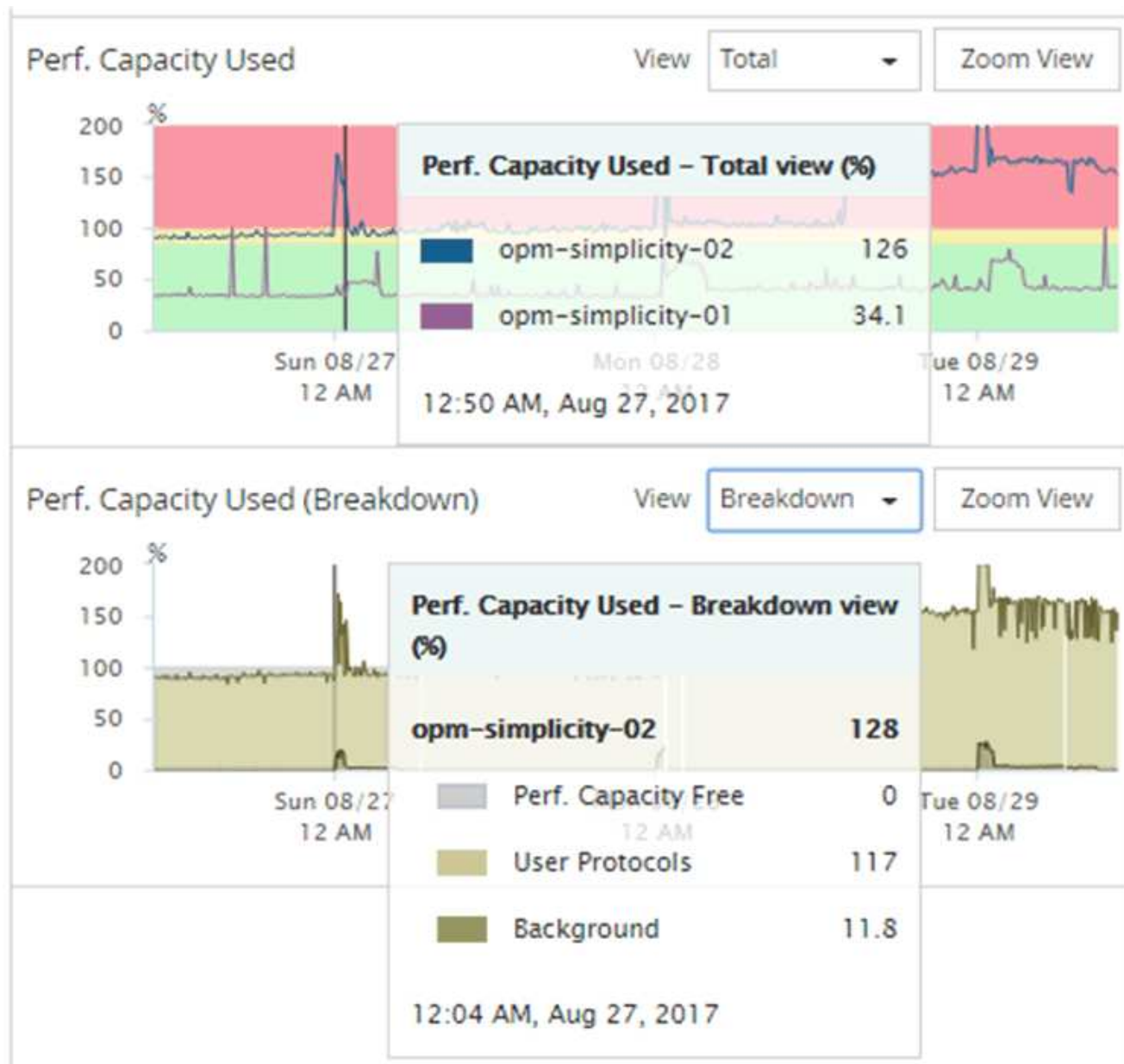


由于一些与系统和数据管理相关的后台活动被识别为用户工作负载并归类为用户协议，因此当这些进程运行时，用户协议百分比可能会显得人为地高。这些进程通常在集群使用率较低的午夜左右运行。如果您发现午夜左右用户协议活动激增，请验证集群备份作业或其他后台活动是否配置为在该时间运行。

### 步骤

1. 从节点或聚合\*登陆\*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。已用容量\*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）、对象何时未得到充分利用（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. 如果您想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，以将同一时间范围内的性能容量使用值与 IOPS 或 MBps 值进行比较。

## 性能容量使用性能阈值条件

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，可以为节点配置“性能容量使用接管”阈值策略。此阈值策略将 HA 对中两个节点的性能容量使用统计信息相加，以确定当另一个节点发生故障时，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工作负载的组合，因此可以对两个节点应用相同的性能容量使用接管策略。





这种性能容量使用等效性在节点之间通常是正确的。但是，如果通过故障转移伙伴节点发往其中一个节点的跨节点流量明显增多，则在一个伙伴节点上运行所有工作负载时所使用的总性能容量与在另一个伙伴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，具体取决于哪个节点发生故障。

性能容量使用条件还可以用作辅助性能阈值设置，以在定义 LUN 和卷的阈值时创建组合阈值策略。性能容量使用条件适用于卷或 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     | 临界阈值     | 持续时间 |
|------|----------|----------|----------|------|
| 卷    | 延迟       | 15 毫秒/操作 | 25 毫秒/操作 | 20分钟 |
| 聚合   | 已使用的性能容量 | 80%      | 95%      |      |

组合阈值策略仅当整个持续时间内同时违反两个条件时才会生成事件。

## 使用性能容量使用计数器来管理性能

通常，组织希望以低于 100 的性能容量使用百分比来运营，以便高效利用资源，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来自定义何时发送高性能容量使用值警报。

您可以根据您的性能要求制定具体的目标。例如，金融服务公司可能会保留更多的履约能力，以保证交易的及时执行。这些公司可能希望将性能容量使用阈值设置在 70% 至 80% 的范围内。如果利润较小的制造公司愿意冒着性能风险来更好地管理 IT 成本，他们可能会选择保留较少的性能容量。这些公司可能会将性能容量使用阈值设置在 85-95% 范围内。

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。这些事件还可以用作需要在节点和聚合内进行工作负载移动和更改的指标。

## 了解并使用节点故障转移规划页面

如果节点的高可用性 (HA) 伙伴节点发生故障，性能/节点故障转移规划页面将估计对节点性能的影响。Unified Manager 根据 HA 对中节点的历史性能进行估计。

估计故障转移对性能的影响有助于您在以下情况下进行规划：

- 如果故障转移持续使接管节点的估计性能降低到不可接受的水平，您可以考虑采取纠正措施来减少故障转移造成的性能影响。
- 在启动手动故障转移来执行硬件维护任务之前，您可以估计故障转移对接管节点性能的影响，以确定执行该任务的最佳时间。

## 使用节点故障转移计划页面确定纠正措施

根据“性能/节点故障转移规划”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，为了减少故障转移对性能的估计影响，您可以将某些卷或 LUN 从 HA 对中的节点移动到集群中的其他节点。这样做可确保主节点在故障转移后能够继续提供可接受的性能。

## 节点故障转移计划页面的组件

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。

### 绩效统计网格

性能/节点故障转移规划页面显示一个网格，其中包含延迟、IOPS、利用率和使用的性能容量的统计信息。



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预测节点故障转移的值。

在网格中，每个节点被分配以下角色之一：

- 主云

当 HA 合作伙伴发生故障时接管该合作伙伴的节点。根对象始终是主节点。

- 合作伙伴

故障转移场景中发生故障的节点。

- 估计接管

与主节点相同。该节点显示的性能统计数据显示了接管节点接管故障伙伴节点后的性能。



尽管故障转移后接管节点的工作负载相当于两个节点工作负载的总和，但估计接管节点的统计数据并不是主节点和合作伙伴节点统计数据的总和。例如，如果主节点的延迟为 2 ms/op，合作伙伴节点的延迟为 3 ms/op，则估计接管节点的延迟可能为 4 ms/op。此值是 Unified Manager 执行的计算。

如果您希望合作伙伴节点成为根对象，可以单击其名称。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”选项卡来查看此节点故障场景下性能如何变化。例如，如果 Node1 是主节点，Node2 是合作伙伴节点，则可以单击 Node2 使其成为主节点。通过这种方式，您可以看到估计的性能如何根据哪个节点发生故障而变化。

### 比较窗格

以下列表描述了比较窗格中默认显示的组件：

- 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。它们仅属于主节点。

- 反图表

它们显示网格中显示的性能计数器的历史统计数据。在每个图表中，估计接管节点的图形显示了在任何给定

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 2 月 8 日上午 11 点预计接管节点的利用率为 73%。如果当时发生故障转移，接管节点的利用率将达到 73%。

历史统计数据可以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。您仅可以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，根对象和伙伴节点的统计信息都会显示在比较窗格中。与性能/节点性能资源管理器页面不同，此页面不显示\*添加\*按钮供您添加对象进行统计比较。

您可以按照与在性能/节点性能资源管理器页面中相同的方式自定义比较窗格。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”可在新窗口中显示特定计数器的详细图表。

## 将阈值策略与节点故障转移计划页面结合使用

您可以创建节点阈值策略，以便当潜在故障转移导致接管节点的性能降低到不可接受的水平时，您可以在“性能/节点故障转移计划”页面中收到通知。

如果连续六个收集期（30 分钟）超出阈值，则名为“节点 HA 对过度利用”的系统定义性能阈值策略将生成警告事件。如果 HA 对中节点的组合性能容量使用量超过 200%，则视为超出阈值。

来自系统定义的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，您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预测的延迟值。

除了使用此系统定义的阈值策略之外，您还可以使用“已用性能容量 - 接管”计数器创建阈值策略，然后将该策略应用于选定的节点。指定低于 200% 的阈值使您能够在超出系统定义策略的阈值之前收到事件。如果您希望在生成系统定义的策略事件之前收到通知，还可以指定超出阈值的最短时间段，使其少于 30 分钟。

例如，您可以定义一个阈值策略，当 HA 对中节点的组合性能容量使用量超过 175% 超过 10 分钟时，就会生成警告事件。您可以将此策略应用于构成 HA 对的 Node1 和 Node2。收到节点 1 或节点 2 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预计性能影响。如果发生故障转移，您可以采取纠正措施以避免接管节点过载。如果在节点的综合性能容量使用率低于 200% 时采取措施，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。

## 使用性能容量使用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合作伙伴节点已用性能容量。它还显示了预计接管节点上的可用性能容量。此信息可帮助您确定如果合作伙伴节点发生故障，是否会出现性能问题。

除了显示节点使用的总性能容量之外，细分图表还将每个节点的值细分为用户协议和后台进程。

- 用户协议是从用户应用程序到集群的 I/O 操作。
- 后台进程是涉及存储效率、数据复制和系统健康的内部系统进程。

通过这一额外的详细信息级别，您可以确定性能问题是由用户应用程序活动还是后台系统进程（例如重复数据删除、RAID 重建、磁盘清理和SnapMirror副本）引起的。

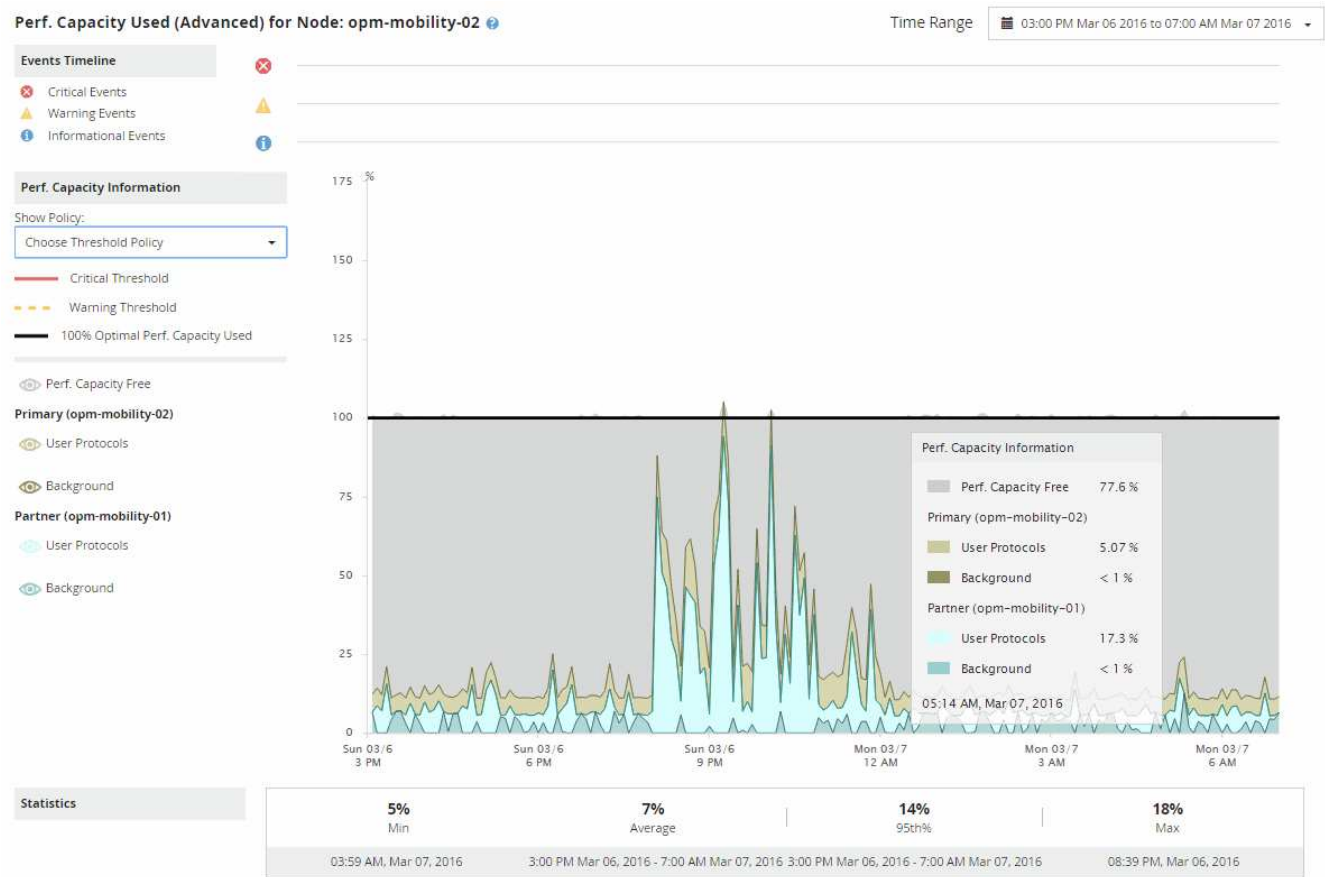
步骤

- 1. 转到将作为预计接管节点的节点的“性能/节点故障转移计划”页面。
- 2. 从\*时间范围\*选择器中，选择计数器网格和计数器图表中显示历史统计数据的时间段。

将显示包含主节点、合作伙伴节点和估计接管节点的统计信息的计数器图表。

- 3. 从\*选择图表\*列表中，选择\*Perf. 已用容量\*。
- 4. 在 **Perf** 中。容量已用\*图表，选择\*细分\*并单击\*缩放视图。

Perf 的详细图表。显示已用容量。



- 5. 将光标移到详细图表上，即可在弹出窗口中查看性能容量使用信息。

穿孔。可用容量百分比是预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还剩下多少性能容量。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可用百分比过低。

如果您计划启动故障转移以进行节点维护，请选择性能容量可用百分比不为 0 时使合作伙伴节点发生故障的时间。

# 收集数据并监控工作负载性能

Unified Manager 每 5 分钟收集并分析一次工作负载活动以识别性能事件，并且每 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 天的工作负载活动才能开始分析，并且 I/O 响应时间的延迟预测才能显示在工作负载分析页面和事件详细信息页面上。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变化。收集 3 天的活动后，Unified Manager 会在每 24 小时的凌晨 12:00 调整一次延迟预测，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。上次收集之前检测到的事件仍然可用。



夏令时 (DST) 会改变系统时间，从而改变受监控工作负载的性能统计数据的延迟预测。Unified Manager 立即开始更正延迟预测，这大约需要 15 天才能完成。在此期间，您可以继续使用 Unified Manager，但是，由于 Unified Manager 使用延迟预测来检测动态事件，因此某些事件可能不准确。时间变化之前检测到的事件不受影响。

## Unified Manager 监控的工作负载类型

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。这些进程是与读取和写入请求相关的进程。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。

如果某个工作负载满足以下一项或多项条件，则该工作负载无法受到 Unified Manager 监控：

- 它是只读模式下的数据保护 (DP) 副本。（DP 卷受到用户生成的流量监控。）
- 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、数据复制和系统健康相关的内部流程包括：

- 存储效率，例如重复数据删除
- 磁盘健康状况，包括 RAID 重建、磁盘清理等
- 数据复制，例如 SnapMirror 副本
- 管理活动
- 文件系统健康状况，包括各种 WAFL 活动
- 文件系统扫描器，例如 WAFL 扫描

- 仅当这些工作负载所使用的集群组件存在争用时，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。

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，这些统计值形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来通知您。

| 测量 | 描述                                                                                                                                                                                                                                                                        |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 活动 | <p>策略组中的工作负载使用的 QoS 限制百分比。</p> <div>  <p>如果 Unified Manager 检测到策略组发生变化（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定限制的 100%。如果值超过设定限值的 100%，则显示为 &gt;100%。如果值小于设定限值的 1%，则显示为 &lt;1%。</p> </div> |
| 实际 | 对于给定的工作负载，在特定时间测量的性能值。                                                                                                                                                                                                                                                    |



| 测量         | 描述                                                                                                                                                                                        |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 偏差         | <p>预期值与实际值之间的变化。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。</p> <div>  <p>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。</p> </div> |
| 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的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         | 一段时间内测得的最大值。                                                                                                                                                                              |
| 峰值偏差       | 一段时间内测得的最大偏差值。                                                                                                                                                                            |
| 队列深度       | 在互连组件处等待的待处理 I/O 请求数。                                                                                                                                                                     |
| 利用率        | 对于网络处理、数据处理和聚合组件，一段时间内完成工作负载操作的繁忙时间百分比。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。                                                                                                                                 |

## 预期的表现范围是多少

延迟预测是对特定时间的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。电子邮件服务器需求的增加意味着此时间段内后端存储的工作负载活动也会增加。员工可能会注意到他们的电子邮件客户端的响应时间很慢。

在中午 12 点到下午 1 点之间的午餐时间以及下午 5 点之后的工作时间结束时，大多数员工可能都不会使用电脑。对电子邮件服务器的需求通常会减少，对后端存储的需求也会减少。或者，可以有预定的工作负载操作，例如存储备份或病毒扫描，这些操作在下午 5:00 之后开始，并增加后端存储的活动。

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），并确定了工作负载的上限和下限。当对象的实际工作负载活动超出上限或下限，并在一段时间内保持超出边界时，这可能表明该对象被过度使用或未得到充分使用。

## 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 I/O 响应时间的延迟预测才能显示在 GUI 中。所需的最低限度的数据收集并未考虑到工作负载活动发生的所有变化。收集前 3 天的活动后，Unified Manager 会在凌晨 12:00 每 24 小时调整一次延迟预测，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) 会改变系统时间，从而改变受监控工作负载的性能统计数据延迟预测。 Unified Manager 立即开始更正延迟预测，这大约需要 15 天才能完成。在此期间，您可以继续使用 Unified Manager，但是，由于 Unified Manager 使用延迟预测来检测动态事件，因此某些事件可能不准确。时间变化之前检测到的事件不受影响。

## 延迟预测如何用于性能分析

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，它会提醒您，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它。

延迟预测为工作负载设定了性能基准。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。预期范围的上限确定了动态性能阈值。 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。实际值和预期值之间的比较为工作负载创建了性能概况。

当工作负载的实际延迟超过动态性能阈值时，由于集群组件的争用，延迟会很高，工作负载的执行速度会比预期慢。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要慢。

Unified Manager 分析阈值交叉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较长时间内（例如几个小时）保持一致，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具有较低的活动性，其中延迟的延迟预测不会随时间发生很大的变化。为了在性能事件分析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，卷的延迟预测为灰色，最低为每操作 3.5 毫秒 (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的争用，实际延迟（蓝色）突然增加到 10 ms/op，则它高于延迟预测并已超过动态性能阈值。

当网络流量减少或集群组件不再争用时，延迟将恢复到延迟预测范围内。如果延迟长时间保持在 10 ms/op 或以上，您可能需要采取纠正措施来解决该事件。



## Unified Manager 如何使用工作负载延迟来识别性能问题

工作负载延迟（响应时间）是集群上的卷响应来自客户端应用程序的 I/O 请求所需的时间。Unified Manager 使用延迟来检测性能事件并向您发出警报。

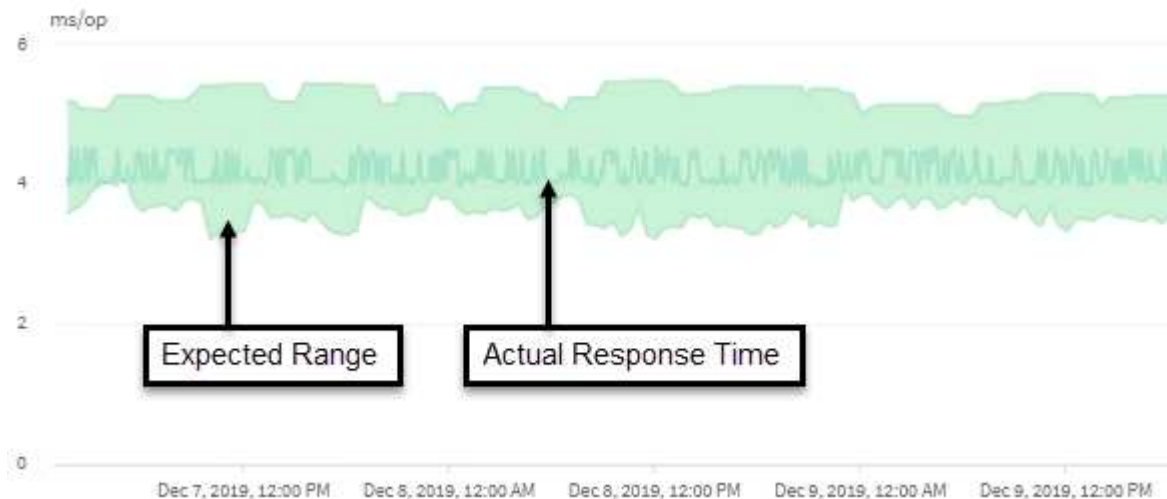
高延迟意味着应用程序对集群上的卷的请求所花的时间比平时要长。高延迟的原因可能是集群本身，因为一个或多个集群组件存在争用。高延迟也可能由集群外部的因素引起，例如网络瓶颈、托管应用程序的客户端问题或应用程序本身的问题。



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）会增加对其他工作负载共享的集群组件的需求，也会导致高延迟。如果实际延迟超过预期范围（延迟预测）的动态性能阈值，Unified Manager 会分析该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) 来衡量。

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和分析，以了解各个进程（例如读取和写入请求）的活动与整体延迟统计数据的情况。通过比较，您可以确定哪些操作具有最高的活动，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。

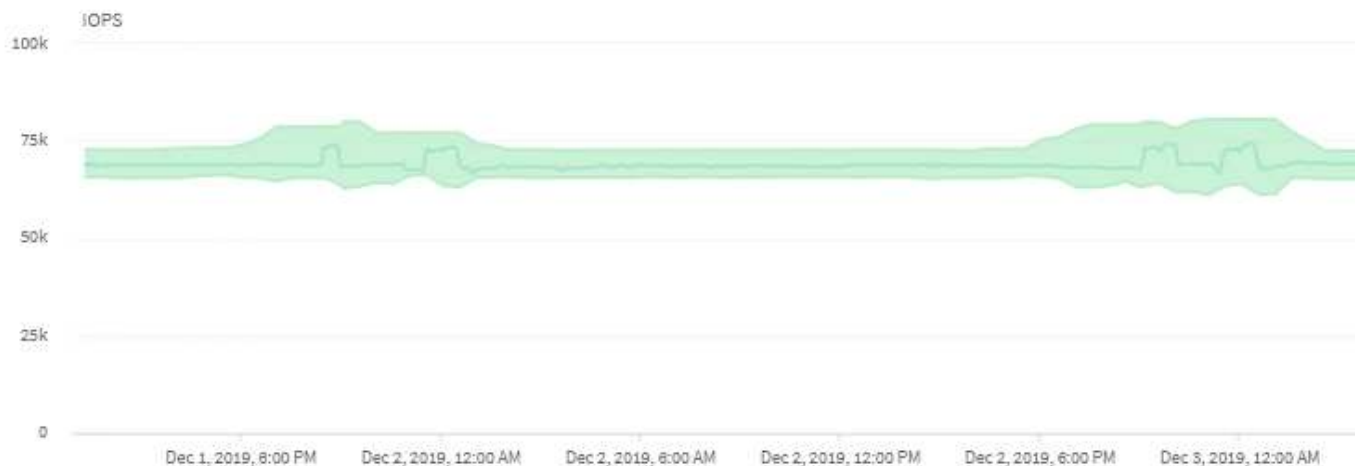


如果 Unified Manager 无法收集数据，蓝线中可能会出现间隙。发生这种情况可能是因为集群或卷无法访问、Unified Manager 在此期间关闭或收集时间超过 5 分钟的收集时间。

## 集群操作如何影响工作负载延迟

操作（IOPS）代表集群上所有用户定义和系统定义的工作负载的活动。IOPS 统计数据可帮助您确定集群进程（例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）或可能导致或促成性能事件。

分析性能事件时，您可以使用 IOPS 统计数据来确定性能事件是否由集群问题引起。您可以识别可能是性能事件主要影响因素的特定工作负载活动。IOPS 以每秒操作数 (ops/sec) 来衡量。



此示例显示 IOPS 图表。实际操作统计数据为蓝线，操作统计数据的 IOPS 预测为绿色。



在某些情况下，当集群过载时，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，以便收集统计数据。

## MetroCluster配置的性能监控

Unified Manager 使您能够监控MetroCluster配置中集群之间的写入吞吐量，以识别具有大量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，Unified Manager 会触发性能事件来通知您。



Unified Manager 将MetroCluster配置中的集群视为单独的集群。它不区分合作伙伴集群或关联每个集群的写入吞吐量。

当MetroCluster配置中的本地集群将其数据镜像到其伙伴集群时，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利用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被称为\_受害者\_，而写入NVRAM的吞吐量偏差高于平常、导致争用的工作负载被称为\_欺凌者\_。由于只有写入请求镜像到伙伴集群，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。您可以按集群过滤结果。从左侧导航窗格：

- 存储 > 集群 > 性能：所有集群 视图。请参见
- 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"

"识别绩效事件中涉及的欺凌工作负载"

"识别性能事件中涉及的shark工作负载"

## 了解性能事件和警报

性能事件是与集群上的工作负载性能相关的事件。它们可以帮助您识别响应时间较慢的工作负载。结合同同时发生的健康事件，您可以确定可能导致或造成响应时间缓慢的问题。

当 Unified Manager 检测到同一集群组件多次出现同一事件条件时，它会将所有出现的事件视为单个事件，而不是单独的事件。

您可以配置警报，以便在发生某些严重程度类型的性能事件时自动发送电子邮件通知。

### 性能事件源

性能事件是与集群上的工作负载性能相关的问题。它们可以帮助您识别响应时间较慢（也称为高延迟）的存储对象。结合同同时发生的其他健康事件，您可以确定可能导致或造成响应时间缓慢的问题。

Unified Manager 从以下来源接收性能事件：

- 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，以便在性能计数器的阈值被突破时生成事件。

您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，以解决常见的性能问题。

这些阈值策略默认启用，您可能在添加集群后不久看到事件。

- 动态性能阈值事件

由于 IT 基础设施故障或错误，或工作负载过度利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解决，或者可以通过修复或配置更改来解决。动态阈值事件表示ONTAP系统上的工作负载由于其他工作负载对共享集群组件的使用率较高而导致运行速度较慢。

这些阈值默认启用，您可能在从新集群收集数据三天后看到事件。

## 性能事件严重性类型

每个性能事件都与一个严重性类型相关联，以帮助您确定需要立即采取纠正措施的事件的优先级。

- 批判的

发生了性能事件，如果不立即采取纠正措施，可能会导致服务中断。

关键事件仅从用户定义的阈值发送。

- 警告

群集对象的性能计数器超出正常范围，应进行监视以确保其不会达到严重程度。这种严重程度的事件不会导致服务中断，并且可能不需要立即采取纠正措施。

警告事件由用户定义、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，就会发生该事件。例如，当删除任何存储对象或发生任何配置更改时，就会生成严重性类型为信息的事件。

当 ONTAP 检测到配置更改时，会直接从 ONTAP 发送信息事件。

有关详细信息，请参阅以下链接：

- ["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"](#)

## Unified Manager 检测到的配置更改

Unified Manager 监控集群的配置变化，以帮助您确定变化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 (●) 来指示检测到变化的日期和时间。

您可以查看性能资源管理器页面和工作负载分析页面中的性能图表，以了解更改事件是否影响了所选集群对象的性能。如果在性能事件发生时或大约同时检测到变化，则该变化可能导致问题，从而触发事件警报。

Unified Manager 可以检测以下变更事件，这些事件被归类为信息事件：

- 卷在聚合体之间移动。

Unified Manager 可以检测移动何时进行、完成或失败。如果 Unified Manager 在卷移动期间关闭，则当它重新启动时，它会检测卷移动并显示其更改事件。

- 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）限制发生变化。

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，这也可能会触发策略组的事件。延迟逐渐恢

复正常，并且由峰值引起的任何事件都会消失。

- HA 对中的节点接管或归还其配对节点的存储。

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，Unified Manager 将不会检测到该事件。

- ONTAP 升级或恢复操作已成功完成。

显示先前版本和新版本。

## 系统定义的性能阈值策略的类型

Unified Manager 提供了一些标准阈值策略，用于监控集群性能并自动生成事件。这些策略默认启用，当监控的性能阈值被突破时，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。

如果您从任何系统定义的性能阈值策略收到不必要的事件，您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会分配给 Unified Manager 监控的每个集群：

- 集群负载不平衡

识别一个节点的负载比集群中其他节点高得多的情况，因此可能会影响工作负载延迟。

它通过比较集群中所有节点的性能容量使用值来查看是否有任何节点超过 30% 的阈值超过 24 小时。这是一个警告事件。

- 集群容量不平衡

识别一个聚合的已用容量比集群中的其他聚合高得多的情况，因此可能会影响操作所需的空間。

它通过比较集群中所有聚合的已用容量值来查看聚合之间是否存在 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 Unified Manager 监控的集群中的每个节点：

- 已突破性能容量使用阈值

识别单个节点的运行效率超出其界限并因此可能影响工作负载延迟的情况。

它通过寻找使用性能容量超过 100% 且持续时间超过 12 小时的节点来实现这一点。这是一个警告事件。

- 节点 HA 对过度利用

识别 HA 对中的节点运行超出 HA 对运行效率界限的情况。

它通过查看 HA 对中两个节点的性能容量使用值来实现这一点。如果两个节点使用的性能容量总和超过 200% 且持续时间超过 12 小时，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的情况，从而降低关键系统服务的速度并可能影响节点上的工作负载延迟。

它通过查看节点上所有聚合的某些读写操作比率来实现这一点。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触发此策略。这是一个警告事件。



“节点磁盘碎片”策略仅分析 HDD 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 Unified Manager 监控的集群中的每个聚合：

- 聚合磁盘过度利用

识别聚合运行超出其运行效率极限的情况，从而可能影响工作负载延迟。它通过查找聚合中磁盘利用率超过 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 重新同步和重新奇偶校验。

- 磁盘架光纤通道互连是否存在通信瓶颈？

- 总体而言，可用空间是否太少？仅当三项下属政策中的一项（或多项）也被视为违反时，才会针对该政策发出警告事件。如果仅聚合中的磁盘利用率超过 95%，则不会触发性能事件。



“聚合磁盘过度利用”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分配给任何具有已配置性能服务级别策略且具有已定义“预期延迟”值的工作负载：

- 工作负载卷/LUN 延迟阈值超出性能服务级别定义

识别超出其“预期延迟”限制并影响工作负载性能的卷（文件共享）和 LUN。这是一个警告事件。

它通过查找前一小时内 30% 的时间内超过预期延迟值的工作负载来实现这一点。

## QoS 阈值策略

系统定义的 QoS 性能阈值策略分配给任何具有配置的 ONTAP QoS 最大吞吐量策略（IOPS、IOPS/TB 或 MB/s）的工作负载。当工作负载吞吐量值比配置的 QoS 值低 15% 时，Unified Manager 会触发一个事件：



- **QoS 最大 IOPS 或 MB/s 阈值**

识别已超出其 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。

当将单个工作负载分配给策略组时，它会通过查找前一小时每个收集期间内超过分配的 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，它会通过将策略中所有工作负载的 IOPS 或 MB/s 相加并根据阈值检查总数来实现此目的。

- **QoS 峰值 IOPS/TB 或具有块大小阈值的 IOPS/TB**

识别已超出其自适应 QoS 峰值 IOPS/TB 吞吐量限制（或具有块大小限制的 IOPS/TB）且影响工作负载延迟的卷。这是一个警告事件。

它通过将自适应 QoS 策略中定义的峰值 IOPS/TB 阈值转换为基于每个卷大小的 QoS 最大 IOPS 值来实现此目的，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 及更高版本的软件时，此策略才适用于卷。

当自适应 QoS 策略中定义了“块大小”元素时，阈值将根据每个卷的大小转换为 QoS 最大 MB/s 值。然后，它会查找前一小时每个性能收集期间内超过 QoS 最大 MB/s 的卷。



仅当集群安装了 ONTAP 9.5 及更高版本的软件时，此策略才适用于卷。

## 性能事件分析和通知

性能事件会通知您因集群组件争用而导致的工作负载的 I/O 性能问题。Unified Manager 会分析该事件以确定所涉及的所有工作负载、存在争用的组件以及该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，该组件就会发生争用，无法以最佳水平运行以满足工作负载需求。使用相同组件的其他工作负载的性能可能会受到影响，导致其延迟增加。如果延迟超过动态性能阈值，Unified Manager 将触发性能事件来通知您。

### 事件分析

Unified Manager 使用前 15 天的性能统计数据执行以下分析，以识别事件中涉及的受害者工作负载、欺凌工作负载和集群组件：

- 识别延迟已超过动态性能阈值（即延迟预测的上限）的受害者工作负载：
  - 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 超过每秒 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 毫秒且 IOPS 大于 100 操作/秒时才会触发事件。
- 识别处于争用的集群组件。



如果集群互连处受害工作负载的延迟大于 1 毫秒，Unified Manager 会将其视为重大事件并触发集群互连事件。

- 识别过度使用集群组件并导致其发生争用的霸凌工作负载。
- 根据集群组件的利用率或活动的偏差对所涉及的工作负载进行排序，以确定哪些欺凌者对集群组件的使用变化最大，以及哪些受害者受到的影响最大。

事件可能只发生短暂的一瞬间，然后在其使用的组件不再争用后自行纠正。连续事件是指在五分钟间隔内针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 在两个连续的分析间隔内检测到相同事件后会触发警报。

事件解决后，它将保留在 Unified Manager 中，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

事件可以处于以下状态之一：

- 积极的

表示性能事件当前处于活动状态（新的或已确认）。导致该事件的问题尚未自行纠正或尚未解决。存储对象的性能计数器仍然高于性能阈值。

- 过时的

表示该事件不再有效。导致该事件的问题已自行纠正或已解决。存储对象的性能计数器不再高于性能阈值。

## 事件通知

这些事件显示在仪表板页面和用户界面的许多其他页面上，并且这些事件的警报会发送到指定的电子邮件地址。您可以在事件详情页面和工作负载分析页面查看事件的详细分析信息并获得解决该事件的建议。

## 事件交互

在事件详情页面和工作负载分析页面，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，显示检测到该事件的日期和时间。

如果同一时间段内有多个事件，则消息会显示事件的数量。

- 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多详细信息，包括所涉及的集群组件。

有争议的组件被圈出并以红色突出显示。您可以点击“查看完整分析”在事件详情页面查看完整分析。如果同一时间段内有多个事件，对话框将显示最近三个事件的详细信息。您可以点击某个事件，在事件详情页面查看该事件的分析。



## Unified Manager 如何确定事件对性能的影响

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级别。此信息决定了事件中每个工作负载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预期值范围（延迟预测）进行比较。最后分析的值与预期值范围之间的差异可确定受事件影响最大的工作负载。

例如，假设一个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 的延迟预测为每操作 5-10 毫秒 (ms/op)，而其实际延迟通常在 7 ms/op 左右。工作负载 B 的延迟预测为 10-20 ms/op，其实际延迟通常在 15 ms/op 左右。两种工作负载都完全符合其延迟预测。由于集群上的争用，两个工作负载的延迟都增加到 40 ms/op，超过了动态性能阈值（即延迟预测的上限），并触发事件。对于工作负载 A，从预期值到性能阈值以上的值的延迟偏差约为 33 ms/op，而对于工作负载 B，延迟偏差约为 25 ms/op。两种工作负载的延迟都飙升至 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，为 33 ms/op。

在“事件详细信息”页面的“系统诊断”部分中，您可以根据集群组件的活动、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，以确定工作负载排序顺序。对于延迟，红点 (●) 表示受害工作负载跨越了性能阈值，以及随后对延迟的影响。每个红点表示延迟的偏差程度较高，这有助于您识别受事件影响最大的延迟受害者工作负载。

## 集群组件及其争用的原因

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的性能会变慢，并且其对客户端请求的响应时间（延迟）会增加，从而触发 Unified Manager 中的事件。

存在争用的组件无法达到最佳性能。它的性能已经下降，并且其他集群组件和工作负载（称为“受害者”）的性能可能会增加延迟。要使组件摆脱争用，必须减少其工作负载或提高其处理更多工作的能力，以便性能恢复到正常水平。由于 Unified Manager 以五分钟为间隔收集和分析工作负载性能，因此它仅检测集群组件何时持续过度使用。未检测到在五分钟内仅持续很短时间的过度使用瞬态峰值。

例如，存储聚合可能处于争用状态，因为其上的一个或多个工作负载正在竞争满足其 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，以减少当前聚合上的总体工作负载需求。对于 QoS 策略组，您可以调整吞吐量限制，或将工作负载移至其他策略组，这样工作负载就不会再受到限制。

Unified Manager 监控以下集群组件，并在它们发生争用时提醒您：

- 网络

表示集群上外部网络协议的 I/O 请求的等待时间。等待时间是指集群响应 I/O 请求之前等待“传输就绪”事务完成所花费的时间。如果网络组件处于争用状态，则意味着协议层的高等待时间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的 I/O 处理的软件组件。负责网络处理的节点可能会在检测到事件后发生更改。如果网络处理组件存在争用，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。

在主动-主动配置中使用全 SAN 阵列群集时，将显示两个节点的网络处理延迟值，以便您可以验证节点是否平等地共享负载。

- **QoS 限制最大值**

表示分配给工作负载的存储服务质量 (QoS) 策略组的最大吞吐量（峰值）设置。如果策略组组件存在争用，则意味着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 限制最小值**

表示由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。如果某些工作负载上设置的 QoS 最小值使用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多延迟。

- **集群互连**

表示集群节点物理连接的电缆和适配器。如果集群互连组件处于争用状态，则意味着集群互连处 I/O 请求的等待时间过长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与包含工作负载的存储聚合之间的 I/O 处理的软件组件。负责数据处理的节点可能会在检测到事件后发生更改。如果数据处理组件存在争用，则意味着数据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。

- **音量激活**

表示跟踪所有活动卷使用情况的进程。在有超过 1000 个卷处于活动状态的大型环境中，此过程会跟踪有多少个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，一些非关键卷将会出现此处标识的延迟。

- **\* 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的工作负载的高写入吞吐量或链路健康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，则不会显示此图标。

- **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。聚合由所有 HDD 组成，或由 HDD 和 SSD 的混合（Flash Pool 聚合）组成，或由 HDD 和云层的混合（FabricPool 聚合）组成。“SSD 聚合”由所有 SSD（全闪存聚合）或 SSD 和云层（FabricPool 聚合）的混合组成。

- **云延迟**

表示集群中涉及集群和存储用户数据的云层之间的 I/O 处理的软件组件。如果云延迟组件存在争用，则意味着托管在云层上的卷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，则意味着 SnapMirror 同步操作的活动正在影响一个或多个工作负载的延迟。

## 性能事件中涉及的工作负载的角色

Unified Manager 使用角色来识别工作负载在性能事件中的参与情况。角色包括受害者、欺凌者和鲨鱼。用户定义的工作负载可以同时是受害者、欺凌者和鲨鱼。

| 角色        | 描述                                                                                                                                     |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------|
| 受影响       | 一种用户定义的工作负载，由于其他工作负载（称为“bullies”）过度使用集群组件，导致其性能下降。只有用户定义的工作负载才会被识别为受害者。 Unified Manager 根据延迟偏差来识别受害工作负载，其中事件期间的实际延迟与其延迟预测（预期范围）相比大大增加。 |
| 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）的性能下降。 Unified Manager 根据集群组件使用情况的偏差来识别欺凌工作负载，其中事件期间的实际使用情况大大超出了其预期的使用范围。                       |
| 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，例如聚合以及用于网络和数据处理的 CPU。当工作负载（例如卷）对集群组件的使用率增加到该组件无法有效满足工作负载需求的程度时，该组件就会处于争用状态。过度使用集群组件的工作负载是一个恶霸。共享这些组件的其他工作负载，其性能受到欺凌的影响，是受害者。系统定义的工作负载（例如重复数据删除或 Snapshot 副本）的活动也可能升级为“欺凌”。

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，包括导致事件的欺凌工作负载、处于争用的集群组件以及由于欺凌工作负载活动增加而导致性能下降的受害工作负载。



如果 Unified Manager 无法识别欺凌工作负载，它只会对受害工作负载和所涉及的集群组件发出警报。

Unified Manager 可以识别受欺凌工作负载影响的工作负载，还可以识别这些工作负载何时成为欺凌工作负载。工作量本身就可能是一种负担。例如，受到策略组限制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。在正在进行的绩效事件中作为欺凌者或受害者的工作负载可能会改变其角色或不再是该事件的参与者。

## 管理绩效阈值

性能阈值策略使您能够确定 Unified Manager 生成事件的时间点，以便通知系统管理员可能影响工作负载性能的问题。这些阈值策略被称为\_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。通过动态和系统定义的性能阈值，Unified Manager 可以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。如果您从任何系统定义的性能阈值策略收到不必要的事件，您可以从事件设置页面禁用单个策略。

## 用户定义的性能阈值策略如何工作

您可以在存储对象（例如，聚合和卷）上设置性能阈值策略，以便可以向存储管理员发送事件，通知管理员集群正在遇到性能问题。

您可以通过以下方式为存储对象创建性能阈值策略：

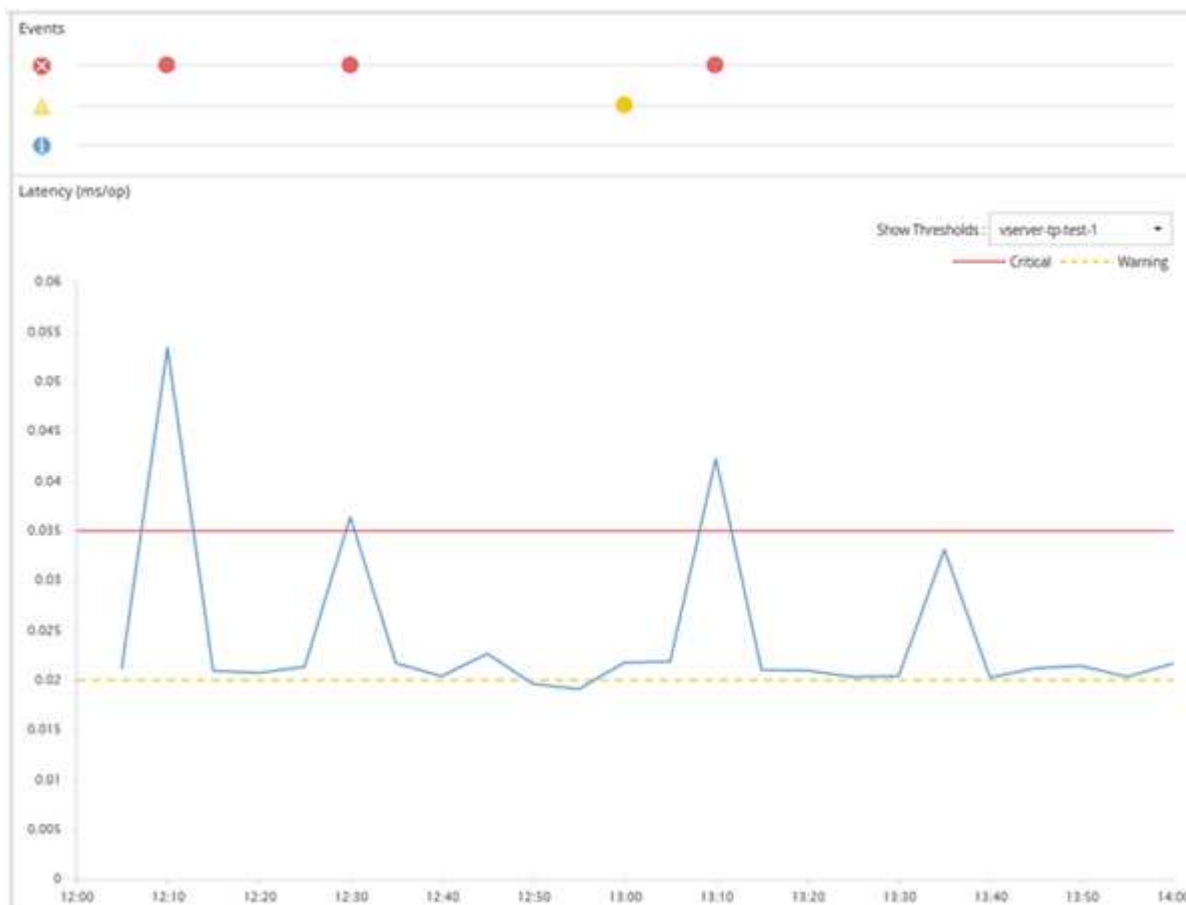
- 选择存储对象
- 选择与该对象关联的性能计数器
- 指定定义被视为警告和严重情况的性能计数器上限的值
- 指定一个时间段，定义计数器必须超过上限的时间

例如，您可以在卷上设置性能阈值策略，以便每当该卷的 IOPS 连续 10 分钟超过每秒 750 次操作时，您都会收到关键事件通知。相同的阈值策略还可以指定当 IOPS 超过每秒 500 次操作持续 10 分钟时发送警告事件。



当前版本提供了阈值，当计数器值超过阈值设置时，就会发送事件。您无法设置在计数器值低于阈值设置时发送事件的阈值。

此处显示了一个示例计数器图表，表明警告阈值（黄色图标）在 1:00 被突破，并且关键阈值（红色图标）在 12:10、12:30 和 1:10 被突破：



阈值突破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制值，则后续违规将被视为新持续时间的开始。

一些集群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 | 临界阈值 | 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当同时满足两个条件时才会生成事件。例如，使用表中定义的阈值策略：

| 如果音量延迟是平均的... | 并且总磁盘利用率是... | 操作       |
|---------------|--------------|----------|
| 15毫秒          | 50%          | 未报告任何事件。 |
| 15毫秒          | 75%          | 报告警告事件。  |
| 25毫秒          | 75%          | 报告警告事件。  |
| 25毫秒          | 90%          | 已报告严重事件。 |

### 当违反绩效阈值策略时会发生什么

当计数器值超过其定义的性能阈值并持续指定的时间量时，将突破阈值并报告事件。

该事件导致启动以下操作：

- 该事件显示在仪表板、性能集群摘要页面、事件页面和特定于对象的性能清单页面中。
- （可选）可以向一个或多个电子邮件收件人发送有关该事件的电子邮件警报，并且可以向陷阱接收器发送 SNMP 陷阱。
- （可选）可以执行脚本来自动修改或更新存储对象。

第一个动作总是被执行。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独特的操作。

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，此时该限制的持续时间将重置。当阈值不断被超出时，事件的结束时间会不断更新，以反映该事件正在进行中。

阈值事件捕获或冻结与严重性和策略定义相关的信息，以便唯一阈值信息随事件一起显示，即使将来修改阈值策略也是如此。

### 可以使用阈值跟踪哪些性能计数器

一些常见的性能计数器，例如 IOPS 和 MB/s，可以为所有存储对象设置阈值。还有其他计

计数器可以仅为某些存储对象设置阈值。

#### 可用的性能计数器

| 存储对象                      | 性能计数器                       | 描述                             |
|---------------------------|-----------------------------|--------------------------------|
| 集群                        | IOPS                        | 集群每秒处理的平均输入/输出操作数。             |
| MB/秒                      | 每秒传输到该集群和从该集群传输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                           |
| 每秒传输到该节点和从该节点传输的平均数据兆字节数。 | 延迟                          | 节点响应应用程序请求所需的平均毫秒数。            |
| 利用率                       | 节点的 CPU 和 RAM 的平均使用百分比。     | 已用性能容量                         |
| 节点消耗的性能容量的平均百分比。          | 已用性能容量 - 接管                 | 节点所消耗的性能容量的平均百分比，加上其伙伴节点的性能容量。 |
| 聚合                        | IOPS                        | 聚合每秒处理的平均输入/输出操作数。             |
| MB/秒                      | 每秒传输到该聚合体和从该聚合体传输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                    | 聚合所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                           |
| 每秒传输到和从此 SVM 的数据的平均兆字节数。  | 延迟                          | SVM 响应应用程序请求所需的平均毫秒数。          |
| 卷                         | IOPS                        | 该卷每秒处理的平均输入/输出操作数。             |
| MB/秒                      | 每秒传输到该卷和从该卷传输的平均数据兆字节数。     | 延迟                             |

| 存储对象                  | 性能计数器                           | 描述                                  |
|-----------------------|---------------------------------|-------------------------------------|
| 卷响应应用程序请求所需的平均毫秒数。    | 缓存未命中率                          | 来自客户端应用程序的读取请求中，从卷返回而不是从缓存返回的平均百分比。 |
| LUN                   | IOPS                            | LUN 每秒处理的平均输入/输出操作数。                |
| MB/秒                  | 每秒传输到该 LUN 和从该 LUN 传输的平均数据兆字节数。 | 延迟                                  |
| LUN 响应应用程序请求所需的平均毫秒数。 | 命名空间                            | IOPS                                |
| 命名空间每秒处理的输入/输出操作的平均数。 | MB/秒                            | 每秒传输到该命名空间和从该命名空间传输的平均数据兆字节数。       |
| 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                 | 正在使用的端口可用带宽的平均百分比。              | MB/秒                                |
| 每秒从该端口传输的平均数据兆字节数。    | 网络接口 (LIF)                      | MB/秒                                |

## 哪些对象和计数器可以组合使用阈值策略

组合策略中只能使用部分性能指标。当指定主性能计数器和辅助性能计数器时，两个性能计数器都必须超过其最大限制才会生成事件。

| 主存储对象和计数器  | 二级存储对象和计数器      |
|------------|-----------------|
| 卷延迟        | 卷 IOPS          |
| 体积 MB/s    | 聚合利用率           |
| 已用总性能容量    | 节点利用率           |
| 节点性能容量使用情况 | 节点性能容量使用情况 - 接管 |
| LUN延迟      | LUN IOPS        |
| LUN MB/秒   | 聚合利用率           |

|            |                 |
|------------|-----------------|
| 主存储对象和计数器  | 二级存储对象和计数器      |
| 已用总性能容量    | 节点利用率           |
| 节点性能容量使用情况 | 节点性能容量使用情况 - 接管 |



当卷组合策略应用于FlexGroup卷而不是FlexVol volume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，并且您将收到描述这种情况的错误消息。这是因为FlexGroup卷可以存在于多个节点或聚合上。

### 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。事件通知表明集群正在经历性能问题。

开始之前

您必须具有应用程序管理员角色。

您可以通过在“创建性能阈值策略”页面上输入阈值来创建性能阈值策略。您可以通过定义此页面中的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\_）。

有效阈值为数字 0.001 到 10,000,000、百分比 0.001-100 和性能容量使用百分比 0.001-200。



当前版本提供了阈值，当计数器值超过阈值设置时，就会发送事件。您无法设置在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”。

将显示“性能阈值”页面。

2. 根据您是想构建新策略还是想克隆类似策略并修改克隆版本来单击相应的按钮。

| 目的     | 点击...         |
|--------|---------------|
| 创建新策略  | 创造            |
| 克隆现有策略 | 选择现有策略并单击*克隆* |

进入“创建性能阈值策略”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为策略指定名称和描述。
  - 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。



您必须定义至少一个警告限制或一个临界限制。您不需要定义两种类型的限制。

c. 如果需要，选择一个辅助性能计数器，并指定警告和严重事件的限制值。

包括辅助计数器要求两个计数器都超过限制值，然后才会突破阈值并报告事件。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会发送事件的持续时间。

克隆现有策略时，必须为该策略输入新名称。

4. 单击“保存”以保存该策略。

您将返回到“性能阈值”页面。页面顶部的成功消息确认阈值策略已创建，并提供该对象类型的库存页面链接，以便您可以立即将新策略应用于存储对象。

如果此时您想将新的阈值策略应用于存储对象，您可以单击“立即转到 object\_type”链接转到“库存”页面。

### 为存储对象分配性能阈值策略

您可以将用户定义的性能阈值策略分配给存储对象，以便当性能计数器的值超过策略设置时，Unified Manager 会报告事件。

开始之前

您必须具有应用程序管理员角色。

您要应用于对象的性能阈值策略或策略必须存在。

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。将策略分配给多个对象时，如果任何对象已分配最大数量的策略，则 Unified Manager 将执行以下操作：

- 将策略应用于所有未达到最大值的选定对象
- 忽略已达到最大策略数量的对象
- 显示一条消息，表明该策略未分配给所有对象

步骤

1. 从任意存储对象的性能清单页面中，选择要分配阈值策略的一个或多个对象：

| 分配阈值给... | 点击...                                                                                                        |
|----------|--------------------------------------------------------------------------------------------------------------|
| 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 | 这  下拉框，然后选择“选择此页面上的所有对象”。 |

|           |                                                                                                       |
|-----------|-------------------------------------------------------------------------------------------------------|
| 分配阈值给...  | 点击...                                                                                                 |
| 所有同一类型的对象 | 这  下拉框，然后选择*选择所有对象*。 |

您可以使用排序和过滤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. 做出选择，然后单击“分配性能阈值策略”。

将显示“分配性能阈值策略”页面，其中显示了针对该特定类型存储对象存在的阈值策略列表。

- 3. 单击每个策略以显示性能阈值设置的详细信息，以验证您是否选择了正确的阈值策略。
- 4. 选择适当的阈值策略后，单击“分配策略”。

页面顶部的成功消息确认阈值策略已分配给该对象或多个对象，并提供指向警报页面的链接，以便您可以为该对象和策略配置警报设置。

如果您希望通过电子邮件发送警报或以 SNMP 陷阱的形式通知您已生成特定性能事件，则必须在警报设置页面中配置警报设置。

### 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，其中包括针对所有类型存储对象的策略。您可以单击列标题来按该列对策略进行排序。如果您正在寻找特定的策略，请使用过滤和搜索机制来优化库存列表中出现的阈值策略列表。

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来创建、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”。

将显示“性能阈值”页面。

### 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。如果您发现收到的某些阈值条件下的警报过多或过少，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。

您无法更改现有阈值策略的策略名称或正在监视的存储对象的类型。

#### 步骤

- 1. 在左侧导航窗格中，选择“事件阈值”>“性能”。

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”。

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”。

您将返回到“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上。

根据您对策略所做更改的类型，您可能需要查看在警报设置页面中为使用该策略的对象配置的警报设置。

从存储对象中删除性能阈值策略

当您不再希望 Unified Manager 监控性能计数器的值时，您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。

每次只能从选定对象中删除一个策略。

您可以通过在列表中选择多个存储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\*库存\*页面中，选择一个或多个应用了至少一个性能阈值策略的对象。

| 清除...的阈值 | 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 | 点击  在列标题中。 |

2. 单击“清除性能阈值策略”。

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”。

当您选择阈值策略时，将显示该策略的详细信息，以便您确认已选择适当的策略。

当性能阈值策略改变时会发生什么

如果调整现有性能阈值策略的计数器值或持续时间，则策略更改将应用于使用该策略的所有存储对象。新的设置会立即生效，并且 Unified Manager 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过时，并且阈值策略将开始作为新定义的阈值策略监视计数器。

在计数器图表详细视图中查看已应用阈值的计数器时，临界阈值线和警告阈值线反映当前阈值设置。即使您查看旧阈值设置生效时的历史数据，原始阈值设置也不会出现在此页面上。



由于较旧的阈值设置不会出现在计数器图表详细视图中，因此您可能会看到出现在当前阈值线以下的历史事件。

## 当对象移动时性能阈值策略会发生什么变化

由于性能阈值策略被分配给存储对象，因此如果您移动某个对象，则在移动完成后，所有分配的阈值策略仍会附加到该对象。例如，如果您将卷或 LUN 移动到不同的聚合，则阈值策略对于新聚合上的卷或 LUN 仍然有效。

如果阈值策略（组合策略）存在辅助计数器条件（例如，如果为聚合或节点分配了附加条件），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。

如果对于使用更改后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过时，并且阈值策略将开始按照新定义的阈值策略监视计数器。

卷移动操作会导致ONTAP发送信息更改事件。性能资源管理器页面和工作负载分析页面的事件时间线中会出现一个更改事件图标，指示移动操作完成的时间。



如果将对象移动到不同的集群，则会从该对象中删除用户定义的阈值策略。如果需要，您必须在移动操作完成后为对象分配阈值策略。然而，动态和系统定义的阈值策略会在对象移动到新集群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还操作时，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更改，因此直到下次轮询集群配置时才能确定切换到新节点的影响。



如果接管和交还操作都发生在 15 分钟的配置更改收集期内，您可能看不到性能统计信息从一个节点移动到另一个节点。

## 聚合迁移期间的阈值策略功能

如果使用 `aggregate relocation start` 命令，单一和组合阈值策略都会保留在所有对象上，并且阈值策略的节点部分会应用于新节点。

## 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，您可以对已移动到伙伴集群的卷和 LUN 应用阈值策略。当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，请参阅["切换和切回期间的卷行为"](#)。

# 分析性能事件

您可以分析性能事件以确定何时检测到它们、它们是活动的（新的或已确认的）还是过时的、所涉及的工作负载和集群组件，以及自行解决事件的选项。

## 显示有关性能事件的信息

您可以使用事件管理库存页面查看 Unified Manager 监控的集群上的所有性能事件的列表。通过查看这些信息，您可以确定最关键的事件，然后深入了解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，最新事件列在最前面。您可以单击列标题来根据该列对事件进行排序。例如，您可以按状态列排序以按严重性查看事件。如果您正在寻找特定事件或特定类型的事件，您可以使用过滤器和搜索机制来优化列表中出现的事件列表。

所有来源的事件都显示在此页面上：

- 用户自定义性能阈值策略
- 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以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. 从“查看”菜单中，选择“活动性能事件”。

该页面显示过去 7 天内生成的所有新的和已确认的绩效事件。

3. 找到您要分析的事件并单击事件名称。

将显示事件的详细信息页面。



您还可以通过单击“性能资源管理器”页面和警报电子邮件中的事件名称链接来显示事件的详细信息页面。

## 根据用户定义的性能阈值分析事件

从用户定义的阈值生成的事件表明某个存储对象（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。这表明集群对象正在遇到性能问题。

您可以使用事件详细信息页面来分析性能事件，并在必要时采取纠正措施，使性能恢复正常。

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过用户定义的警告或严重阈值而导致的性能事件。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。
- 必须有新的或过时的表演事件。

步骤

1. 显示\*活动详情\*页面以查看有关活动的信息。
2. 查看\*描述\*，其中描述了导致该事件的阈值违规。

例如，消息“456 ms/op 的延迟值根据 400 ms/op 的阈值设置触发了警告事件”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、必须违反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\*，以便您可以调查是否可能同时发生其他可能导致此事件的事件。
5. 按照以下选项之一进一步调查该事件，以确定是否需要执行任何操作来解决性能问题：

| 选项                     | 可能采取的调查行动                                                                          |
|------------------------|------------------------------------------------------------------------------------|
| 单击源对象名称可显示该对象的资源管理器页面。 | 此页面使您能够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在同一时间存在性能问题。例如，查看同一聚合上的其他卷是否也存在性能问题。 |
| 单击集群名称即可显示集群摘要页面。      | 此页面使您能够查看此对象所在集群的详细信息，以查看是否在同一时间发生了其他性能问题。                                         |

根据系统定义的性能阈值分析事件

从系统定义的性能阈值生成的事件表明某个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。这表明存储对象（例如聚合或节点）正在遇到性能问题。

您可以使用事件详细信息页面来分析性能事件，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。

响应系统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过系统定义的警告阈值而导致的性能事

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表演事件。

#### 步骤

1. 显示\*活动详情\*页面以查看有关活动的信息。
2. 查看\*描述\*，其中描述了导致该事件的阈值违规。

例如，消息“节点利用率值 90% 根据阈值设置 85% 触发了警告事件”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\*，以便您可以调查是否可能同时发生其他可能导致此事件的事件。
4. 在\*系统诊断\*下，查看系统定义的策略对集群对象执行的分析类型的简要描述。

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“建议的操作”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，以尝试自行解决性能事件。

#### 响应 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、公认的或过时的绩效事件。

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 会生成违反 QoS 策略的警告事件。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 在图表上仅显示收集期间的“平均”吞吐量。因此，您可能会收到 QoS 事件，而工作负载的吞吐量可能尚未超过图表中显示的策略阈值。

您可以使用 System Manager 或ONTAP命令来管理策略组，包括以下任务：

- 为工作负载创建新的策略组
- 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
- 将工作负载移动到不同的聚合或节点

#### 步骤

1. 显示\*活动详情\*页面以查看有关活动的信息。
2. 查看\*描述\*，其中描述了导致该事件的阈值违规。

例如，消息“vol1\_NFS1 上的 IOPS 值为 1,352 IOPS 已触发警告事件以识别工作负载的潜在性能问题”表示在卷 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和事件持续时长的更多详细信息。

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。通过这种方式安排，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，吞吐量图表中显示前三个工作负载。如果有三个以上的工作负载共享 QoS 策略，则其他工作负载将被添加到“其他工作负载”类别中。此外，延迟图表显示 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 根据卷大小从分配的 IOPS/TB 阈值策略转换的 IOPS 或 MBps 值。

5. 在“建议的操作”部分下，查看建议并确定应执行哪些操作以避免工作负载延迟增加。

如果需要，请单击“帮助”按钮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。

了解具有定义块大小的自适应 **QoS** 策略中的事件

自适应 QoS 策略组根据卷大小自动扩展吞吐量上限或下限，并在卷大小发生变化时保持 IOPS 与 TB 的比率。从 ONTAP 9.5 开始，您可以在 QoS 策略中指定块大小，以便同时有效地应用 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进行限制。根据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，因此给处理操作的节点带来更大的负担。

工作负载的 MB/s 值是使用以下公式生成的：

$$\text{MB/s} = (\text{IOPS} * \text{Block Size}) / 1000$$

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，则该工作负载的有效 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，则该工作负载的有效 MB/s 为 144。您可以看到，当块大小较大时，节点处理的数据增加了 50%。

让我们看一下具有定义块大小的以下自适应 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。对于已使用容量为 1 TB 的卷，这实际上将 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。在以下情况下会生成事件：



| 已用容量 | 当吞吐量超过此数量时会生成事件... |          |
|------|--------------------|----------|
|      | IOPS               | MB/秒     |
| 1 TB | 2,250 IOPS         | 72 MB/秒  |
| 2 TB | 4,500 IOPS         | 144 MB/秒 |
| 5 TB | 11,250 IOPS        | 360MB/秒  |

如果卷使用 2TB 可用空间，IOPS 为 4,000，且客户端上的 QoS 块大小设置为 32KB，则 MB/ps 吞吐量为 128 MB/s  $((4,000 \text{ IOPS} * 32 \text{ KB}) / 1000)$ 。在这种情况下不会生成任何事件，因为 4,000 IOPS 和 128 MB/s 均低于使用 2 TB 空间的卷的阈值。

如果卷使用 2TB 可用空间，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  $((4,000 \text{ IOPS} * 64 \text{ KB}) / 1000)$ 。在这种情况下，4,000 IOPS 不会生成事件，但 256 MB/s 的 MB/s 值高于 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，则会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，请参阅 ["绩效管理概述"](#)。

#### 响应节点资源过度利用的性能事件

当单个节点的运行超出其运行效率界限时，Unified Manager 会生成节点资源过度利用警告事件，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。
- 必须有新的或过时的表演事件。

Unified Manager 通过查找性能容量使用率超过 100% 且持续时间超过 30 分钟的节点，生成违反节点资源过度利用策略的警告事件。

您可以使用 System Manager 或 ONTAP 命令来纠正此类性能问题，包括以下任务：

- 创建并应用 QoS 策略到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
- 将工作负载移动到不同的聚合或节点
- 通过向节点添加磁盘或升级到具有更快 CPU 和更多 RAM 的节点来增加容量

#### 步骤

1. 显示\*活动详情\*页面以查看有关活动的信息。
2. 查看\*描述\*，其中描述了导致该事件的阈值违规。

例如，消息“Perf. simple-02 上的容量使用值为 139%，已触发警告事件，以识别数据处理单元中的潜在性能问题。”表示节点 simple-02 上的性能容量已过度使用，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的延迟。按照这种方式排列，您可以看到哪些工作负载是导致节点延迟的原因。

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，哪些工作负载没有应用。

4. 在“建议的操作”部分下，查看建议并确定应执行哪些操作以避免工作负载延迟增加。

如果需要，请单击“帮助”按钮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。

## 响应集群不平衡性能事件

当集群中某个节点的负载远高于其他节点时，Unified Manager 会生成集群不平衡警告事件，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来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。

这些步骤可帮助您识别以下资源，以便您可以将高性能工作负载移动到利用率较低的节点：

- 同一集群中利用率较低的节点
- 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该事件的信息。
2. 查看\*描述\*，其中描述了导致该事件的阈值违规。

例如，消息“性能容量使用计数器指示集群 Dallas-1-8 上的节点之间的负载差异为 62%，并根据系统阈值 30% 触发了警告事件”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“建议的操作”中的文本，将高性能卷从具有高性能容量使用值的节点移动到具有最低性能容量使用值的节点。
4. 确定性能容量使用值最高和最低的节点：
  - a. 在“事件信息”部分中，单击源集群的名称。
  - b. 在“集群/性能摘要”页面中，单击“管理对象”区域中的“节点”。
  - c. 在“节点”库存页面中，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下这些名称。
5. 确定具有最高性能容量使用值的节点上使用最多 IOPS 的卷：

- a. 单击性能容量使用值最高的节点。
  - 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. 确定具有最低性能容量使用值的节点上利用率最低的聚合：
- a. 单击“存储”>“聚合”以显示“聚合”库存页面。
  - 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 中记下的具有最低性能容量使用值的节点的名称。
  - d. 记下具有最低性能容量使用值的聚合的名称。
7. 将卷从过载节点移动到您确定为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，检查您是否从该集群收到相同的集群不平衡事件。

## 根据动态性能阈值分析事件

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）太高或太低。您可以使用事件详细信息页面来分析性能事件，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系统上未启用动态性能阈值。

### 识别动态性能事件中涉及的受害工作负载

在 Unified Manager 中，您可以确定哪些卷工作负载因存储组件争用而导致响应时间（延迟）偏差最大。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运行速度比平时慢。

#### 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、公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，按组件活动或使用情况的最大偏差或受事件影响最大的程度排序。这些值基于 Unified Manager 在检测和上次分析事件时识别的峰值。

#### 步骤

1. 显示\*活动详情\*页面以查看有关活动的信息。
2. 在工作负载延迟和工作负载活动图表中，选择\*受害者工作负载\*。

3. 将光标悬停在图表上，可以查看影响组件的顶级用户定义工作负载以及受害工作负载的名称。

#### 识别动态性能事件中涉及的工作负载

在 Unified Manager 中，您可以确定哪些工作负载对于争用的集群组件的使用偏差最大。识别这些工作负载有助于您了解集群上的某些卷响应时间（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、公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，按组件使用率最高或受事件影响最大的程度排序。这些值基于 Unified Manager 在检测和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“工作负载延迟”和“工作负载活动”图表中，选择“Bully Workloads”。
3. 将光标悬停在图表上，查看影响组件的顶级用户定义欺凌工作负载。

#### 识别动态性能事件中涉及的shark工作负载

在 Unified Manager 中，您可以确定哪些工作负载对于争用的存储组件的使用偏差最大。识别这些工作负载有助于您确定是否应将这些工作负载移动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、已确认的或已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，按组件使用率最高或受事件影响最大的程度排序。这些值基于 Unified Manager 在检测和上次分析事件时识别的峰值。

##### 步骤

1. 显示\*活动详情\*页面以查看有关活动的信息。
2. 在工作负载延迟和工作负载活动图表中，选择 **Shark Workloads**。
3. 将光标悬停在图表上，查看影响组件的顶级用户定义工作负载以及 shark 工作负载的名称。

#### MetroCluster配置的性能事件分析

您可以使用 Unified Manager 分析MetroCluster配置的性能事件。您可以识别事件中涉及的工作负载并查看解决该事件的建议操作。

MetroCluster性能事件可能是由于过度利用集群之间的交换机间链路 (ISL) 的 `_bully_` 工作负载，或由于链路健康问题造成的。Unified Manager 独立监控MetroCluster配置中的每个集群，而不考虑伙伴集群上的性能事件。

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”页面来检查每个集群的运行状况并查看它们的关系。

您可以使用 Unified Manager 分析MetroCluster配置中检测到性能事件的集群。您可以识别集群名称、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

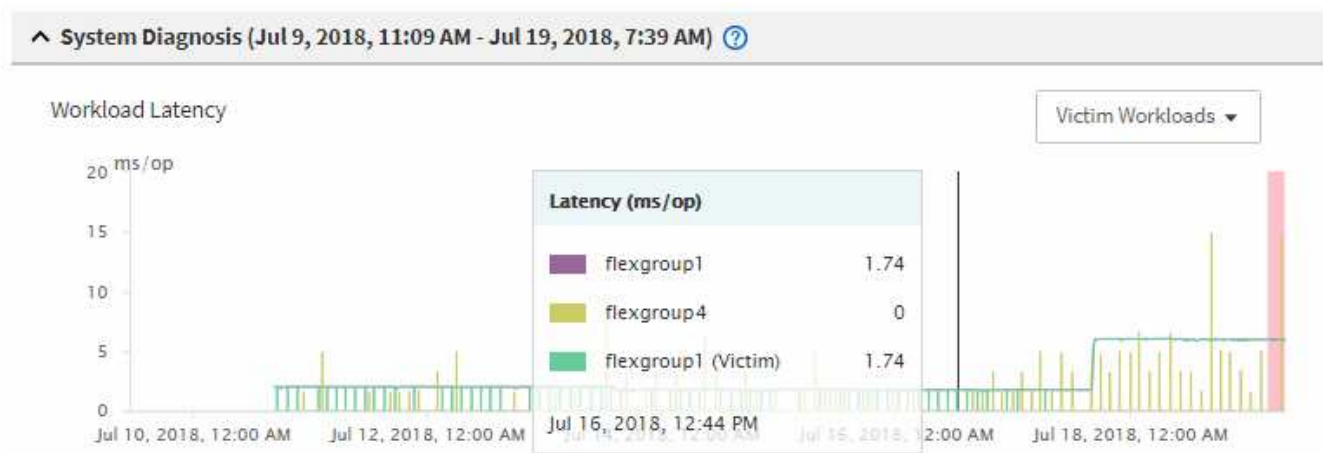
1. 显示\*活动详情\*页面以查看有关活动的信息。
2. 查看事件描述以了解所涉及的工作负载的名称以及所涉及的工作负载的数量。

在此示例中， MetroCluster资源图标为红色，表示MetroCluster资源处于争用状态。将光标放在图标上即可显示该图标的描述。



3. 记下集群名称和事件检测时间，您可以使用它们来分析伙伴集群上的性能事件。
4. 在图表中，查看\_受害者\_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。延迟图表从高层次显示了所涉及的受害工作负载的一致延迟模式。即使受害工作负载的异常延迟触发了该事件，一致的延迟模式可能表明工作负载在其预期范围内执行，但 I/O 的峰值增加了延迟并触发了该事件。



如果您最近在访问这些卷工作负载的客户端上安装了应用程序，并且该应用程序向它们发送大量 I/O，那么您可能会预计它们的延迟会增加。如果工作负载的延迟恢复到预期范围内，事件状态变为过时，并保持此状态超过 30 分钟，您可能可以忽略该事件。如果事件正在进行，并且保持新状态，您可以进一步调查以确定是否有其他问题导致了该事件。

5. 在工作负载吞吐量图表中，选择 **Bully Workloads** 来显示负载较大的工作负载。

存在欺凌工作负载表明该事件可能是由于本地集群上的一个或多个工作负载过度利用MetroCluster资源而导致的。欺负工作负载的写入吞吐量（MB/s）偏差较大。

该图表从总体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 模式来识别异常吞吐量，这可能表明工作负载过度利用了MetroCluster资源。

如果事件中不涉及任何欺凌工作负载，则该事件可能是由集群之间的链接的健康问题或伙伴集群上的性能问题引起的。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 检查和分析合作伙伴集群上的性能事件。

#### 分析MetroCluster配置上的远程集群的动态性能事件

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。
- 您必须已经分析了MetroCluster配置中本地集群上的性能事件并获取了事件检测时间。
- 您必须检查涉及性能事件的本地集群及其伙伴集群的健康状况，并获取伙伴集群的名称。

#### 步骤

1. 登录到正在监控合作伙伴集群的 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\*过去一小时\*，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\*，在文本字段中输入合作伙伴集群的名称，然后单击\*应用过滤器\*。

如果所选集群在过去一小时内没有发生任何事件，则表明该集群在其伙伴集群上检测到该事件期间没有遇到任何性能问题。

5. 如果选定集群在过去一小时内检测到事件，则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。

如果这些事件涉及导致数据处理组件争用的霸凌工作负载，则这些霸凌者中的一个或多个可能在本地集群上引发了该事件。您可以单击该事件来分析它，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凌工作负载，则它们不会导致本地集群上的性能事件。

#### 响应由 QoS 策略组限制引起的动态性能事件

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) 所导致的性能事件。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来确定是否需要策略组施加新的限制以停止限制。

#### 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。

- 必须有新的、公认的或过时的绩效事件。

## 步骤

1. 显示\*活动详情\*页面以查看有关活动的信息。
2. 阅读\*描述\*，其中显示受限制影响的工作负载的名称。



描述可以显示受害者和欺凌者的相同工作负载，因为限制使工作负载成为其自身的受害者。

3. 使用文本编辑器等应用程序记录卷的名称。

您可以稍后搜索卷名来找到它。

4. 在“工作负载延迟”和“工作负载利用率”图表中，选择“Bully Workloads”。
5. 将光标悬停在图表上，即可查看影响策略组的主要用户定义工作负载。

列表顶部的工作负载偏差最大，导致发生节流。活动是个工作负载使用的策略组限制的百分比。

6. 在“建议的操作”区域中，单击排名靠前的工作负载的“分析工作负载”按钮。
7. 在工作负载分析页面中，设置延迟图表查看所有集群组件，设置吞吐量图表查看细分。

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，以查看在事件发生时多少限制量影响了延迟。

QoS 策略组的最大吞吐量为每秒 1,000 个操作 (op/sec)，其中的工作负载总和不能超过该吞吐量。事件发生时，策略组中的工作负载的合并吞吐量超过 1,200 操作/秒，这导致策略组将其活动限制回 1,000 操作/秒。

9. 将\*读取/写入延迟\*值与\*读取/写入/其他\*值进行比较。

两个图表都显示读取请求数量较多且延迟较高，但写入请求的数量和延迟量较低。这些值可帮助您确定是否存在大量吞吐量或大量操作增加了延迟。在决定对吞吐量或操作设置策略组限制时，您可以使用这些值。

10. 使用ONTAP系统管理器将策略组的当前限制增加到 1,300 op/sec。
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. 选择吞吐量细分图表。

显示读取/写入/其他图表。

13. 在页面顶部，将光标指向更改事件图标 (●) 来更改策略组限制。
14. 将\*读取/写入/其他\*图表与\*延迟\*图表进行比较。

读写请求相同，但节流已停止，延迟也减少了。

## 响应由磁盘故障引起的动态性能事件

您可以使用 Unified Manager 调查由工作负载过度利用聚合所导致的性能事件。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、公认的或过时的绩效事件。

步骤

1. 显示\*活动详情\*页面以查看有关活动的信息。
2. 阅读\*描述\*，其中描述了事件所涉及的工作负载和争用的集群组件。

有多个受害卷的延迟受到争用中的集群组件的影响。聚合体处于 RAID 重建过程中，用备用磁盘替换故障磁盘，是处于争用的集群组件。在“争用中的组件”下，“聚合”图标以红色突出显示，并且聚合的名称显示在括号中。

3. 在工作负载利用率图表中，选择 **Bully Workloads**。
4. 将光标悬停在图表上，可以查看影响该组件的主要工作负载。

自检测到事件以来峰值利用率最高的工作负载显示在图表顶部。最重要的工作负载之一是系统定义的工作负载磁盘健康，它表示 RAID 重建。重建是使用备用磁盘重建聚合所涉及的内部过程。磁盘运行状况工作负载以及聚合上的其他工作负载可能会导致聚合上的争用和相关事件。

5. 确认磁盘运行状况工作负载的活动导致该事件后，等待大约 30 分钟以完成重建，并等待 Unified Manager 分析该事件并检测聚合是否仍处于争用状态。
6. 刷新\*活动详情\*。

RAID重建完成后，查看State为obsolete，表示事件已解决。

7. 在“工作负载利用率”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“建议的操作”区域中，单击排名靠前的工作负载的“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所选卷的过去 24 小时（1 天）的数据。

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。

事件发生时，聚合利用率显示大量读写活动，这是由 RAID 重建过程引起的，这增加了所选卷的延迟。事件发生几个小时后，读写和延迟均有所减少，证实聚合不再存在争用。

响应由 HA 接管引起的动态性能事件

您可以使用 Unified Manager 调查由高可用性 (HA) 对中的集群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、公认的或过时的绩效事件。

#### 步骤

1. 显示\*活动详情\*页面以查看有关活动的信息。
2. 阅读\*描述\*，其中描述了事件所涉及的工作负载和争用的集群组件。

有一个受害卷的延迟受到争用的集群组件的影响。数据处理节点从其伙伴节点接管了所有工作负载，是处于争用的集群组件。在“争用中的组件”下，“Data Processing”图标以红色突出显示，并且在事件发生时处理数据处理的节点的名称显示在括号中。

3. 在“描述”中，单击卷的名称。

将显示卷性能资源管理器页面。在页面顶部的事件时间线中，有一个更改事件图标 (  ) 表示 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，悬停文本将显示有关 HA 接管的详细信息。

在延迟图表中，事件表明所选卷在 HA 接管的同时由于高延迟而超过了性能阈值。

5. 单击“缩放视图”以在新页面上显示延迟图表。
6. 在“查看”菜单中，选择“集群组件”以查看集群组件的总延迟。
7. 将鼠标光标指向 HA 接管开始的更改事件图标，并将数据处理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，数据处理量出现激增。CPU 利用率的增加增加了延迟并触发了该事件。

8. 修复故障节点后，使用ONTAP系统管理器执行 HA 交还，将工作负载从合作伙伴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 库存页面中找到由 HA 接管触发的事件和工作负载。

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。数据处理组件的延迟减少了，从而降低了总延迟。选定卷现在用于数据处理的节点已解决该事件。

## 解决性能事件

您可以使用建议的操作来尝试自行解决性能事件。前三个建议始终显示，第四个建议下的操作特定于所显示的事件类型。

\*帮助我执行此操作\*链接为每个建议的操作提供了附加信息，包括执行特定操作的说明。某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。

### 确认延迟在预期范围内

当集群组件处于争用状态时，使用该组件的卷工作负载可能会减少响应时间（延迟）。您可以检查争用组件上每个受害者工作负载的延迟，以确认其实际延迟在预期范围内。您还可以单击卷名称来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。

## 审查配置更改对工作负载性能的影响

集群上的配置更改（例如磁盘故障、HA 故障转移或移动卷）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，了解最近配置更改发生的时间，并将其与操作和延迟（响应时间）进行比较，以查看所选卷工作负载的活动是否发生了变化。

Unified Manager 的性能页面只能检测有限数量的变化事件。健康页面提供由配置更改引起的其他事件的警报。您可以在 Unified Manager 中搜索该卷以查看事件历史记录。

## 从客户端提高工作负载性能的选项

您可以检查向涉及性能事件的卷发送 I/O 的客户端工作负载（例如应用程序或数据库），以确定客户端更改是否可以纠正该事件。

当连接到集群上的卷的客户端增加其 I/O 请求时，集群必须更加努力地满足需求。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该卷的客户端数量或减少该卷的 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，以确定客户端是否发送了比平时更多的 I/O，这可能会导致集群组件争用。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顶级卷工作负载。如果您知道哪个客户端正在访问特定卷，您可以转到该客户端来确定客户端硬件或应用程序是否未按预期运行或是否比平时做更多的工作。

在 MetroCluster 配置中，对本地集群上的卷的写入请求将镜像到远程集群上的卷。保持本地集群上的源卷与远程集群上的目标卷同步也会增加 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，从而减少对其他工作负载的性能影响。

## 检查客户端或网络问题

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。集群需求的增加可能会导致组件争用，增加使用该组件的工作负载的延迟，并在 Unified Manager 中触发事件。

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顶级卷工作负载。如果您知道哪个客户端正在访问特定卷，您可以转到该客户端来确定客户端硬件或应用程序是否未按预期运行或是否比平时做更多的工作。您可能需要联系客户管理员或应用程序供应商寻求帮助。

您可以检查网络基础设施，以确定是否存在硬件问题、瓶颈或竞争工作负载，这些问题可能导致集群和连接的客户端之间的 I/O 请求执行速度比预期慢。您可能需要联系网络管理员寻求帮助。

## 验证 QoS 策略组中的其他卷是否具有异常高的活动

您可以查看服务质量 (QoS) 策略组中活动变化最大的工作负载，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定的吞吐量限制，或者是否已回到预期的活动范围内。

在“事件详细信息”页面的“系统诊断”部分中，您可以按活动峰值偏差对工作负载进行排序，以将活动变化最大的

工作负载显示在表格顶部。这些工作负载可能是“欺凌者”，其活动超出了设定的限制，并可能导致了该事件的发生。

您可以导航到每个卷工作负载的工作负载分析页面来查看其 IOPS 活动。如果工作负载在某个时期的操作活动非常频繁，则可能对该事件有所贡献。您可以更改工作负载的策略组设置或将工作负载移动到其他策略组。

您可以使用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。

### 移动逻辑接口 (LIF)

将逻辑接口 (LIF) 移动到不太繁忙的端口可以帮助改善负载平衡、协助维护操作和性能调整，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，让ONTAP自动将繁忙的 LIF 移动到其他端口，或者您可以手动移动 LIF。

| 好处                                                                          | 注意事项                                                                                                                                                                       |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• 改善负载平衡。</li><li>• 减少间接访问。</li></ul> | <div><div>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。</div></div> |

您可以使用ONTAP命令来配置负载平衡。有关更多信息，请参阅ONTAP网络文档。

您可以使用ONTAP系统管理器和ONTAP CLI 命令手动移动 LIF。

### 在不太繁忙的时间运行存储效率操作

您可以修改处理存储效率操作的策略或计划，以便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占用大量集群 CPU 资源，并成为运行操作的卷的负担。如果在运行存储效率操作的同时受害卷具有较高的活动性，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峰值偏差显示 QoS 策略组中的工作负载，以识别欺凌工作负载。如果您看到表格顶部附近显示“存储效率”，则这些操作正在欺负受害者工作负载。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，您可以防止存储效率操作引起集群争用。

您可以使用ONTAP系统管理器来管理效率策略。您可以使用ONTAP命令来管理效率策略和计划。

## 什么是存储效率

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 的存储效率策略基于其核心ONTAP操作系统和随处写入文件布局 (WAFL) 文件系统提供的内置存储虚拟化和统一存储基础。

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、闪存、Flash Pool 聚合和支持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一平台上有效地整合存储区域网络 (SAN)、网络附加存储 (NAS) 和二级存储。

高密度磁盘驱动器（例如在 Flash Pool 聚合内配置的串行高级技术附件 (SATA) 驱动器或使用 Flash Cache 和 RAID-DP 技术配置的串行高级技术附件 (SATA) 驱动器）可提高效率，而不会影响性能和弹性。

启用FabricPool的聚合包括全 SSD 聚合或 HDD 聚合（从ONTAP 9.8 开始）作为本地性能层和指定为云层的对象存储。配置FabricPool可帮助您根据数据是否经常被访问来管理应存储哪个存储层（本地层或云层）。

精简配置、Snapshot 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等技术可以实现更好的节省。您可以单独或一起使用这些技术来实现最大的存储效率。

## 添加磁盘并重新分配数据

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，只有在添加的磁盘之间重新分配数据后，您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：

- 当您收到动态阈值事件时，在事件详细信息页面上，代表争用聚合的集群组件图标将以红色突出显示。

图标下方的括号中是聚合的名称，用于标识可以添加磁盘的聚合。

- 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并重新分配数据。

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，您可能需要联系管理员或购买更多磁盘。您可以使用ONTAP系统管理器或ONTAP命令将磁盘添加到聚合。



仅在使用 HDD 和 Flash Pool 聚合时才应重新分配数据。不要在 SSD 或FabricPool聚合上重新分配数据。

## 在节点上启用闪存如何提高工作负载性能

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。

闪存模块（或基于 PCIe 的性能加速模块）通过充当智能外部读取缓存来优化随机读取密集型工作负载的性能。该硬件与ONTAP的WAFL外部缓存软件组件协同工作。

在 Unified Manager 的“事件详细信息”页面上，代表争用聚合的集群组件图标以红色突出显示。图标下方的括号中是聚合的名称，用于标识聚合。您可以在聚合所在的节点上启用闪存。

您可以使用 ONTAP System Manager 或 ONTAP 命令查看 Flash Cache 是否已安装或启用，如果尚未启用，则启用它。以下命令指示特定节点上是否启用了 Flash Cache：**cluster::> run local options flexscale.enable**

有关 Flash Cache 及其使用要求的更多信息，请参阅以下技术报告：

["技术报告 3832：闪存缓存最佳实践指南"](#)

## 在存储聚合上启用 **Flash Pool** 可以如何提高工作效率

您可以通过在聚合上启用 Flash Pool 功能来提高工作效率。Flash Pool 是包含 HDD 和 SSD 的聚合体。HDD 用于主存储，SSD 提供高性能读写缓存以提高总体性能。

在 Unified Manager 中，“事件详细信息”页面显示存在争用的聚合的名称。您可以使用 ONTAP 系统管理器或 ONTAP 命令来查看是否为聚合启用了 Flash Pool。如果您安装了 SSD，则可以使用命令行界面来启用它。如果您安装了 SSD，则可以在聚合上运行以下命令来查看 Flash Pool 是否已启用：**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 及其使用要求的更多信息，请参阅《集群模式 Data ONTAP 物理存储管理指南》。

## MetroCluster 配置健康检查

您可以使用 Unified Manager 通过 IP 或 FC 查看 MetroCluster 配置中集群的运行状况。健康状况和事件可帮助您确定是否存在可能影响工作效率的硬件或软件问题。

如果您将 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可能导致性能事件的本地或远程集群的任何健康问题。在 Unified Manager GUI 中，您可以选择 事件管理 来查看当前事件列表，然后使用过滤器仅显示 MetroCluster 配置事件。

有关详细信息，请参阅["检查 MetroCluster 配置中集群的运行状况"](#)

## MetroCluster 配置验证

通过确保正确设置 MetroCluster 配置，您可以防止 MetroCluster 通过 FC 和 IP 配置中的镜像工作效率出现性能问题。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效率。

参考 ["MetroCluster 文档"](#) 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与镜像卷数据进行通信。有关 MetroCluster over IP 设置的特定信息，请参阅 ["安装 MetroCluster IP 配置"](#)。

您可以将 MetroCluster 配置与 ["MetroCluster 文档"](#) 确定更改或升级 MetroCluster 配置中的组件是否可以提高工作效率。这个比较可以帮助您回答以下问题：

- 这些控制器是否适合您的工作效率？

- 您是否需要将 ISL 捆绑升级到更大的带宽以处理更多的吞吐量？
- 您能否调整交换机上的缓冲区到缓冲区信用（BBC）来增加带宽？
- 如果您的工作负载对固态硬盘 (SSD) 存储具有较高的写入吞吐量，您是否需要升级 FC 到 SAS 桥接器以适应吞吐量？

## 相关信息

- 有关更换或升级MetroCluster组件的信息，请参阅 ["MetroCluster文档"](#)。
- 有关升级控制器的信息，请参阅 ["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"](#)

## 将工作负载移至不同的聚合

您可以使用 Unified Manager 来帮助识别比工作负载当前所在聚合繁忙程度较低的聚合，然后您可以将选定的卷或 LUN 移动到该聚合。将高性能工作负载移至不太繁忙的聚合体或启用了闪存的聚合体，可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。
- 您必须记录当前存在性能问题的聚合的名称。
- 您必须记录聚合接收事件的日期和时间。
- Unified Manager 必须收集并分析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，以便您可以将高性能工作负载移动到利用率较低的聚合：

- 同一集群中利用率较低的聚合
- 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”页面上，单击聚合所在集群的名称。

集群详细信息显示在性能/集群登陆页面中。

- b. 在“摘要”页面上，单击“管理对象”窗格中的“聚合”。

显示此集群上的聚合列表。

- c. 单击“利用率”列，按利用率最低的顺序对聚合进行排序。

您还可以识别那些具有最大\*可用容量\*的聚合。这提供了您可能想要移动工作负载的潜在聚合列表。

- d. 写下要将工作负载移动到的聚合的名称。

#### 2. 从接收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。您想要移动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\*。

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. 写下要移动到不同聚合的卷的名称。

3. 将高性能卷移动到您确定为利用率较低的聚合。

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，检查您是否从该节点或聚合接收到相同类型的事件。

## 将工作负载移至其他节点

您可以使用 Unified Manager 来帮助识别比当前运行工作负载的节点繁忙程度较低的其他节点上的聚合，然后您可以将选定的卷移动到该聚合。将高性能工作负载移至不太繁忙的节点上的聚合体，可使两个节点上的工作负载更高效地执行。

### 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。
- 您必须记录当前存在性能问题的节点的名称。
- 您必须记录节点接收性能事件的日期和时间。
- Unified Manager 必须收集并分析一个月或更长时间的性能数据。

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利用率较低的节点：

- 同一集群中具有最大可用性能容量的节点
- 新节点上具有最大可用性能容量的聚合
- 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“事件详情”页面，单击该节点所在集群的名称。

集群详细信息显示在性能/集群登陆页面中。

- b. 在“摘要”选项卡上，单击“管理对象”窗格中的“节点”。

显示该集群上的节点列表。

- c. 单击“已使用的性能容量”列，按使用率最低的百分比对节点进行排序。

这提供了您可能想要将工作负载移动到的潜在节点的列表。

- d. 写下您想要将工作负载移动到的节点的名称。

## 2. 确定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“查看”菜单中选择“性能”>“所有聚合”。

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”，在文本字段中输入节点的名称，然后单击“应用过滤器”。

性能：所有聚合视图将重新显示此节点上可用的聚合列表。

- c. 单击“已使用的性能容量”列，按最少使用对聚合进行排序。

这提供了您可能想要移动工作负载的潜在聚合列表。

- d. 写下要将工作负载移动到的聚合的名称。

## 3. 从接收事件的节点识别高性能工作负载：

- a. 返回活动的“活动详情”页面。

- b. 在“受影响的卷”字段中，单击卷数的链接。

性能：所有卷视图显示该节点上卷的过滤列表。

- c. 单击“总容量”列，按分配的最大空间对卷进行排序。

这提供了您可能想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. 将卷移动到您确定为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，您可以检查是否从该节点或聚合接收到相同类型的事件。

## 将工作负载移动到不同节点上的聚合

您可以使用 Unified Manager 来帮助识别比工作负载当前运行的节点繁忙程度较低的其他节点上的聚合，然后您可以将选定的卷移动到该聚合。将高性能工作负载移至不太繁忙的节点上的聚合体，可使两个节点上的工作负载更高效地执行。

### 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。
- 您必须记录当前存在性能问题的节点的名称。



- 您必须记录节点接收性能事件的日期和时间。
- Unified Manager 必须收集并分析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，以便您可以将高性能工作负载移动到利用率较低的节点：

- 同一集群中利用率较低的节点
- 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/集群登陆页面中。

- b. 在“摘要”页面上，单击“管理对象”窗格中的“节点”。

显示该集群上的节点列表。

- c. 单击“利用率”列按利用率最低的顺序对节点进行排序。

您还可以识别具有最大\*可用容量\*的节点。这提供了您可能想要将工作负载移动到的潜在节点的列表。

- d. 写下您想要将工作负载移动到的节点的名称。

### 2. 确定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“查看”菜单中选择“性能”>“所有聚合”。

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”，在文本字段中输入节点的名称，然后单击“应用过滤器”。

性能：所有聚合视图将重新显示此节点上可用的聚合列表。

- c. 单击“利用率”列，按利用率最低的顺序对聚合进行排序。

您还可以识别那些具有最大\*可用容量\*的聚合。这提供了您可能想要移动工作负载的潜在聚合列表。

- d. 写下要将工作负载移动到的聚合的名称。

### 3. 从接收事件的节点识别高性能工作负载：

- a. 返回活动的“活动”详细信息页面。

- b. 在“受影响的卷”字段中，单击卷数的链接。

性能：所有卷视图显示该节点上卷的过滤列表。

- c. 单击“总容量”列，按分配的最大空间对卷进行排序。

这提供了您可能想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. 将卷移动到您确定为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，检查您是否从该节点或聚合接收到相同类型的事件。

## 将工作负载移至不同 HA 对中的节点

您可以使用 Unified Manager 来帮助识别不同高可用性 (HA) 对中节点上的聚合，该聚合比您的工作负载当前运行的 HA 对具有更多的可用性能容量。然后，您可以将选定的卷移动到新 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。
- 您的集群必须至少包含两个 HA 对

如果您的集群中只有一个 HA 对，则无法使用此修复过程。

- 您必须记录 HA 对中当前存在性能问题的两个节点的名称。
- 您必须记录节点接收性能事件的日期和时间。
- Unified Manager 必须收集并分析一个月或更长时间的性能数据。

将高性能工作负载移动到具有更多可用性能容量的节点上的聚合体，可使两个节点上的工作负载更高效地执行。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不同 HA 对上具有更多可用性能容量的节点：

- 同一集群上不同 HA 对中具有最大可用性能容量的节点
- 新节点上具有最大可用性能容量的聚合
- 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“事件详情”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/集群登陆页面中。
  - b. 在“摘要”页面上，单击“管理对象”窗格中的“节点”。

该集群上的节点列表显示在“性能：所有节点”视图中。
  - c. 记下与当前存在性能问题的 HA 对不同的 HA 对中的节点的名称。
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”视图中，单击“已用性能容量”列，按使用率最低的百分比对节点进行排序。

这提供了您可能想要将工作负载移动到的潜在节点的列表。

- b. 记下您想要将工作负载移动到的不同 HA 对上的节点的名称。

### 3. 确定新节点上具有最大可用性能容量的聚合：

- a. 在“性能：所有节点”视图中，单击该节点。

节点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“已使用的性能容量”列，按最少使用对聚合进行排序。

这提供了您可能想要移动工作负载的潜在聚合列表。

- 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. 返回活动的“活动”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链接。

性能：所有卷视图显示该节点上卷的过滤列表。

- c. 单击“总容量”列，按分配的最大空间对卷进行排序。

这提供了您可能想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. 针对此事件的第二个节点执行步骤 4c 和 4d，以确定您想要从该节点移动的可能的卷。

### 5. 将卷移动到您确定为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，您可以检查是否从该节点或聚合接收到相同类型的事件。

## 将工作负载移至不同 HA 对中的另一个节点

您可以使用 Unified Manager 来帮助识别不同 HA 对中节点上的聚合，该聚合的繁忙程度低于您的工作负载当前正在运行的 HA 对。然后，您可以将选定的卷移动到新 HA 对上的聚合。将高性能工作负载移至不太繁忙的节点上的聚合体，可使两个节点上的工作负载更高效地执行。

### 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。
- 您的集群必须至少包含两个 HA 对；如果您的集群中只有一个 HA 对，则无法使用此修复过程。

- 您必须记录 HA 对中当前存在性能问题的两个节点的名称。
- 您必须记录节点接收性能事件的日期和时间。
- Unified Manager 必须收集并分析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，以便您可以将高性能工作负载移动到不同 HA 对上利用率较低的节点：

- 同一集群上不同 HA 对中利用率较低的节点
- 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. 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“查看”菜单中选择“性能”>“所有集群”。

性能：显示所有集群视图。

- b. 单击当前集群的“节点数”字段中的数字。

将显示“性能：所有节点”视图。

- c. 记下与当前存在性能问题的 HA 对不同的 HA 对中的节点的名称。

### 2. 确定新 HA 对中利用率最低的节点：

- a. 单击“利用率”列按利用率最低的顺序对节点进行排序。

您还可以识别具有最大\*可用容量\*的节点。这提供了您可能想要将工作负载移动到的潜在节点的列表。

- b. 写下您想要将工作负载移动到的节点的名称。

### 3. 确定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“查看”菜单中选择“性能”>“所有聚合”。

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”，在文本字段中输入节点的名称，然后单击“应用过滤器”。

性能：所有聚合视图将重新显示此节点上可用的聚合列表。

- c. 单击“利用率”列，按利用率最低的顺序对聚合进行排序。

您还可以识别那些具有最大\*可用容量\*的聚合。这提供了您可能想要移动工作负载的潜在聚合列表。

- 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. 返回活动的“活动”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链接。

性能：所有卷视图显示该节点上卷的过滤列表。

c. 单击“总容量”列，按分配的最大空间对卷进行排序。

这提供了您可能想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. 针对此事件的第二个节点执行步骤 4c 和 4d，以确定您想要从该节点移动的可能的卷。

5. 将卷移动到您确定为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，检查您是否从该节点或聚合接收到相同类型的事件。

## 使用 QoS 策略设置来优先处理此节点上的工作

您可以对 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（例如默认策略组）中，或者设置的限制不能满足您的需求，您可以增加设置的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。

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会显示涉及的卷列表的链接。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，可能导致该事件。

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，策略组可以限制工作负载以限制其活动，从而减少该节点上资源的使用。

您可以使用ONTAP系统管理器或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

## 删除非活动卷和 LUN

当聚合可用空间被确定为问题时，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。

如果聚合上的性能事件是由磁盘空间不足引起的，则您可以通过几种方法确定哪些卷和 LUN 不再使用。

要识别未使用的卷：

- 在事件详细信息页面上，\*受影响的对象数\*字段提供了一个链接，显示受影响卷的列表。

单击该链接可在“性能：所有卷”视图中显示卷。从那里您可以按 **IOPS** 对受影响的卷进行排序，以查看哪些卷尚未激活。

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“查看”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** 对受影响的 LUN 的结果列表进行排序，以查看不活动的 LUN。

确定未使用的卷和 LUN 后，您可以使用ONTAP系统管理器或ONTAP命令删除这些对象。

### 添加磁盘并执行聚合布局重建

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能看到性能的提升。

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并重建数据。

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，您可能需要联系管理员或购买更多磁盘。您可以使用ONTAP系统管理器或ONTAP命令将磁盘添加到聚合。

["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商之间建立连接

Unified Manager 服务器和外部数据提供商之间的连接使您能够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商之间的连接是通过维护控制台中标有“外部数据提供商”的菜单选项建立的。

### 可以发送到外部服务器的性能数据

Unified Manager 从其监控的所有集群收集各种性能数据。您可以将特定的数据组发送到外部服务器。

根据您想要绘制的性能数据，您可以选择发送以下一组统计信息：

| 统计信息组 | 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： <ul style="list-style-type: none"><li>• LUN</li><li>• 卷</li></ul> | 该组提供所有受监控集群中所有 LUN 和卷的总 IOPS 或延迟。<br><br>该组提供的统计数据最少。 |

| 统计信息组 | 包含的数据                                                                                                                                                                   | 详细信息                                                                                        |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 资源利用率 | 以下对象的资源利用率统计： <ul style="list-style-type: none"> <li>• 节点</li> <li>• 聚合</li> </ul>                                                                                      | 该组提供节点的利用率统计信息并聚合所有受监控集群中的物理资源。<br><br>它还提供性能监视器组中收集的统计数据。                                  |
| 深入研究  | 所有跟踪对象的低级读/写和每个协议的统计信息： <ul style="list-style-type: none"> <li>• 节点</li> <li>• 聚合</li> <li>• LUN</li> <li>• 卷</li> <li>• 磁盘</li> <li>• LIF</li> <li>• 端口/NIC</li> </ul> | 该组为所有受监控集群中的所有七种跟踪对象类型提供读/写和每个协议的细分。<br><br>它还提供性能监视器组和资源利用率组中收集的统计数据。<br><br>该组提供了最多的统计数据。 |



如果存储系统上的集群或集群对象的名称发生更改，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”）。这两个对象并不相关，而是同一个对象。例如，如果将卷的名称从“volume1\_acct”更改为“acct\_vol1”，您将看到旧卷的旧性能数据和新卷的新性能数据。

有关可发送到外部数据提供商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商的 [Unified Manager 性能计数器](#)"

## 设置 Graphite 以从 Unified Manager 接收性能数据

Graphite 是一个用于收集和绘制计算机系统性能数据的开放软件工具。您的 Graphite 服务器和软件必须正确配置才能从 Unified Manager 接收统计数据。

NetApp不会测试或验证 Graphite 或其他第三方工具的特定版本。



Graphite 服务器未从 Unified Manager 接收卷的性能数据。

按照安装说明安装 Graphite 后，您需要进行以下更改以支持从 Unified Manager 传输统计数据：

- 在 /opt/graphite/conf/carbon.conf` 文件，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` ) 。

根据您配置中的集群数量和您选择发送的统计对象，可能需要最初创建数千个新文件。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初始创建所有指标文件。创建所有唯一度量文件后，此参数不再相关。

- 如果您在使用 IPv6 地址部署的服务器上运行 Graphite，则 /opt/graphite/conf/carbon.conf` 文件

必须从“`0.0.0.0`”更改为“`::`”(LINE\_RECEIVER\_INTERFACE = `::`)

- 在 `/opt/graphite/conf/storage-schemas.conf` 文件，`retentions` 必须使用参数将频率设置为 5 分钟，并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的时间长短而定，但对于至少一个保留设置，频率值必须设置为 5 分钟。在以下示例中，使用 `pattern` 参数，其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”更改为其他标签，则该更改必须反映在 `pattern` 参数也是如此。



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，并且收集的数据中会出现差距。

## 配置从 Unified Manager 服务器到外部数据提供商的连接

Unified Manager 可以将集群性能数据发送到外部服务器。您可以指定发送的统计数据类型以及发送数据的间隔。

### 开始之前

- 您必须拥有授权登录 Unified Manager 服务器维护控制台的用户 ID。
- 您必须具有有关外部数据提供商的以下信息：
  - 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）
- 您必须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。
- 您必须知道要发送哪组统计数据：
  - PERFORMANCE\_INDICATOR：性能监视器统计信息
  - RESOURCE\_UTILIZATION：资源利用率和性能监视器统计信息
  - DRILL\_DOWN：所有统计数据
- 您必须知道传输统计数据的时间间隔：5、10 或 15 分钟

默认情况下，Unified Manager 每隔 5 分钟收集一次统计数据。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是使用默认 5 分钟间隔时的两倍（或三倍）。



如果将 Unified Manager 性能收集间隔更改为 10 或 15 分钟，则必须更改传输间隔，使其等于或大于 Unified Manager 收集间隔。

您可以配置一台 Unified Manager 服务器和一台外部数据提供商服务器之间的连接。

### 步骤



1. 以维护用户身份登录到 Unified Manager 服务器的维护控制台。

显示 Unified Manager 维护控制台提示。

2. 在维护控制台中，输入\*外部数据提供者\*菜单选项的编号。

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。

显示当前服务器连接信息。

4. 出现提示时，输入 `y` 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，输入 `y` 验证您输入的信息是否正确。

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。

显示当前服务器配置信息。

9. 出现提示时，输入 `y` 继续。

10. 出现提示时，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：

| 为了..  | 进入...                                                                                                                                                                                     |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 统计组ID | <b>0- PERFORMANCE_INDICATOR</b> （默认）<br><br><b>1- 资源利用率</b><br><br><b>2- DRILL_DOWN</b>                                                                                                   |
| 供应商标签 | 外部服务器上存储统计信息的文件夹的描述性名称。<br>“netapp-performance”是默认名称，但您可以输入其他值。<br><br>通过使用点分符号，您可以定义分层文件夹结构。例如，通过输入 <b>`stats.performance.netapp`</b> 统计数据位于 <b>stats &gt; performance &gt; netapp</b> 。 |
| 传输间隔  | <b>5</b> （默认）， <b>10</b> ，或者 <b>`15`</b> 分钟                                                                                                                                               |
| 启用/禁用 | <b>0- 禁用</b><br><br><b>1- 启用</b> （默认）                                                                                                                                                     |

11. 出现提示时，输入 `y` 验证您输入的信息是否正确。

12. 按任意键返回外部服务器连接菜单。

### 13. 类型 `x` 退出维护控制台。

配置连接后，选定的性能数据将按照您指定的时间间隔发送到目标服务器。指标需要几分钟才会开始出现在外部工具中。您可能需要刷新浏览器才能看到指标层次结构中的新指标。

# 监视和管理集群健康状况

## Active IQ Unified Manager健康监控简介

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运行ONTAP软件的大量系统。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、管理保护功能以及捆绑诊断数据并将其发送给技术支持。

您可以使用 Unified Manager 来监控您的集群。当集群中出现问题时，Unified Manager 会通过事件通知您此类问题的详细信息。有些事件还会为您提供可以采取的补救措施来纠正问题。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 通过将存储对象与注释关联来管理环境中的存储对象。您可以创建自定义注释，并通过规则将集群、存储虚拟机 (SVM) 和卷与注释动态关联。

您还可以使用容量和运行状况图表中提供的信息来为各个集群对象规划集群对象的存储要求。

### 物理和逻辑容量

Unified Manager 利用用于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（例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）。逻辑空间是指理论上如何使用空间，不考虑重复数据删除或压缩的结果。“使用的逻辑空间”是使用的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）节省的空间。该测量值通常看起来大于物理使用容量，因为这没有反映数据压缩和物理空间的其他减少。因此，总逻辑容量可能高于配置的空间。

### 容量测量单位

Unified Manager 根据 1024 (2<sup>10</sup>) 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ONTAP的所有版本，吞吐量使用的单位仍然是每秒千字节 (Kbps)、每秒兆字节 (Mbps)、每秒千兆字节 (Gbps) 或每秒太字节 (Tbps) 等等。

| Unified Manager for ONTAP 9.10.0 及更早版本中显示的容量单位 | Unified Manager for ONTAP 9.10.1 中显示的容量单位 | 计算方式        | 以字节为单位的值     |
|------------------------------------------------|-------------------------------------------|-------------|--------------|
| KB                                             | KiB                                       | 1024        | 1024 字节      |
| MB                                             | MiB                                       | 1024 * 1024 | 1,048,576 字节 |

| Unified Manager for<br>ONTAP 9.10.0<br>及更早版本中显示的容量<br>单位 | Unified Manager for<br>ONTAP 9.10.1<br>中显示的容量单位 | 计算方式                        | 以字节为单位的值             |
|----------------------------------------------------------|-------------------------------------------------|-----------------------------|----------------------|
| GB                                                       | GiB                                             | $1024 * 1024 * 1024$        | 1,073,741,824 字节     |
| TB                                                       | TiB                                             | $1024 * 1024 * 1024 * 1024$ | 1,099,511,627,776 字节 |

## Unified Manager 运行状况监控功能

Unified Manager 建立在服务器基础架构上，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：

- 发现、监控和通知安装了ONTAP软件的系统：
  - 物理对象：节点、磁盘、磁盘架、SFO 对、端口和闪存
  - 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、连接路径、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）和SnapVault关系
- 查看集群发现和监控状态
- MetroCluster通过 FC 和 IP 配置：查看和监控集群组件的配置、问题和连接状态。适用于 FC 配置上的MetroCluster的 MetroCluster交换机和网桥
- 增强的警报、事件和阈值基础设施
- LDAP、LDAPS、SAML 身份验证和本地用户支持
- RBAC（针对一组预定义的角色）
- 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事件影响的“可能影响”区域
- 建议的纠正措施区域，其中显示了可以执行的操作，以解决某些故障磁盘、 MetroCluster聚合镜像降级和MetroCluster备用磁盘遗留等事件
- 可能受影响的资源区域，显示可能受事件（例如卷脱机事件、卷限制事件和精简配置卷空间处于风险事件）影响的资源
- 支持具有FlexVol或FlexGroup卷的 SVM

- 支持监控节点根卷
- 增强的 Snapshot 副本监控，包括计算可回收空间和删除 Snapshot 副本
- 存储对象的注解
- 报告创建和管理存储对象信息，例如物理和逻辑容量、利用率、空间节省、性能和相关事件
- 与OnCommand Workflow Automation集成以执行工作流

存储自动化商店包含经NetApp认证的自动化存储工作流程包，这些工作流程包专为与OnCommand Workflow Automation(WFA) 配合使用而开发。您可以下载这些包，然后将其导入到 WFA 来执行它们。自动化工作流程可在此处获得：

["存储自动化商店"](#)

## 用于管理存储系统健康状况的 **Unified Manager** 界面

这些部分包含有关Active IQ Unified Manager提供的两个用户界面的信息，用于解决数据存储容量、可用性和保护问题。这两个 UI 是 Unified Manager Web UI 和维护控制台。

如果您想使用 Unified Manager 中的保护功能，您还必须安装和配置OnCommand Workflow Automation (WFA)。

### **Unified Manager Web UI**

Unified Manager Web UI 使管理员能够监控和排除与数据存储容量、可用性和保护相关的集群问题。

这些部分介绍了管理员可以遵循的一些常见工作流程，以解决 Unified Manager Web UI 中显示的存储容量、数据可用性或保护问题。

### 维护控制台

Unified Manager 维护控制台使管理员能够监控、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。

## 管理和监控集群和集群对象健康状况

Unified Manager 使用定期 API 查询和数据收集引擎从集群收集数据。通过将集群添加到 Unified Manager 数据库，您可以监控和管理这些集群的任何可用性和容量风险。

### 了解集群监控

您可以将集群添加到 Unified Manager 数据库，以监控集群的可用性、容量和其他详细信息，例如 CPU 使用率、接口统计信息、可用磁盘空间、qtree 使用率和机箱环境。

如果状态异常或超出预定义的阈值，则会生成事件。如果配置为这样做，当事件触发警报时，Unified Manager 会向指定收件人发送通知。

## 了解节点根卷

您可以使用 Unified Manager 监控节点根卷。最佳做法是节点根卷应具有足够的容量以防止节点关闭。

当节点根卷的已用容量超过节点根卷总容量的 80% 时，将生成节点根卷空间将满事件。您可以为事件配置警报以获取通知。您可以使用 ONTAP 系统管理器或 ONTAP CLI 采取适当的措施来防止节点关闭。



如果集群运行 ONTAP 9.14.1 版本或更高版本，则监控节点根卷的功能不可用。

## 了解节点根聚合的事件和阈值

您可以使用 Unified Manager 监控节点根聚合。最佳做法是在根聚合中密集配置根卷，以防止节点停止运行。

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。只有技术支持代表可以修改生成这些事件的设置。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 系统管理器或 ONTAP CLI 采取适当的措施来防止节点停止。



如果集群运行 ONTAP 9.14.1 版本或更高版本，则监控节点根聚合的功能不可用。

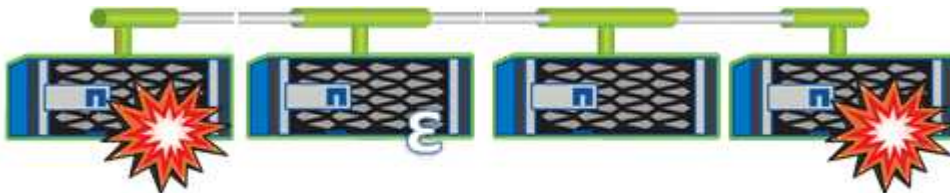
## 了解法定人数和 epsilon

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应对潜在的通信和连接挑战。

Quorum 是集群完全正常运行的先决条件。如果集群处于仲裁状态，则过半数的节点运行状况良好，并可相互通信。如果失去仲裁状态，则集群将无法完成正常的集群操作。由于所有节点共同共享单一数据视图，因此任何时候都只能有一个节点集合具有仲裁。因此，如果允许两个不通信的节点以不同的方式修改数据，就不再可能将数据协调到单个数据视图中。

集群中的每个节点都参与投票协议，选举一个节点主节点；其余每个节点都是辅助节点。主节点负责整个集群的信息同步。当法定人数形成后，通过持续投票来维持。如果主节点离线并且集群仍然处于仲裁状态，则由保持在线的节点选出新的主节点。

由于在具有偶数个节点的集群中存在平局的可能性，因此一个节点具有称为 epsilon 的额外分数投票权重。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群集，其中两个节点发生故障。然而，由于其中一个幸存节点拥有 epsilon，因此即使健康节点的数量不达到简单多数，集群仍保持法定人数。



创建集群时，Epsilon 会自动分配到第一个节点。如果持有 epsilon 的节点变得不健康、接管其高可用性伙伴节点或被其高可用性伙伴节点接管，则 epsilon 会自动重新分配到不同 HA 对中的健康节点。

使节点脱机可能会影响集群保持仲裁的能力。因此，如果您尝试执行使集群脱离法定人数或使其因失去法定人数而发生一次中断的操作，ONTAP会发出警告消息。您可以在高级权限级别使用 `cluster quorum-service options modify` 命令禁用仲裁警告消息。

一般来说，假设集群节点之间的连接可靠，则较大的集群比较小的集群更稳定。与 2 个节点的集群相比，在 24 个节点的集群中更容易维持半数节点加 epsilon 的简单多数的法定人数要求。

双节点集群在保持仲裁方面具有一定的难度。双节点集群使用集群 HA，其中两个节点都不持有 epsilon；相反，两个节点都会被持续轮询，以确保如果一个节点发生故障，另一个节点可以完全读写数据，并可以访问逻辑接口和管理功能。

## 查看集群列表及详情

您可以使用“健康状况：所有集群”视图来查看集群清单。容量：所有集群视图使您能够查看有关所有集群的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，例如集群运行状况、容量、配置、LIF、节点和该集群中的磁盘。

健康状况：所有集群视图、容量：所有集群视图和集群/健康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：所有集群”视图中选择一个特定的集群，并获取容量详细信息以确定该集群是否具有所需的空間。

### 步骤

1. 在左侧导航窗格中，单击“存储”>“集群”。
2. 在“查看”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”视图以查看有关所有集群的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该集群的完整详细信息。

### 相关信息

- ["集群/健康详情页面"](#)
- ["性能：所有集群视图"](#)
- ["监控MetroCluster配置"](#)
- ["查看集群和存储虚拟机的安全状态"](#)
- ["正在评估哪些安全标准"](#)

## 检查MetroCluster配置中集群的运行状况

您可以使用Active IQ Unified Manager（Unified Manager）检查MetroCluster over FC和MetroCluster over IP 配置中的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，则健康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。
- 您必须已经分析了MetroCluster配置的性能事件并获取了所涉及的集群的名称。
- 通过 FC 和 IP 的MetroCluster配置中的两个集群必须由同一个 Unified Manager 实例监控。

确定MetroCluster通过 FC 配置中的集群运行状况

按照以下步骤确定MetroCluster over FC 配置中的集群运行状况。

步骤

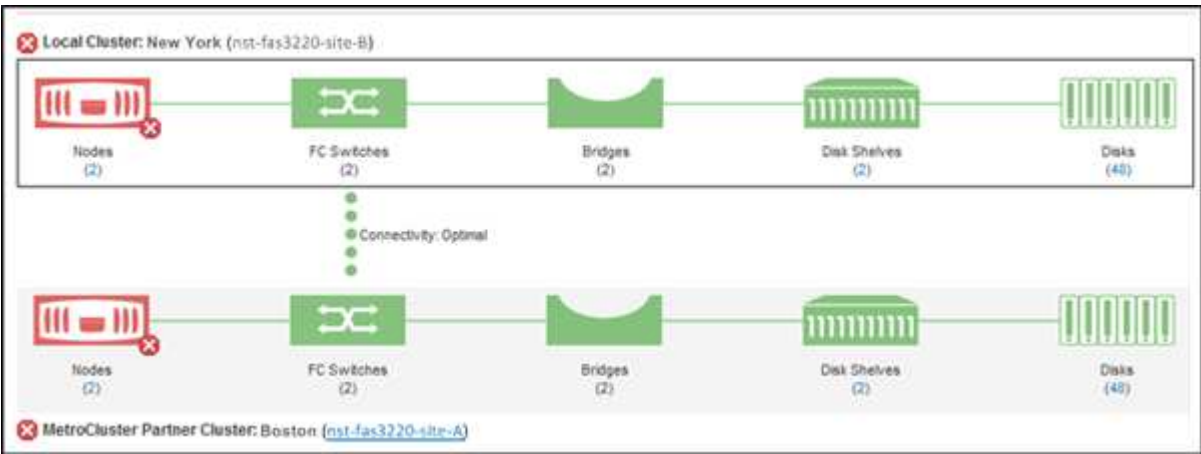
1. 在左侧导航栏中，点击“事件管理”，显示事件列表。
2. 在过滤器面板中，选择“源类型”类别下的所有MetroCluster过滤器。您会看到您的环境中针对所有MetroCluster配置引发的所有事件。
3. 在MetroCluster事件旁边，单击集群的名称。



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 配置相关的事件所涉及的集群的名称。

健康状况：所有集群视图显示有关该事件的详细信息。

4. 选择“MetroCluster Connectivity”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。

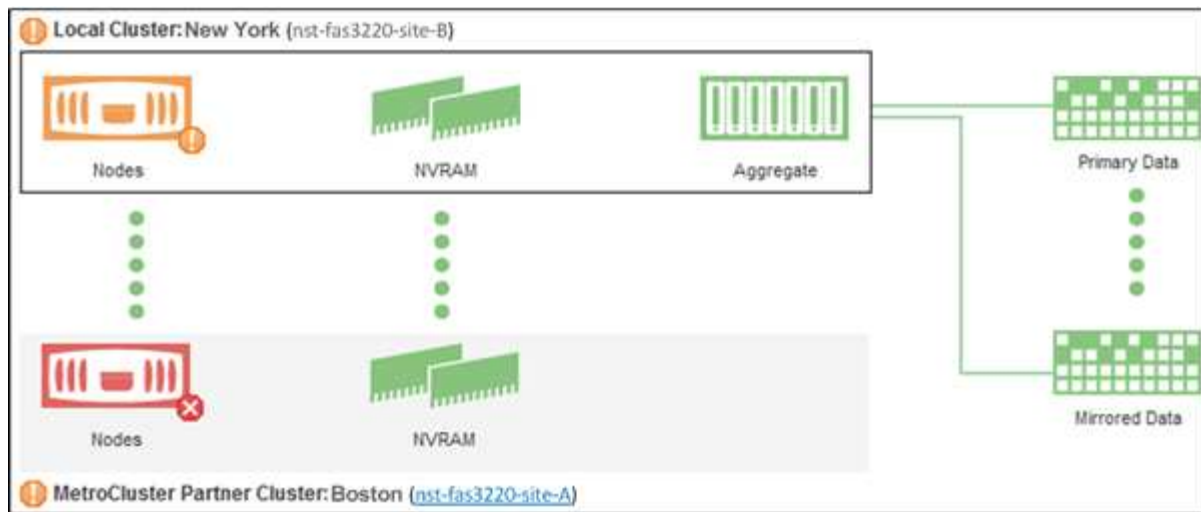


在此示例中，显示了本地集群及其伙伴集群的名称和组件。黄色或红色图标表示突出显示的组件的健康事件。连接图标表示集群之间的链接。您可以将鼠标光标指向图标以显示事件信息，或者单击图标以显示事件。任一集群的健康问题都可能导致性能事件。

Unified Manager 监控集群之间链接的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，则可能是链路健康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集群上的NVRAM图标为黄色或红色，则NVRAM的健康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，则可能是合作伙伴集群上的性能问题导致了性能事件。

## 确定MetroCluster over IP 配置中的集群运行状况

按照以下步骤确定MetroCluster over IP 配置中的集群运行状况。

### 步骤

1. 在左侧导航栏中，点击“事件管理”，显示事件列表。
2. 在过滤器面板的“源类型”类别下，选择 `MetroCluster Relationship` 筛选。您会看到您的环境中针对所有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MetroCluster over IP 配置相关的事件所涉及的集群名称进行搜索。

3. 在相关的MetroCluster事件旁边，单击集群的名称。将显示“集群”页面，其中包含该集群的详细信息。有关确定健康问题的信息，请参阅[“监控MetroCluster通过 IP 配置中的连接问题”](#)。

## 查看所有 SAN 阵列集群的健康和容量状态

您可以使用集群清单页面显示所有 SAN 阵列集群的健康和容量状态。

### 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”视图中查看所有 SAN 阵列集群的概述信息。此外，您还可以在集群/健康详情页面查看详细信息。

### 步骤

1. 在左侧导航窗格中，单击“存储”>“集群”。
2. 确保“个性”列显示在\*健康：所有集群\*视图中，或使用\*显示/隐藏\*控件添加它。

此列显示您的所有 SAN 阵列集群的“所有 SAN 阵列”。

- 3. 查看信息。
- 4. 要查看这些集群中的存储容量信息，请选择容量：所有集群视图。
- 5. 要查看这些集群的运行状况和存储容量的详细信息，请单击全 SAN 阵列集群的名称。

在“集群/健康详情”页面的“健康”、“容量”和“节点”选项卡中查看详细信息

查看节点列表及详情

您可以使用“运行状况：所有节点”视图来查看集群中的节点列表。您可以使用集群/健康详情页面来查看有关受监控集群的节点的详细信息。

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。

您可以查看节点状态、包含该节点的集群、聚合容量详细信息（已用容量和总计容量）以及原始容量详细信息（可用容量、备用容量和总计容量）等详细信息。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“**Health: All Nodes**”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显示在集群/健康详细信息页面中。左侧窗格显示 HA 对列表。默认情况下，HA 详细信息是打开的，其中显示与所选 HA 对相关的 HA 状态详细信息和事件。

- 3. 要查看有关节点的其他详细信息，请执行相应的操作：

| 查看项        | 点击... |
|------------|-------|
| 有关磁盘架的详细信息 | 磁盘架。  |
| 港口相关信息     | 端口。   |

有关详细信息，请参阅：For more information, see:

- ["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"](#)

生成合同续签的硬件清单报告

您可以生成一个报告，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、磁盘类型和计数、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\* > \* > 硬件清单报告\*。

硬件清单报告以 .csv 文件的形式下载，其中包含截至当前日期的完整信息。

4. 将此信息提供给您的NetApp支持联系人以进行合同续签。

## 查看存储虚拟机列表和详细信息

从“运行状况：所有存储虚拟机”视图中，您可以监控存储虚拟机 (SVM) 的库存。您可以使用存储虚拟机/运行状况详细信息页面查看有关受监控的 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”>“存储虚拟机”。
2. 选择以下方式之一查看 SVM 详细信息：
  - 要查看所有集群中所有 SVM 的运行状况信息，请在“查看”菜单中选择“运行状况：所有存储虚拟机视图”。
  - 要查看完整详细信息，请单击存储虚拟机名称。

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”来查看与 SVM 相关的对象。

#### 相关信息

- ["存储虚拟机：健康详情页面"](#)
- ["性能：所有存储虚拟机视图"](#)
- ["安全：反勒索软件视图"](#)
- ["查看集群和存储虚拟机的安全状态"](#)
- ["关系：所有关系视图"](#)

## 查看汇总列表和详细信息

从“健康状况：所有聚合体”视图中，您可以监控聚合体的库存。通过“容量：所有聚合”视图，您可以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/健康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：
  - 要查看有关所有集群中所有聚合的健康状况的信息，请在“查看”菜单中选择“健康状况：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“查看”菜单中选择“容量：所有聚合视图”。
  - 要查看完整详细信息，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”来查看与聚合相关的对象。

相关信息

- ["聚合/健康详情页面"](#)
- ["性能：所有聚合视图"](#)
- ["自定义聚合容量报告"](#)

查看FabricPool容量信息

您可以在这些对象的容量和性能清单和详细信息页面上查看集群、聚合和卷的FabricPool容量信息。当配置了镜像层时，这些页面还会显示FabricPool镜像信息。

这些页面显示的信息包括本地性能层和云层上的可用容量、两个层中使用的容量、哪些聚合连接到云层以及哪些卷通过将某些信息移动到云层来实现FabricPool功能。

当一个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/健康详细信息页面中。

步骤

1. 执行以下操作之一：

| 要查看容量信息... | 操作                                                                                                    |
|------------|-------------------------------------------------------------------------------------------------------|
| 集群         | <div>a. 在容量：所有集群视图中，单击一个集群。</div> <div>b. 在集群/健康详情页面，单击“配置”选项卡。</div> <div>显示屏显示该集群所连接的任何云层的名称。</div> |

| 要查看容量信息... | 操作                                                                                                                                                                                                                                       |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 聚合         | <p>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。</p> <p>b. 在聚合/健康详细信息页面上，单击“容量”选项卡。</p> <p>显示屏显示云层中使用的总容量。</p> <p>c. 单击“磁盘信息”选项卡。</p> <p>显示屏显示云层的名称和使用的容量。</p> <p>d. 单击“配置”选项卡。</p> <p>显示屏显示云层的名称以及有关云层的其他详细信息。</p> |
| 卷          | <p>a. 在“容量：所有卷”视图中，单击“分层策略”字段中出现策略名称的卷。</p> <p>b. 在卷/健康详情页面上，单击“配置”选项卡。</p> <p>显示屏显示分配给该卷的FabricPool分层策略的名称。</p>                                                                                                                         |

2. 在\*工作负载分析\*页面中，您可以选择\*容量趋势\*区域中的“云层视图”来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，请参阅 ["磁盘和聚合概述"](#)。

### 查看存储池详细信息

您可以查看存储池的详细信息，以监控存储池的健康状况、总缓存和可用缓存以及已用分配和可用分配。

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。

显示所选聚合的详细信息。

3. 单击“磁盘信息”选项卡。

显示详细的磁盘信息。



仅当选定的聚合正在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。

显示存储池的详细信息。

## 查看卷列表和详细信息

从“健康状况：所有卷”视图中，您可以监控卷的库存。容量：所有卷视图使您能够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“存储”>“卷”。
2. 选择以下方式之一查看卷详细信息：
  - 要查看有关集群中卷的健康状况的详细信息，请在“查看”菜单中选择“健康状况：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“查看”菜单中选择“容量：所有卷”视图。
  - 要查看完整详细信息，请单击卷名称。

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. \*可选：\*通过单击最小详细信息对话框中的“查看相关”来查看与卷相关的对象。

### 相关信息

- ["卷：健康详情页面"](#)
- ["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"](#)

## 查看有关 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”视图查看所有受监控集群上的所有 NFS 共享，并使用“存储虚拟机/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

- 必须在集群上启用 NFS 许可证。
- 必须配置服务于 NFS 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。

#### 步骤

1. 在左侧导航窗格中，根据您要查看所有 NFS 共享还是仅查看特定 SVM 的 NFS 共享，执行以下步骤。

| 目的                | 请按照以下步骤操作...                                                                                                                                                    |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 查看所有 NFS 共享       | 单击“存储”>“NFS 共享”                                                                                                                                                 |
| 查看单个 SVM 的 NFS 共享 | <ol style="list-style-type: none"> <li>a. 单击“存储”&gt;“存储虚拟机”</li> <li>b. 单击要查看其 NFS 共享详细信息的 SVM。</li> <li>c. 在存储虚拟机/运行状况详细信息页面中，单击 <b>NFS 共享</b> 选项卡。</li> </ol> |

有关详细信息，请参阅[“配置文件共享卷”](#)和[“使用 API 调配 CIFS 和 NFS 文件共享”](#)。

### 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、连接路径、包含的对象、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”视图查看所有受监控集群上的所有 SMB 共享，并使用“存储虚拟机/运行状况详细信息”页面查看特定存储虚拟机 (SVM) 上的所有 SMB 共享。

#### 开始之前

- 必须在集群上启用 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。



文件夹中的共享不显示。

#### 步骤

1. 在左侧导航窗格中，根据您要查看所有 SMB/CIFS 共享还是仅查看特定 SVM 的共享，执行以下步骤。

| 目的               | 请按照以下步骤操作...    |
|------------------|-----------------|
| 查看所有 SMB/CIFS 共享 | 单击“存储”>“SMB 共享” |

| 目的                     | 请按照以下步骤操作...                                                                                                                                                |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 查看单个 SVM 的 SMB/CIFS 共享 | <ol style="list-style-type: none"> <li>单击“存储”&gt;“存储虚拟机”</li> <li>单击要查看其 SMB/CIFS 共享详细信息的 SVM。</li> <li>在存储虚拟机/运行状况详细信息页面中，单击 <b>SMB 共享</b> 选项卡。</li> </ol> |

有关详细信息，请参阅 ["使用 API 调配 CIFS 和 NFS 文件共享"](#)。

## 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 副本列表来计算删除一个或多个 Snapshot 副本后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“存储”>“卷”。
2. 在“**Health: All Volumes**”视图中，选择包含要查看的 Snapshot 副本的卷。
3. 在“\*Volume / Health\*”详细信息页面中，单击\*Capacity\*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 副本数量是一个显示 Snapshot 副本列表的链接。

### 相关信息

["健康/容量页面"](#)

## 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，或者如果不再需要 Snapshot 副本，也可以将其删除。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

该卷必须处于在线状态。

要删除处于繁忙或锁定状态的 Snapshot 副本，您必须从正在使用它的应用程序中释放该 Snapshot 副本。

- 如果 FlexClone 卷正在使用基线 Snapshot 副本，则您无法删除父卷中的该 Snapshot 副本。



基本 Snapshot 副本是用于创建FlexClone卷并显示状态的 Snapshot 副本 `Busy`和应用程序依赖关系 `Busy, Vclone`在父卷中。

- 您无法删除SnapMirror关系中使用的锁定 Snapshot 副本。

Snapshot 副本已被锁定，下次更新时需要它。

#### 步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“**Health: All Volumes**”视图中，选择包含要查看的 Snapshot 副本的卷。

将显示 Snapshot 副本列表。

3. 在\*Volume / Health\*详细信息页面中，单击\*Capacity\*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 副本数量是一个显示 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“删除所选”。

## 计算 Snapshot 副本的可回收空间

您可以计算删除一个或多个 Snapshot 副本后可以回收的磁盘空间量。

#### 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。
- 该卷必须处于在线状态。
- 该卷必须是FlexVol volume； FlexGroup卷不支持此功能。

#### 步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“**Health: All Volumes**”视图中，选择包含要查看的 Snapshot 副本的卷。

将显示 Snapshot 副本列表。

3. 在\*Volume / Health\*详细信息页面中，单击\*Capacity\*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 副本数量是一个显示 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\*。

显示卷上的可回收空间（以百分比、KB、MB、GB 等单位）。

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”。

## 集群对象窗口和对话框说明

您可以从相应的存储对象页面查看所有集群和集群对象。您也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 INVENTORY 的以下 STORAGE 和 PROTECTION 部分启动系统管理器用户界面。

- 集群清单、集群运行状况和集群性能页面
- 汇总库存、汇总健康状况和汇总绩效页面
- 卷清单、卷运行状况和卷性能页面
- 节点清单和节点性能页面
- StorageVM 库存、StorageVM 运行状况和 StorageVM 性能页面
- 保护关系页面

## 常见的 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状况；恢复丢失的数据；配置和管理卷；以及捆绑并发送诊断数据给技术支持（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、可用性和保护健康状况，然后快速识别、定位、诊断和分配可能出现的任何特定问题的解决方案。

与集群、存储虚拟机 (SVM)、卷或 FlexGroup 卷相关的最重要的问题会影响托管存储对象的存储容量或数据可用性，这些问题显示在“仪表板”页面上的系统运行状况图表和事件中。当发现严重问题时，此页面会提供链接来支持适当的故障排除工作流程。

Unified Manager 还可以包含在包含相关可管理性工具（例如 OnCommand Workflow Automation (WFA)）的工作流程中，以支持存储资源的直接配置。

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仪表板页面中显示数据可用性事件，存储管理员可以按照嵌入的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

管理员可以监视和管理被监视的存储系统资源的性能。查看["Active IQ Unified Manager 性能监控简介"](#)了解更多信息。

- 诊断和管理卷容量问题

如果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的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

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、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。查看["创建、监控和排除保护关系故障"](#)了解更多信息。

- 创建备份文件并从备份文件恢复数据。
- 将存储对象与注释关联

通过将存储对象与注释关联，存储管理员可以过滤和查看与存储对象相关的事件，从而使存储管理员能够确定与事件相关的问题的优先级并解决这些问题。

- 使用 REST API 查看 Unified Manager 捕获的运行状况、容量和性能信息，从而帮助管理集群。看["Active IQ Unified Manager REST API 入门"](#)了解更多信息。
- 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。

## 监控和排除数据可用性故障

Unified Manager 监控授权用户访问您存储的数据的可靠性，提醒您阻止或妨碍访问的情况，并使您能够诊断这些情况并分配和跟踪其解决方案。

本节中的可用性工作流程主题描述了存储管理员如何使用 Unified Manager Web UI 来发现、诊断和分配对数据可用性产生不利影响的硬件和软件条件的解决方案的示例。

### 扫描并解决存储故障转移互连链路故障情况

此工作流程提供了一个示例，说明如何扫描、评估和解决故障存储故障转移互连链路状况。在这种情况下，您是管理员，使用 Unified Manager 在节点上启动ONTAP版本升级之前扫描存储故障转移风险。

#### 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。

如果在无中断升级尝试期间 HA 对节点之间的存储故障转移互连失败，则升级失败。因此，通常的做法是管理员在升级开始之前监视并确认要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\*库存页面中，选择\*活动可用性事件\*。
3. 在“活动管理”库存页面“名称”列顶部，点击  并输入 `\*failover` 在文本框中限制要显示的事件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 在其可用性事件部分显示事件“存储故障转移互连一个或多个链接关闭”。

4. 如果“事件管理”清单页面上显示与存储故障转移相关的一个或多个事件，请执行以下步骤：

- a. 单击事件标题链接可显示该事件的事件详细信息。

在此示例中，您单击事件标题“存储故障转移互连一个或多个链接关闭”。

将显示该事件的事件详细信息页面。

- a. 在事件详细信息页面上，您可以执行以下一项或多项任务：

- 查看原因字段中的错误消息并评估问题。
- 将事件分配给管理员。
- 确认该事件。

## 相关信息

["事件详细信息页面"](#)

["Unified Manager 用户角色和功能"](#)

对存储故障转移互连链路执行纠正措施

当您显示与存储故障转移相关的事件的事件详细信息页面时，您可以查看该页面的摘要信息以确定事件的紧急程度、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故障情况的以下信息：

```
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)
```

示例事件信息表明，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。由于一个链接处于活动状态，远程动态内存访问 (RDMA) 仍在运行，并且存储故障转移作业仍可成功。

但是，为了确保链路不会发生故障并且存储故障转移保护不会被完全禁用，您决定进一步诊断 Link1 发生故障的原因。

#### 步骤

1. 在“\*事件\*详细信息”页面中，您可以单击“源”字段中指定的事件的链接，以获取可能与存储故障转移互连链路故障情况相关的其他事件的更多详细信息。

在这个例子中，事件的来源是名为 `aardvark` 的节点。单击该节点名称会在集群/健康详情页面的节点选项卡上显示受影响的 HA 对 `aardvark` 和 `bonobo` 的 HA 详情，并显示受影响的 HA 对上最近发生的其他事件。

2. 查看\*HA 详细信息\*以获取有关该事件的更多信息。

在此示例中，相关信息位于事件表中。该表显示了“存储故障转移连接一个或多个链接断开”事件、事件生成的时间以及该事件的起源节点。

使用 HA 详细信息中的节点位置信息，请求或亲自完成受影响的 HA 对节点上的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"](#)

#### 解决卷离线问题

此工作流程提供了一个示例，说明如何评估和解决 Unified Manager 可能在事件管理库存页面中显示的卷离线事件。在此场景中，您是使用 Unified Manager 排除一个或多个卷离线事件故障的管理员。

#### 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。

由于多种原因，卷可能会被报告为离线：

- SVM 管理员已故意使卷脱机。
- 该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失败了。
- 该卷的托管存储虚拟机 (SVM) 已停止，因为托管该 SVM 根卷的节点已关闭。
- 由于两个 RAID 磁盘同时发生故障，该卷的托管聚合已关闭。

您可以使用事件管理库存页面和集群/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\*库存页面中，选择\*活动可用性事件\*。
3. 单击卷离线事件显示的超文本链接。

将显示可用性事件的事件详细信息页面。

4. 在该页面上，检查注释，查看是否有任何迹象表明 SVM 管理员已将相关卷脱机。
5. 在“\*事件\*详细信息”页面上，您可以查看以下一项或多项任务的信息：
  - 查看原因字段中显示的信息以获取可能的诊断指导。

在此示例中，“原因”字段中的信息仅通知您卷处于脱机状态。

- 检查“注释和更新”区域，查看是否有任何迹象表明 SVM 管理员故意将相关卷脱机。
- 单击事件源（在本例中为报告离线的卷）以获取有关该卷的更多信息。
- 将事件分配给管理员。
- 确认该事件，或者如果适用，将其标记为已解决。

#### 对卷离线情况执行诊断操作

导航到报告离线的卷的卷/健康详情页面后，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。

如果报告脱机的卷不是故意脱机的，则该卷可能由于多种原因而脱机。

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来确认或消除可能的原因：

- 单击“卷/运行状况”详细信息页面链接，确定卷是否处于离线状态，因为其主机节点已关闭，并且到其 HA 对伙伴的存储故障转移也失败了。

看["确定卷离线情况是否由故障节点引起"](#)。

- 单击“\*卷/运行状况\*详细信息”页面链接，确定卷是否处于脱机状态，以及其主机存储虚拟机 (SVM) 是否已停止，因为托管该 SVM 根卷的节点已关闭。

看["确定卷是否处于脱机状态以及 SVM 是否因节点关闭而停止"](#)。

- 单击“卷/健康”详细信息页面链接，确定卷是否由于其主机聚合中的磁盘损坏而处于离线状态。

看["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"](#)

确定卷是否由于其主机节点关闭而处于离线状态

您可以使用 Unified Manager Web UI 来确认或排除卷离线的可能性，因为其主机节点已关闭，并且存储故障转移到其 HA 对伙伴失败。

#### 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。

要确定卷离线情况是否由托管节点故障和随后的存储故障转移失败引起，请执行以下操作：

#### 步骤

1. 找到并单击离线卷的 [卷/运行状况 详细信息页面](#)的 [相关设备](#) 窗格中 SVM 下显示的超文本链接。

存储虚拟机/运行状况详细信息页面显示有关离线卷的托管存储虚拟机 (SVM) 的信息。

2. 在“存储虚拟机/运行状况”详细信息页面的“相关设备”窗格中，找到并单击“卷”下显示的超文本链接。

运行状况：所有卷视图显示有关 SVM 托管的所有卷的信息表。

3. 在“**Health: All Volumes**”视图“State”列标题上，单击过滤器符号 ，然后选择选项\*离线\*。

仅列出处于脱机状态的 SVM 卷。

4. 在“Health: All Volumes”视图中，单击网格符号 ，然后选择选项\*集群节点\*。

您可能需要在网格选择框中滚动以找到\*集群节点\*选项。

集群节点列被添加到卷清单中，并显示托管每个离线卷的节点的名称。

5. 在“**Health: All Volumes**”视图中，找到离线卷的列表，然后在其“Cluster Node”列中单击其托管节点的名称。

集群/健康详情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。显示屏上指示了托管节点的状态和任何集群故障转移操作的成功情况。

确认卷离线情况存在是因为其主机节点关闭并且存储故障转移到 HA 对伙伴节点失败后，请联系相应的管理员或操作员手动重新启动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并且其 **SVM** 是否因节点关闭而停止

您可以使用 Unified Manager Web UI 来确认或排除卷处于脱机状态的可能性，因为托管该 SVM 根卷的节点已关闭，导致其主机存储虚拟机 (SVM) 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。

要确定卷脱机情况是否由于托管该 SVM 根卷的节点关闭而导致其主机 SVM 停止，请执行以下操作：

#### 步骤

1. 找到并单击离线卷的 [卷/运行状况 详细信息页面](#)的 [相关设备](#) 窗格中 SVM 下方显示的超文本链接。

存储虚拟机/运行状况详细信息页面显示托管 SVM 的“正在运行”或“已停止”状态。如果 SVM 状态为正在运行，则卷离线情况不是由托管该 SVM 根卷的节点关闭引起的。

2. 如果 SVM 状态为停止，则单击“查看 SVM”以进一步确定托管 SVM 停止的原因。

3. 在“运行状况：所有存储虚拟机”视图的 SVM 列标题上，单击筛选符号  然后输入已停止的 SVM 的名称。



该 SVM 的信息显示在表中。

4. 在“运行状况：所有存储虚拟机”视图中，单击然后选择选项\*Root Volume\*。

根卷列添加到 SVM 清单中，并显示已停止的 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\*存储虚拟机/运行状况\*详细信息页面。

如果 SVM 根卷的状态为（联机），则原始卷脱机情况不是由于托管该 SVM 根卷的节点已关闭而导致的。

6. 如果 SVM 根卷的状态为（脱机），则找到并单击 SVM 根卷的“卷/运行状况详细信息”页面的“相关设备”窗格中“聚合”下显示的超文本链接。
7. 找到并单击聚合的\*聚合/健康\*详细信息页面的\*相关设备\*窗格中节点下显示的超文本链接。

集群/运行状况详细信息页面上的节点选项卡显示 SVM 根卷的托管节点所属的 HA 节点对的状态。节点的状态显示在显示屏上。

确认卷离线状态是由该卷的主机 SVM 离线状态引起的（而主机 SVM 离线状态本身是由托管该 SVM 根卷的节点关闭引起的）后，请联系相应的管理员或操作员手动重新启动关闭的节点。

确定卷是否由于聚合中的磁盘损坏而处于脱机状态

您可以使用 Unified Manager Web UI 来确认或消除卷脱机的可能性，因为 RAID 磁盘问题已导致其主机聚合脱机。

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。

要确定卷脱机情况是否由导致托管聚合脱机的 RAID 磁盘问题引起，请执行以下操作：

步骤

1. 找到并单击“**Volume / Health**”详细信息页面的“**Related Devices**”窗格中“Aggregate”下显示的超文本链接。

聚合/健康详情页面显示托管聚合的在线或离线状态。如果聚合状态为在线，则 RAID 磁盘问题不是导致卷离线的原因。

2. 如果聚合状态为离线，则单击“磁盘信息”，然后在“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”下显示的超文本链接。

显示集群/健康详情页面。

4. 单击“磁盘”，然后在“过滤器”窗格中选择“损坏”以列出所有处于损坏状态的磁盘。

如果处于损坏状态的磁盘导致主机聚合处于脱机状态，则该聚合的名称将显示在“受影响的聚合”列中。

确认卷脱机状态是由损坏的 RAID 磁盘和随之而来的主机聚合脱机引起的后，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重新联机。



## 解决容量问题

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 页面来查看任何受监控的存储对象是否存在容量问题。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“仪表板”页面的“容量\*”面板中，单击“卷空间已满”错误事件的名称。

将显示错误的事件详细信息页面。

2. 在“活动”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的描述。
  - 单击源字段中的对象名称（在本例中为卷）以获取有关该对象的详细信息。
  - 查找可能已添加的有关此事件的注释。
  - 为事件添加注释。
  - 将事件分配给另一个用户。
  - 确认该事件。
  - 将该事件标记为已解决。

### 相关信息

["事件详细信息页面"](#)

### 对整个卷执行建议的补救措施

收到“卷空间已满”错误事件后，您可以查看事件详细信息页面上建议的补救措施，并决定执行其中一项建议的操作。

### 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中使用 Unified Manager 的所有任务。

在此示例中，您在 Unified Manager 事件管理库存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。

对于已满卷，您可以执行的补救措施包括：

- 在卷上启用自动增长、重复数据删除或压缩
- 调整卷大小或移动卷

- 从卷中删除或移动数据

尽管所有这些操作都必须从ONTAP系统管理器或ONTAP CLI 执行，但您可以使用 Unified Manager 来查找可能需要的信息，以确定要采取哪些操作。

#### 步骤

1. 在“事件”详细信息页面中，单击“源”字段中的卷名称即可查看有关受影响卷的详细信息。
2. 在“卷/健康”详细信息页面上，单击“配置”并查看卷上已启用重复数据删除和压缩。

您决定调整卷的大小。

3. 在“相关设备”窗格中，单击托管聚合的名称以查看该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，您会看到托管完整卷的聚合确实具有足够的未提交容量，因此您可以使用ONTAP系统管理器来调整卷的大小，从而为其提供更多容量。

#### 相关信息

["事件详细信息页面"](#)

### 管理健康阈值

您可以为所有聚合、卷和 qtree 配置全局健康阈值，以跟踪任何健康阈值违规。

#### 存储容量健康阈值是什么

存储容量健康阈值是 Unified Manager 服务器生成事件以报告存储对象的任何容量问题的点。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 的存储容量健康阈值均设置为默认值。您可以根据需要更改一个对象或一组对象的设置。

#### 配置全局健康阈值设置

您可以配置容量、增长、快照预留、配额和 inode 的全局健康阈值条件，以有效监控聚合、卷和 qtree 大小。您还可以编辑生成超过滞后阈值的事件的设置。

全局健康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，就会生成一个事件，并且如果配置了警报，则会发送警报通知。阈值默认值设置为推荐值，但您可以修改它们以按一定间隔生成事件，以满足您的特定需求。当阈值发生变化时，事件会在下一个监控周期中生成或淘汰。

可以从左侧导航菜单的事件阈值部分访问全局健康阈值设置。您还可以从该对象的库存页面或详细信息页面修改单个对象的阈值设置。

- 有关信息，请参阅["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，请参阅["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、覆盖保留空间和 inode 的运行状况阈值设置，以跟踪任何阈值违规。

- 有关信息，请参阅["配置全局 qtree 运行状况阈值"](#)。

您可以编辑所有 qtree 的容量健康阈值设置，以跟踪任何阈值违规。

- 有关信息，请参阅["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滞后时间百分比，以便以更适合您需要的间隔生成事件。

#### 配置全局聚合健康阈值

您可以为所有聚合配置全局健康阈值，以跟踪任何阈值违规。对于阈值突破，会生成适当的事件，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。

当您全局配置选项时，对象的默认值将被修改。但是，如果在对象级别更改了默认值，则不会修改全局值。

阈值选项具有默认值以便更好地监控，但是，您可以更改这些值以满足您的环境要求。

当在聚合上的卷上启用自动增长时，聚合容量阈值将被视为已突破，具体取决于自动增长设置的最大卷大小，而不是原始卷大小。



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“保存”。

#### 相关信息

["添加用户"](#)

#### 配置全局卷健康阈值

您可以配置所有卷的全局健康阈值来跟踪任何阈值违规。对于健康阈值违规，会生成适当的事件，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卷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。

大多数阈值选项都有默认值，以便更好地监控。但是，您可以更改这些值以满足您的环境要求。

请注意，当在卷上启用自动增长时，容量阈值将根据自动增长设置的最大卷大小（而不是原始卷大小）被视为已突破。



1000 个 Snapshot 副本的默认值仅适用于 ONTAP 版本为 9.4 或更高版本的 FlexVol 卷，以及 ONTAP 版本为 9.8 及更高版本的 FlexGroup 卷。对于安装了旧版本 ONTAP 软件的集群，每个卷的最大 Snapshot 副本数量为 250 个。对于这些旧版本，Unified Manager 将此数字 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，您将继续接收事件。如果您希望将这些旧版本的阈值设置为小于 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”>“音量”。
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“保存”。

## 相关信息

### ["添加用户"](#)

#### 配置全局 qtree 运行状况阈值

您可以为所有 qtree 配置全局健康阈值，以跟踪任何阈值违规。对于健康阈值违规，会生成适当的事件，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 qtree 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。

阈值选项具有默认值以便更好地监控，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。如果用户配额或组配额中定义的空间超出阈值，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“保存”。

#### 为非托管保护关系配置滞后阈值设置

您可以编辑非托管保护关系的全局默认滞后警告和错误健康阈值设置，以便按照适合您需要的间隔生成事件。

## 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，如果传输时间表是每小时一次，那么滞后时间不得超过一小时。滞后阈值用于指定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%，那么当滞后时间超过 1.5 小时时，您将收到事件。

此任务中描述的设置将全局应用于所有非托管保护关系。无法指定这些设置并将其专门应用于一个非托管保护关

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. 要禁用因任何滞后阈值量而触发的警告或错误事件，请取消选中“已启用”旁边的框。
4. 单击“保存”。

#### 相关信息

["添加用户"](#)

#### 编辑单个聚合健康阈值设置

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。当超过阈值时，就会生成警报并且您会收到通知。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。

根据阈值的变化，事件会在下一个监控周期中生成或淘汰。

当在聚合上的卷上启用自动增长时，聚合容量阈值将被视为已突破，具体取决于自动增长设置的最大卷大小，而不是原始卷大小。

#### 步骤

1. 在左侧导航窗格中，单击“存储”>“聚合”。
2. 在“**Health: All Aggregates**”视图中，选择一个或多个聚合，然后单击“**Edit Thresholds**”。
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之一的阈值设置：容量、增长或 Snapshot 副本。
4. 单击“保存”。

#### 相关信息

["添加用户"](#)

#### 编辑单个卷健康阈值设置

您可以编辑一个或多个卷的卷容量、增长、配额和空间预留的运行状况阈值设置。当超过阈值时，就会生成警报并且您会收到通知。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。

根据阈值的变化，事件会在下一个监控周期中生成或淘汰。

请注意，当在卷上启用自动增长时，容量阈值将根据自动增长设置的最大卷大小（而不是原始卷大小）被视为已突破。



1000 个 Snapshot 副本的默认值仅适用于 ONTAP 版本为 9.4 或更高版本的 FlexVol 卷，以及 ONTAP 版本为 9.8 及更高版本的 FlexGroup 卷。对于安装了旧版本 ONTAP 软件的集群，每个卷的最大 Snapshot 副本数量为 250 个。对于这些旧版本，Unified Manager 将此数字 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，您将继续接收事件。如果您希望将这些旧版本的阈值设置为小于 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“存储”>“卷”。
2. 在“**Health: All Volumes**”视图中，选择一个或多个卷，然后单击“**Edit Thresholds**”。
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，编辑以下之一的阈值设置：容量、Snapshot 副本、qtree 配额、增长或 inode。
4. 单击“保存”。

#### 相关信息

[“添加用户”](#)

#### 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，就会生成警报并且您会收到通知。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。

根据阈值的变化，事件会在下一个监控周期中生成或淘汰。

#### 步骤

1. 在左侧导航窗格中，单击“存储”>“Qtree”。
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 或 qtree 的容量阈值，然后单击“保存”。



您还可以从存储虚拟机/运行状况详细信息页面上的 Qtrees 选项卡设置单独的 qtree 阈值。

## 管理集群安全目标

Unified Manager 提供了一个仪表板，可根据《NetApp ONTAP 9 安全强化指南》中定义的建议来确定 ONTAP 集群、存储虚拟机 (SVM) 和卷的安全性。

安全仪表板的目的是显示 ONTAP 集群与 NetApp 推荐指南不一致的任何区域，以便您可以修复这些潜在问题。大多数情况下，您可以使用 ONTAP System Manager 或 ONTAP CLI 来解决问题。您的组织可能不会遵循所有建议，因此在某些情况下您不需要进行任何更改。

查看 ["NetApp ONTAP 9 安全强化指南"](#) (TR-4569) 以获取详细的建议和解决方案。

除了报告安全状态之外，Unified Manager 还会为任何存在安全违规的集群或 SVM 生成安全事件。您可以在事件管理库存页面中跟踪这些问题，并且可以为这些事件配置警报，以便在发生新的安全事件时通知您的存储管理员。

有关详细信息，请参阅 ["正在评估哪些安全标准"](#)。

正在评估哪些安全标准

一般来说，您的ONTAP集群、存储虚拟机 (SVM) 和卷的安全标准将根据《NetApp ONTAP 9 安全强化指南》中定义的建议进行评估。

一些安全检查包括：

- 集群是否使用安全身份验证方法，例如 SAML
- 对等集群的通信是否加密
- 存储虚拟机是否启用了审计日志
- 您的卷是否启用了软件或硬件加密

请参阅合规类别和 ["NetApp ONTAP 9 安全强化指南"](#)了解详细信息。



Active IQ平台报告的升级事件也被视为安全事件。这些事件标识了需要您升级ONTAP软件、节点固件或操作系统软件（以获取安全公告）才能解决的问题。这些事件不会显示在安全面板中，但可以从事件管理库存页面中获取。

有关详细信息，请参阅 ["管理集群安全目标"](#)。

集群合规性类别

该表描述了 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性的整体判定。

集群上存在不合规的 SVM 将影响集群的合规性值。因此在某些情况下，您可能需要先修复 SVM 的安全问题，然后集群安全性才被视为合规。

请注意，下面列出的每个参数并非都会出现在所有安装中。例如，如果您没有对等集群，或者您在集群上禁用了AutoSupport，那么您将不会在 UI 页面中看到 Cluster Peering 或AutoSupport HTTPS Transport 项。

| 参数      | 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 时，TLSv1 和 SSLv3 被禁用，并且只允许使用 TLSv1.1 和 TLSv1.2。 | 已启用 | 是       |



| 参数                   | 描述                                                                                                                                                    | 建议  | 影响集群合规性 |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----|---------|
| Telnet               | 指示是否启用或禁用 Telnet 系统访问。NetApp 建议使用安全外壳 (SSH) 进行安全远程访问。                                                                                                 | 已禁用 | 是       |
| 不安全 SSH 设置           | 指示 SSH 是否使用不安全的密码，例如以 *cbc 开头的密码。                                                                                                                     | 否   | 是       |
| 登录横幅                 | 指示是否对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否加密或未加密。必须在源集群和目标集群上配置加密，此参数才被视为合规。                                                                                                       | 已加密 | 是       |
| 网络时间协议               | 指示集群是否已配置一个或多个 NTP 服务器。为了实现冗余和最佳服务，NetApp 建议您至少三个 NTP 服务器与集群关联。                                                                                       | 已配置 | 是       |
| OCSP                 | 从 9.14.1 开始，Active IQ Unified Manager 在存储虚拟机 (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 验证适用于与 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       |
| 远程审计日志               | 指示日志转发 (Syslog) 是否加密。                                                                                                                                 | 已加密 | 是       |
| AutoSupport HTTPS 传输 | 指示是否使用 HTTPS 作为向 NetApp 支持发送 AutoSupport 消息的默认传输协议。                                                                                                   | 已启用 | 是       |
| 默认管理员用户              | 指示默认管理员用户 (内置) 是否启用或禁用。NetApp 建议锁定 (禁用) 任何不需要的内置帐户。                                                                                                   | 已禁用 | 是       |



| 参数                  | 描述                                                                          | 建议   | 影响集群合规性 |
|---------------------|-----------------------------------------------------------------------------|------|---------|
| SAML 用户             | 指示是否配置了 SAML。SAML 使您能够将多重身份验证 (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。对于管理集群的用户而非本地用户来说，Active Directory 和 LDAP 是首选的身份验证机制。          | 否    | 否       |
| 证书用户                | 指示是否配置了证书用户来登录集群。                                                           | 否    | 否       |
| 本地用户                | 指示是否配置本地用户登录集群。                                                             | 否    | 否       |
| 远程 Shell            | 指示 RSH 是否启用。出于安全原因，应禁用 RSH。首选使用安全外壳 (SSH) 进行安全远程访问。                         | 已禁用  | 是       |
| MD5 使用中             | 指示ONTAP用户帐户是否使用安全性较低的 MD5 哈希函数。建议将 MD5 Hashed 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       |

#### 存储虚拟机合规性类别

该表描述了 Unified Manager 评估的存储虚拟机 (SVM) 安全合规性标准、NetApp建议以及该参数是否影响对 SVM 是否合规的整体判断。

| 参数           | 描述                             | 建议  | 影响 <b>SVM</b> 合规性 |
|--------------|--------------------------------|-----|-------------------|
| 审核日志         | 指示审计日志记录是否启用或禁用。               | 已启用 | 是                 |
| 不安全 SSH 设置   | 指示 SSH 是否使用不安全的密码，例如以 cbc*。    | 否   | 是                 |
| 登录横幅         | 指示是否为访问系统上的 SVM 的用户启用或禁用登录横幅。  | 已启用 | 是                 |
| LDAP 加密      | 指示 LDAP 加密是否启用或禁用。             | 已启用 | 否                 |
| NTLM 身份验证    | 指示 NTLM 身份验证是否启用或禁用。           | 已启用 | 否                 |
| LDAP 有效负载签名  | 指示 LDAP 有效负载签名是否启用或禁用。         | 已启用 | 否                 |
| CHAP 设置      | 指示 CHAP 是启用还是禁用。               | 已启用 | 否                 |
| Kerberos V5  | 指示是否启用或禁用 Kerberos V5 身份验证。    | 已启用 | 否                 |
| NIS 身份验证     | 指示是否配置了 NIS 身份验证的使用。           | 已禁用 | 否                 |
| FPolicy 状态有效 | 指示是否创建了 FPolicy。               | 是   | 否                 |
| 已启用 SMB 加密   | 指示是否未启用 SMB-Signing & Sealing。 | 是   | 否                 |
| 已启用 SMB 签名   | 指示是否未启用 SMB 签名。                | 是   | 否                 |

#### 容量合规性类别

下表描述了 Unified Manager 评估的卷加密参数，以确定卷上的数据是否受到充分保护，以免被未经授权的用户访问。

请注意，卷加密参数不会影响集群或存储虚拟机是否被视为合规。

| 参数        | 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的数量。 |
| 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的数量。                                     |
| 未加密       | 显示未加密的卷数。                                              |

### 不合规意味着什么

如果根据《NetApp ONTAP 9 安全强化指南》中定义的建议评估的任何安全标准未得到满足，则集群和存储虚拟机 (SVM) 被视为不合规。此外，当任何 SVM 被标记为不合规时，该集群被视为不合规。

安全卡中的状态图标与其合规性有以下关系：

-  - 参数配置符合推荐要求。
-  - 参数未按建议配置。
-  - 集群上未启用该功能，或者未按建议配置该参数，但该参数对对象的合规性没有贡献。

请注意，卷加密状态不会影响集群或 SVM 是否被视为合规。

### 查看集群和存储虚拟机的安全状态

Active IQ Unified Manager使您能够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，请参阅 ["NetApp ONTAP 9 安全强化指南"](#)

在“安全”页面上查看对象级别的安全状态

作为系统管理员，您可以使用“安全”页面来了解数据中心和站点级别的ONTAP集群和存储虚拟机的安全强度。支持的对象是集群、存储虚拟机和卷。按照下面的步骤进行操作：

#### 步骤

1. 在左侧导航窗格中，单击“仪表板”。
2. 根据您是否要查看所有受监控集群或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。将显示“安全”页面。

单击条形图、计数和 `View Reports` 链接将带您进入卷、集群或存储虚拟机页面，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：数据中心内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：数据中心内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：您环境中所有卷的卷加密状态（已加密或未加密的卷数）
- 卷反勒索软件状态：您环境中所有卷的安全状态（启用或禁用反勒索软件的卷数量）
- 集群身份验证和证书：使用每种身份验证方法的集群数量，例如 SAML、Active Directory 或通过证书和本地身份验证。该面板还显示证书已过期或即将在 60 天内过期的集群数量。

在集群页面查看所有集群的安全详情

通过“集群/安全”详细信息页面，您可以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”>“集群”。
2. 选择“查看”>“安全”>“所有集群”。

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 传输和集群证书过期状态。

您可以单击  更多选项按钮并选择在 Unified Manager 的 安全 页面或系统管理器上查看安全详细信息。您应该拥有有效的凭证才能查看系统管理器上的详细信息。



如果集群的证书已过期，您可以单击 `expired` 在\*集群证书有效性\*下，并从系统管理器（9.10.1 及更高版本）更新它。您无法单击 `expired` 如果系统管理器实例的版本早于 9.10.1。

从存储虚拟机页面查看所有集群的安全详细信息

通过“存储虚拟机/安全”详细信息页面，您可以查看存储虚拟机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”>“存储虚拟机”。
2. 选择“查看”>“安全”>“所有存储虚拟机”。显示具有安全参数的集群列表。

您可以通过检查安全参数（例如存储虚拟机、集群、登录横幅、审计日志和不安全的 SSH 设置）来默认了解存储虚拟机的安全合规性。

您可以单击  更多选项按钮并选择在 Unified Manager 的 安全 页面或系统管理器上查看安全详细信息。您应该拥有有效的凭证才能查看系统管理器上的详细信息。

有关卷和存储虚拟机的反勒索软件安全详细信息，请参阅[查看所有卷和存储虚拟机的反勒索软件状态](#)。

查看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范围为“升级”。这些事件由Active IQ平台报告，它们识别需要升级ONTAP软件、节点固件或操作系统软件（用于安全公告）才能解决的问题。

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。

您可能希望立即对其中一些问题采取纠正措施，而其他问题可能要等到下次预定的维护时再解决。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，如果您不想收到某些安全升级事件的通知，此列表可以帮助您识别这些事件，以便您可以禁用它们。

#### 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（新事件和已确认）事件都会显示在事件管理库存页面上。

2. 从“查看”菜单中，选择“升级事件”。

该页面显示所有活动的升级安全事件。

#### 查看所有集群上用户身份验证的管理方式

安全页面显示用于对每个集群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集群的用户数量。这使您能够验证用户身份验证是否按照组织的定义安全地执行。

#### 步骤

1. 在左侧导航窗格中，单击“仪表板”。
2. 在仪表板顶部，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\*卡片，了解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。

如果某些用户使用不安全的方法访问系统，或者使用NetApp不推荐的方法，您可以禁用该方法。

#### 查看所有卷的加密状态

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，以免被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有：

- 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“存储”>“卷”。
2. 在“查看”菜单中，选择“健康”>“卷加密”
3. 在\*健康：卷加密\*视图中，按\*加密类型\*字段进行排序，或使用过滤器显示具有特定加密类型或未加密的卷（加密类型为“无”）。

查看所有卷和存储虚拟机的反勒索软件状态

您可以查看所有卷和存储虚拟机 (SVM) 及其当前反勒索软件状态的列表，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，请参阅["ONTAP：启用反勒索软件"](#)。

查看所有具有反勒索软件检测功能的卷的安全详细信息

步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“查看”菜单中，选择“健康”>“安全”>“反勒索软件”
3. 在\*安全：反勒索软件\*视图中，您可以按各个字段进行排序或使用过滤器。



离线卷、受限卷、SnapLock卷、FlexGroup卷、FlexCache卷、仅 SAN 卷、已停止的存储虚拟机的卷、存储虚拟机的根卷或数据保护卷不支持反勒索软件。

查看所有具有反勒索软件检测功能的存储虚拟机的安全详细信息

步骤

1. 在左侧导航窗格中，单击“存储”>“存储虚拟机”。
2. 选择“查看”>“安全”>“反勒索软件”。显示具有反勒索软件状态的 SVM 列表。



未启用 NAS 协议的存储虚拟机不支持反勒索软件监控。

查看所有活动的安全事件

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问题的用户。此外，如果您不想接收某些安全事件，此列表可以帮助您识别要禁用的事件。

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，新事件和已确认事件显示在事件管理库存页面上。

2. 从“查看”菜单中，选择“活动安全事件”。

该页面显示过去 7 天内生成的所有新的和已确认的安全事件。

## 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 收到的任何其他事件一样。此外，如果您想平等对待所有安全事件并将电子邮件发送给同一个人，您可以创建单个警报，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。

下面的示例显示如何为“Telnet 协议已启用”安全事件创建警报。如果配置了 Telnet 访问以对集群进行远程管理访问，则将发送警报。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”，然后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群集。
5. 单击“事件”并执行以下操作：
  - a. 在事件严重性列表中，选择\*警告\*。
  - b. 在匹配事件列表中，选择\*Telnet 协议已启用\*。
6. 单击“操作”，然后在“警告这些用户”字段中选择将接收警报电子邮件的用户的姓名。
7. 配置此页面上的任何其他选项，包括通知频率、发出 SNMP trap 和执行脚本。
8. 单击“保存”。

## 禁用特定安全事件

默认情况下，所有事件均启用。您可以禁用特定事件以防止生成那些在您的环境中不重要的事件的通知。如果您想恢复接收已禁用的事件的通知，您可以启用它们。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

当您禁用事件时，系统中先前生成的事件将被标记为过时，并且不会触发为这些事件配置的警报。当您启用已禁用的事件时，将从下一个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来禁用或启用事件：

| 目的   | 操作                                                                                                                                                                                                                     |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 禁用事件 | <ol style="list-style-type: none"> <li>单击“禁用”。</li> <li>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。</li> <li>在“匹配事件”列中，选择要禁用的安全事件，然后单击向右箭头将这些事件移动到“禁用事件”列。</li> <li>单击“保存并关闭”。</li> <li>验证您禁用的事件是否显示在“事件设置”页面的列表视图中。</li> </ol> |
| 启用事件 | <ol style="list-style-type: none"> <li>从已禁用事件列表中，选中要重新启用的一个或多个事件的复选框。</li> <li>单击“启用”。</li> </ol>                                                                                                                      |

## 安全事件

安全事件根据《NetApp ONTAP 9 安全强化指南》中定义的参数，为您提供有关ONTAP集群、存储虚拟机 (SVM) 和卷的安全状态的信息。这些事件会通知您潜在的问题，以便您评估其严重性并在必要时解决问题。

安全事件按来源类型分组，包括事件和陷阱名称、影响级别和严重性。这些事件出现在集群和存储虚拟机事件类别中。

## 管理备份和恢复操作

您可以创建Active IQ Unified Manager的备份，并在系统发生故障或数据丢失时使用恢复功能将备份恢复到同一（本地）系统或新的（远程）系统。

根据安装 Unified Manager 的操作系统以及所管理的集群和节点的数量，有三种备份和还原方法：

| 操作系统                     | 部署规模 | 推荐的备份方法                         |
|--------------------------|------|---------------------------------|
| 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   | NetApp Unified Manager 数据库快照    |



| 操作系统              | 部署规模 | 推荐的备份方法                                   |
|-------------------|------|-------------------------------------------|
| Microsoft Windows | 小型   | Unified Manager MySQL 数据库转储               |
|                   | 大型   | 采用 iSCSI 协议的 Unified Manager 数据库的NetApp快照 |

这些不同的方法将在以下章节中描述。

### 虚拟设备上 **Unified Manager** 的备份和恢复

当 Unified Manager 安装在虚拟设备上时，其备份和恢复模型是捕获和恢复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. 关闭虚拟机并拍摄 Unified Manager 虚拟设备的 VMware 快照。
2. 在数据存储上制作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 副本或等效快照复制到备用存储。
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 Unified Manager 虚拟设备受到保护。

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恢复

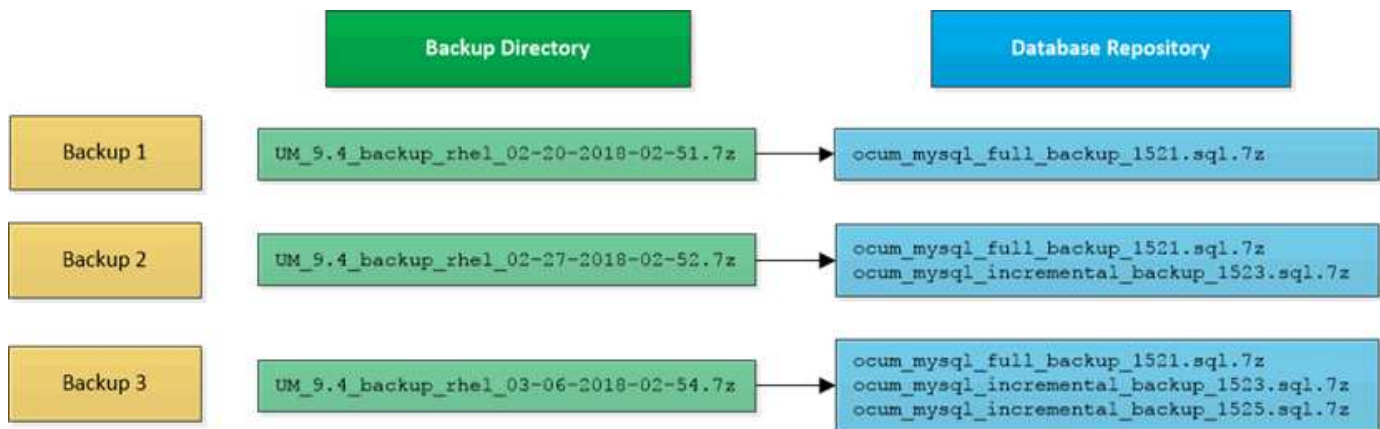
MySQL 数据库转储备份是Active IQ Unified Manager数据库和配置文件的副本，您可以在系统故障或数据丢失时使用它。您可以计划将备份写入本地目标或远程目标。强烈建议您定义Active IQ Unified Manager主机系统外部的远程位置。



当 Unified Manager 安装在 Linux 和 Windows 服务器上时，MySQL 数据库转储是默认备份机制。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，则您可以使用 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，因为它仅包含指向重新创建备份所需的数据库存储库目录中的文件指针。

第一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的备份文件。下次生成备份时，系统将在备份目录中创建单个文件，并在数据库存储库目录中创建增量备份文件，其中包含与完整备份文件的差异内容。当您创建其他备份时，此过程将继续进行，直到达到最大保留设置为止，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。此外，它还会检查系统上是否具有足够的空间来创建备份文件。

#### 配置数据库转储备份的目标和计划

您可以配置 Unified Manager 数据库转储备份设置来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的备份。默认情况下，计划备份是禁用的，但您应该设置备份计划。

#### 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。

- 当 Unified Manager 安装在 Linux 系统上并使用 MySQL 备份时，请确保在备份目录上设置以下权限和所有权。

权限：0750，所有权：jboss: maintenance

- 当 Unified Manager 安装在 Windows 系统上并使用 MySQL 备份时，请确保只有管理员才能访问备份目录。

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您为备份分配的空间来说太大，您可以定期进行完整备份以替换旧备份及其增量文件。另一种选择是，您可以使用 Snapshot 副本进行备份。
- 在新集群添加后的最初 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”。

数据库转储备份文件是根据计划创建的。您可以在数据库备份页面中看到可用的备份文件。

#### 什么是数据库还原

MySQL 数据库恢复是将现有的 Unified Manager 备份文件恢复到相同或不同的 Unified Manager 服务器的过程。您可以从 Unified Manager 维护控制台执行恢复操作。

如果您在同一（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。如果您在不同的 Unified Manager 系统（远程系统）上执行还原操作，则必须在运行还原选项之前将备份文件从辅助存储复制到本地磁盘。

在恢复过程中，您将退出 Unified Manager。在还原过程完成之后，您可以登录到该系统。

如果要将备份映像还原到新服务器，则还原操作完成后，您需要生成新的 HTTPS 安全证书并重新启动 Unified Manager 服务器。如果要将备份映像还原到新服务器时，则您还需要重新配置 SAML 身份验证设置（如果需要这些设置）。



Unified Manager 升级到较新版本的软件后，旧备份文件无法用于恢复映像。为了节省空间，升级 Unified Manager 时会自动删除除最新文件之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 Windows 上还原 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，同时将损失降至最低。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。
- 您必须已将 Unified Manager 备份文件和数据库存储库目录的内容复制到将执行恢复操作的系统。

建议您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 `database\_dumps\_repo` 下的子目录 `backup` 目录。

- 备份文件必须是`.7z`类型。

还原功能与平台和版本相关。您只能在同一版本的 Unified Manager 上恢复 Unified Manager MySQL 备份，并且只能在 Windows 平台上恢复 Windows 备份。



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括在双引号中。

#### 步骤

1. 如果您要在新服务器上执行还原，则在安装 Unified Manager 后，请勿在安装完成后启动 UI 或配置任何集群、用户或身份验证设置。备份文件在恢复过程中填充此信息。
2. 使用管理员凭据登录 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` 然后按 Enter 键。
5. 在维护控制台\*主菜单\*中，输入\*备份恢复\*选项的编号。
6. 输入\*恢复 MySQL 备份\*的号码。
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
```

恢复操作完成后，您可以登录 Unified Manager。

还原备份后，如果 OnCommand Workflow Automation 服务器不工作，请执行以下步骤：

1. 在工作流自动化服务器上，将 Unified Manager 服务器的 IP 地址更改为指向最新的机器。
2. 在 Unified Manager 服务器上，如果在步骤 1 中获取失败，请重置数据库密码。

#### 使用 NetApp 快照进行备份和恢复

NetApp Snapshot 副本会创建 Unified Manager 数据库和配置文件的时间点映像，您可以在系统发生故障或数据丢失时使用这些映像进行恢复。您可以安排定期将 Snapshot 副本写入其中一个 ONTAP 集群上的卷，以便始终拥有最新副本。



此功能不适用于安装在虚拟设备上的 Active IQ Unified Manager。

#### 在 Linux 上配置备份

如果您的 Active IQ Unified Manager 安装在 Linux 机器上，那么您可以决定使用 NetApp Snapshots 配置备份和恢复。

快照复制所需的时间非常短，通常只需几分钟，并且 Unified Manager 数据库的锁定时间非常短，因此对您的安装造成的干扰非常小。此映像占用的存储空间极少，并且性能开销可以忽略不计，因为它仅会记录自上次执行 Snapshot 副本以来对文件所做的更改。由于快照是在 ONTAP 集群上创建的，因此您可以利用其他 NetApp 功能

(例如SnapMirror) 来创建二级保护(如果需要)。

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。



- 您只能在同一版本的Active IQ Unified Manager上恢复 Snapshot 副本。  
例如, 如果您在 Unified Manager 9.16 上创建了备份, 则只能在 Unified Manager 9.16 系统上恢复该备份。
- 如果快照配置有任何变化, 可能会导致快照无效。

### 配置 Snapshot 副本位置

您可以使用ONTAP系统管理器或使用ONTAP CLI 在其中一个ONTAP集群上配置存储 Snapshot 副本的卷。

开始之前

集群、存储虚拟机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
  - 它应该在地理位置上靠近 Unified Manager 服务器
  - 它可以通过 Unified Manager 进行监控, 但这不是必需的
- 存储虚拟机要求:
  - 必须设置名称开关和名称映射才能使用“文件”
  - 创建与客户端用户对应的本地用户
  - 确保选择了“所有读/写访问”
  - 确保在导出策略中将超级用户访问权限设置为“any”
  - 适用于 Linux 的NetApp快照的 NFS
  - 必须在 NFS 服务器上启用 NFSv4, 并在客户端和存储虚拟机上指定 NFSv4 ID 域
  - 该卷的大小至少应为 Unified Manager/opt/netapp/data 目录的两倍

使用命令 `du -sh /opt/netapp/data/` 检查当前大小。

- 音量要求:
  - 该卷的大小至少应为 Unified Manager /opt/netapp/data 目录的两倍
  - 安全模式必须设置为 UNIX
  - 必须禁用本地快照策略
  - 应启用卷自动调整功能
  - 性能服务级别应设置为高IOPS、低延迟的策略, 例如“Extreme”

有关创建 NFS 卷的详细步骤, 请参阅 ["如何在ONTAP 9 中配置 NFSv4"](#)以及 ["ONTAP 9 NFS 配置快速指南"](#)。

## 指定 **Snapshot** 副本的目标位置

您应该在已在某个ONTAP集群中配置的卷上配置Active IQ Unified Manager Snapshot 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Linux 主机的 root 用户凭据。
- 您必须拥有授权登录 Unified Manager 服务器维护控制台的用户 ID 和密码。
- 您必须拥有集群管理 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。
- 您必须已将卷挂载到Active IQ Unified Manager主机，并且必须具有挂载路径。

### 步骤

1. 使用安全外壳连接到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` 然后按 Enter 键。
4. 在维护控制台\*主菜单\*中，输入\*备份恢复\*选项的编号。
5. 输入“配置**NetApp**快照备份”的号码。
6. 输入数字来配置 NFS。
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. 要识别将写入快照的卷，请输入集群管理界面的 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. 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. 如果您尚未执行此操作，请退出维护控制台并启动Active IQ Unified Manager界面来为 Snapshot 副本创建计划。

### 在 **Windows** 上配置备份

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 Snapshots 进行备份和恢复。

当所有 Unified Manager 服务都在运行时，可以进行基于快照的备份。由于备份对整个数据库设置了全局读取锁，以防止任何并发写入，因此数据库的一致状态被捕获为快照的一部分。为了使安装在 Windows 操作系统上的 Unified Manager 系统使用NetApp Snapshots 执行备份和恢复，您应该首先使用维护控制台将 Unified Manager 备份配置为基于 Snapshot。

在配置 Unified Manager 以创建 Snapshot 副本之前，您应该执行以下配置任务。



- 配置ONTAP集群
- 配置 Windows 主机

## 配置 Windows 的备份位置

在 Windows 上备份 Unified Manager 后，您应该配置用于存储 Snapshot 副本的卷。

开始之前

集群、存储虚拟机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
  - 它应该在地理位置上靠近 Unified Manager 服务器
  - 由 Unified Manager 监控
- 存储虚拟机要求：
  - ONTAP集群上的 iSCSI 连接
  - 必须为配置的机器启用 iSCSI 协议
  - 您应该有一个专用卷和 LUN 用于备份配置。所选卷应该仅包含一个 LUN，而不包含任何其他内容。
  - LUN 的大小应至少为 9.9 Active IQ Unified Manager中预期处理的数据大小的两倍。

这也对体积提出了相同的尺寸要求。

- 确保选择了“所有读/写访问”
  - 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：
  - 该卷的大小至少应为 Unified Manager MySQL 数据目录的两倍。
  - 安全模式必须设置为 Windows
  - 必须禁用本地快照策略
  - 应启用卷自动调整功能
  - 性能服务级别应设置为高IOPS、低延迟的策略，例如“Extreme”

## 配置ONTAP集群

在 Windows 系统上使用 Snapshot 副本备份和恢复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系统管理器用户界面配置ONTAP集群。ONTAP集群的配置涉及配置数据 LIF，以便可作为 iSCSI LIF 分配给存储虚拟机。下一步是使用系统管理器用户界面配置启用 iSCSI 的存储虚拟机。您需要为此存储虚拟机配置静态网络路由，以控制 LIF 如何使用网络进行出站流量。



您应该有一个专用卷和一个 LUN 用于备份配置。选定的卷应该只包括一个 LUN。LUN 的大小应至少为Active IQ Unified Manager预计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 的存储虚拟机或使用具有相同配置的现有存储虚拟机。
2. 为已配置的存储虚拟机配置网络路由。
3. 配置适当容量的卷和其中的单个 LUN，确保该卷仅专用于此 LUN。



在系统管理器上创建 LUN 的情况下，取消映射 LUN 可能会删除 igroup，并且还原可能会失败。为避免这种情况，请确保在创建 LUN 时明确创建 LUN，并且在取消映射 LUN 时不会删除该 LUN。

4. 在存储虚拟机中配置启动器组。
5. 配置端口集。
6. 将 igroup 与端口集集成。
7. 将 LUN 映射到 igroup。

#### 配置 Windows 主机

您需要先配置 Windows 主机，然后才能使用 NetApp Snapshot 备份和恢复 Active IQ Unified Manager。要在 Windows 主机上启动 Microsoft iSCSI 启动器，请在搜索栏中输入“iscsi”，然后单击 **iSCSI Initiator**。

#### 开始之前

您应该清理主机上的所有先前配置。

如果您尝试在全新安装的 Windows 上启动 iSCSI 启动器，系统将提示您确认，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 主机上的所有先前配置。

#### 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. 发现在 Windows 机器中配置为设备的 LUN。
7. 在 Windows 中将发现的 LUN 配置为新的卷驱动器。

#### 指定 Windows 上 Snapshot 副本的目标位置

您应该在已在某个 ONTAP 集群中配置的卷上配置 Active IQ Unified Manager Snapshot 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。



- 您必须拥有授权登录 Unified Manager 服务器维护控制台的用户 ID 和密码。
- 您必须拥有集群管理 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安装到Active IQ Unified Manager主机，并且必须具有安装驱动器。

#### 步骤

1. 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` 然后按 Enter 键。
4. 在维护控制台\*主菜单\*中，输入\*备份恢复\*选项的编号。
5. 输入“配置**NetApp**快照备份”的号码。
6. 输入号码来配置 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. 要识别将写入快照的卷，请输入集群管理界面的 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. 验证此信息并输入 y。

系统执行以下任务：

- 存储虚拟机已验证
- 音量已验证
- 安装驱动器并验证状态
- LUN 存在和状态
- 网络驱动器存在
- 已验证安装卷上是否存在推荐空间（大于 mysql 数据目录的两倍）
- 卷中专用 LUN 对应的 LUN 路径
- igroup 名称
- 网络驱动器安装卷的 GUID
- 用于与ONTAP通信的 iSCSI 启动器

10. 退出维护控制台并启动Active IQ Unified Manager界面来创建 Snapshot 副本的计划。

从维护控制台配置 **Snapshot** 副本备份

要使用 Snapshot 副本进行Active IQ Unified Manager备份，您应该从维护控制台执行一些配置步骤。

开始之前

您应该了解系统的以下详细信息：

- 集群 IP 地址
- 存储 VM 名称

- 卷名
- LUN 名称
- 挂载路径
- 存储系统凭证

#### 步骤

1. 访问 Unified Manager 的维护控制台。
2. 输入 4 选择 备份恢复。
3. 输入 2 选择 使用**NetApp Snapshot** 备份和恢复。



如果要更改备份配置，请输入 3 以选择 更新**NetApp Snapshot Backup Configuration**。您只能更新密码。

4. 从菜单中输入 1 选择 配置**NetApp**快照备份。
5. 输入 1 以提供所需信息。
6. 提供维护控制台的用户名和密码，然后确认 LUN 已安装在主机上。

然后，该过程会验证您提供的数据库目录、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安装的存储
- 数据库目录被删除，符号链接被建立
- 服务重新启动在Active IQ Unified Manager界面中完成配置后，备份类型修改为NetApp Snapshot，并在用户界面中反映为数据库备份（基于快照）。

在开始备份操作之前，您必须检查快照配置是否有任何变化，因为这可能会导致快照无效。假设您在 G 盘中配置了备份并拍摄了快照。您稍后将备份重新配置到 E 盘，并且数据将按照新配置保存到 E 盘。如果您尝试恢复在 G 驱动器中拍摄的快照，则会失败并出现错误“G 驱动器不存在”。

为 **Linux** 和 **Windows** 定义备份计划

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。
- 您必须已从维护控制台配置创建 Snapshot 副本的设置，以确定将创建快照的目标位置。

只需几分钟即可创建快照副本，并且 Unified Manager 数据库仅锁定几秒钟。



在新集群添加后的最初 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 Snapshot 副本的最大数量。

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，而不管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”。

快照副本是根据计划创建的。您可以在数据库备份页面中看到可用的备份文件。

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，以便在以下情况下收到通知：

- 卷空间已满 90%。使用事件 **Volume Space Full** 来设置警报。

您可以使用ONTAP System Manager 或ONTAP CLI 向卷添加容量，以便 Unified Manager 数据库不会耗尽空间。

- 快照数量已接近最大数量。使用事件 **Too Many Snapshot Copies** 来设置警报。

您可以使用ONTAP System Manager 或ONTAP CLI 删除旧快照，以便始终有空间存储新的 Snapshot 副本。

您可以在警报设置页面中配置警报。

#### 使用 Snapshot 副本还原 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，同时将数据损失降至最低。您可以使用 Unified Manager 维护控制台将 Unified Manager Snapshot 数据库还原到本地或远程操作系统。

#### 开始之前

- 您必须拥有 Linux 主机的 root 用户凭据以及安装了 Unified Manager 的 Windows 主机的管理权限。
- 您必须拥有授权登录 Unified Manager 服务器维护控制台的用户 ID 和密码。

还原功能与平台和版本相关。您只能在同一版本的 Unified Manager 上恢复 Unified Manager 备份。

#### 步骤

1. 连接到 Unified Manager 系统的 IP 地址或完全限定域名。
  - Linux：安全外壳
  - Windows：Power Shell
2. 使用 root 用户凭据登录系统。
3. 输入命令 `maintenance\_console` 然后按 Enter 键。
4. 在维护控制台\*主菜单\*中，输入 4 作为\*备份恢复\*选项。
5. 输入 2 选择 使用**NetApp Snapshot** 备份和恢复。

如果您要在新服务器上执行还原，则在安装 Unified Manager 后，请勿在安装完成后启动 UI 或配置任何集群、用户或身份验证设置。输入 1 选择 配置**NetApp Snapshot Backup** 并配置 Snapshot 副本的设置，就像它们在原始系统上一样。

6. 输入 3 选择 使用**NetApp Snapshot** 恢复。
7. 选择要从中还原 Unified Manager 的 Snapshot 副本。按 **Enter**。
8. 恢复过程完成后，登录 Unified Manager 用户界面。

恢复备份后，如果工作流自动化服务器不工作，请执行以下步骤：

1. 在工作流自动化服务器上，将 Unified Manager 服务器的 IP 地址更改为指向最新的机器。
2. 在 Unified Manager 服务器上，如果在步骤 1 中获取失败，请重置数据库密码。

#### 修改备份类型

如果您想更改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 选项使您能够恢复到基于 MySQL 的备份。

#### 开始之前

您必须拥有授权登录 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 进行备份和恢复。
3. 从\*备份和恢复菜单\*中选择 2。
4. 选择 4 表示“取消配置**NetApp**快照备份”。

显示执行的操作：停止服务、断开符号链接、将数据从存储移动到目录，然后重新启动服务。

修改备份方式后，备份机制由Snapshot copy改为默认MySQL备份。此更改出现在常规设置的数据库备份部分。

#### Unified Manager 的按需备份

您可以使用Active IQ Unified Manager用户界面在需要时生成按需备份。按需备份使您能够使用现有的备份方法立即创建备份。按需备份不区分基于 MySQL 或NetApp Snapshot 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 Unified Manager 虚拟设备迁移到 Linux 系统

如果您想更改运行 Unified Manager 的主机操作系统，您可以将 Unified Manager MySQL 数据库转储备份从虚拟设备还原到 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。
  - 您必须知道执行恢复操作的 Unified Manager 维护用户的名称。
- 在Linux系统上：
  - 您必须按照["在 Linux 系统上安装 Unified Manager"](#)。
  - 此服务器上的 Unified Manager 版本必须与您使用备份文件的虚拟设备上的版本相同。
  - 安装后，请勿启动 UI 或在 Linux 系统上配置任何集群、用户或身份验证设置。备份文件在恢复过程中填充此信息。
  - 您必须拥有 Linux 主机的 root 用户凭据。

这些步骤描述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，然后将数据库备份恢复到新系统。

#### 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”部分中，选择“每日计划”，然后输入比当前时间晚几分钟的时间，以便尽快创建备份。
5. 单击“应用”。
6. 等待几个小时即可生成备份。

完整备份可能超过 1 GB，并且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，然后使用 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/* .
```

确保您已复制 .7z 备份文件和 /database-dumps-repo 子目录中的所有 .7z 存储库文件。

8. 在命令提示符下，恢复备份：`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 Unified Manager Web UI。

您应该执行以下任务：

- 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），或者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，请重新配置工作流自动化连接的两侧。

- 如果您使用 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

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。当事件触发警报时，脚本就会执行。您可以上传自定义脚本并在生成警报时测试其执行情况。

默认情况下，将脚本上传到 Unified Manager 并运行它们的功能是启用的。如果您的组织由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。

### 脚本如何与警报结合使用

您可以将警报与脚本关联，以便在 Unified Manager 中针对某个事件发出警报时执行该脚本。您可以使用脚本来解决存储对象的问题，或者标识哪些存储对象正在生成事件。

当 Unified Manager 中某个事件生成警报时，会向指定的收件人发送警报电子邮件。如果您已将警报与脚本关联，则系统将执行该脚本。您可以从警报电子邮件中获取传递给脚本的参数详细信息。



如果您创建了自定义脚本并将其与特定事件类型的警报关联，则会根据该事件类型的自定义脚本采取操作，并且“管理操作”页面或 Unified Manager 仪表板上默认不提供“修复”操作。

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
```

## 添加脚本

您可以在 Unified Manager 中添加脚本，并将脚本与警报关联。生成警报时，系统将自动执行这些脚本，使您能够获得有关生成事件的存储对象的信息。

### 开始之前

- 您必须已创建并保存要添加到 Unified Manager 服务器的脚本。
- 脚本支持的文件格式包括 Perl、Shell、PowerShell、Python 和 `.bat` 文件。

| 安装 <b>Unified Manager</b> 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，而脚本仅支持 Perl 5 支持的功能。如果在 Unified Manager 之后安装了 Perl，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来跟踪警报脚本进度，则必须确保日志文件不会在 Unified Manager 安装文件夹内的任何位置创建。

- 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。



如果您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“添加”。

### 删除脚本

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。
- 该脚本不得与警报关联。

#### 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。

### 测试脚本执行

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传到 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 | <div>a. 单击“添加”。</div> <div>b. 在“操作”部分，将警报与您的测试脚本关联。</div>          |
| 编辑警报 | <div>a. 选择一个警报，然后单击“编辑”。</div> <div>b. 在“操作”部分，将警报与您的测试脚本关联。</div> |

5. 单击“保存”。
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\*。

该脚本使用“-test”参数执行，并将通知警报发送到创建警报时指定的电子邮件地址。

### 管理和监控群组

您可以在 Unified Manager 中创建组来管理存储对象。



## 了解群组

您可以在 Unified Manager 中创建组来管理存储对象。了解有关组的概念以及组规则如何使您能够将存储对象添加到组中将有助于您管理环境中的存储对象。

### 什么是群组

组是异构存储对象（集群、SVM 或卷）的动态集合。您可以在 Unified Manager 中创建组来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。
- 您可以将一个组与多个组规则关联。
- 每个组可以包含多种类型的存储对象，例如集群、SVM 或卷。
- 根据组规则的创建时间或 Unified Manager 完成监控周期的时间，存储对象会动态添加到组中。
- 您可以同时对组中的所有存储对象应用操作，例如设置卷的阈值。

### 群组规则如何适用于群组

组规则是您定义的标准，用于将存储对象（卷、集群或 SVM）纳入特定组。您可以使用条件组或条件来定义组的组规则。

- 您必须将组规则与组关联。
- 您必须为组规则关联一个对象类型；一个组规则只能关联一种对象类型。
- 在每个监控周期之后或者创建、编辑或删除规则时，都会在组中添加或删除存储对象。
- 一个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。
- 根据您创建的组规则，存储对象可以属于多个组。

## 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。您可以在组的组规则中应用所有定义的条件组，以指定哪些存储对象包含在组中。

条件组内的条件使用逻辑“与”来执行。条件组中的所有条件必须满足。创建或修改组规则时，将创建一个条件，该条件仅应用、选择和分组满足条件组中所有条件的存储对象。当您想要缩小组中包含的存储对象的范围时，您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来创建具有存储对象的条件。

| 存储对象类型 | 适用操作数                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------|
| 卷      | <ul style="list-style-type: none"> <li>• 对象名称</li> <li>• 所属集群名称</li> <li>• 所属 SVM 名称</li> <li>• 标注</li> </ul> |
| SVM    | <ul style="list-style-type: none"> <li>• 对象名称</li> <li>• 所属集群名称</li> <li>• 标注</li> </ul>                      |
| 集群     | <ul style="list-style-type: none"> <li>• 对象名称</li> <li>• 标注</li> </ul>                                        |

当您选择注释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所选的对象类型而变化。该列表包括对象名称、所属集群名称、所属 SVM 名称以及您在 Unified Manager 中定义的注释。

- 运算符

运算符列表根据条件所选的操作数而变化。 Unified Manager 中支持的运算符是“Is”和“Contains”。

当您选择“Is”运算符时，将评估条件是否为操作数值与所选操作数提供的值完全匹配。

当您选择“包含”运算符时，将评估条件是否满足以下条件之一：

- 操作数值与所选操作数提供的值完全匹配
- 操作数值包含为所选操作数提供的值

- 值

值字段根据所选的操作数而变化。

## 带有条件的组规则示例

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”

此条件组选择名称中包含“vol”且托管在名为“data\_svm”的 SVM 上的所有卷。

## 条件组

条件组使用逻辑或执行，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被纳入某个组。所有条件组的存储对象被合并在一起。您可以使用条件组来增加组中存储对象的范围。

### 具有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”
  - 数据优先级的注释值为“critical” 条件组 2 选择名称中包含“vol”且数据优先级注释值为“critical”的所有卷。

当包含这两个条件组的组规则应用于存储对象时，以下存储对象将添加到选定的组中：

- 名称中包含“vol”且托管在名为“data\_svm”的 SVM 上的所有卷。
- 所有名称中包含“vol”且数据优先级注释值为“critical”的卷。

### 组操作如何作用于存储对象

组操作是对组内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。

群组支持独特的群组行动类型。一个组只能具有一种卷健康阈值组操作类型。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该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有关对存储对象应用哪些组操作的信息。

### 独特的群体行动示例

考虑属于组 G1 和 G2 的卷 A，并且为这些组配置了以下卷健康阈值组操作：

- ‘Change\_capacity\_threshold’等级为 1 的组操作，用于配置卷的容量
- ‘Change\_snapshot\_copies’级别为 2 的组操作，用于配置卷的 Snapshot 副本

这 ‘Change\_capacity\_threshold’集体行动总是优先于 ‘Change\_snapshot\_copies’组操作并应用于卷 A。当 Unified Manager 完成一个监控周期后，将根据 ‘Change\_capacity\_threshold’集体行动。您不能为 G1 或 G2 组配置其他容量阈值类型的组操作。

## 添加群组

您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。

您可以定义组规则来添加或删除组成员以及修改组的组操作。

#### 步骤

1. 在左侧导航窗格中，单击“存储管理”>“组”。
2. 在“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“添加”。

#### 编辑群组

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。

当您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。

#### 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“保存”。

#### 删除群组

当不再需要某个组时，您可以从 Unified Manager 中删除该组。

#### 开始之前

- 任何存储对象（集群、SVM 或卷）都不能与要删除的组关联的任何组规则关联。
- 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。

删除组并不会删除与该组关联的组操作。但是，删除组后，这些组操作将取消映射。

#### 添加群组规则

您可以为组创建组规则，以便将存储对象（例如卷、集群或存储虚拟机 (SVM)）动态添加到该组。您必须配置至少一个包含至少一个条件的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。

一旦创建组规则，就会添加当前监控的存储对象。仅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的类型。
- 5. 在\*组\*字段中，选择要为其创建组规则的组。
- 6. 在“条件”部分中，执行以下步骤来创建条件、条件组或两者：

| 創造.... | 操作                                                                                                                                                                                                                      |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 一个条件   | <ul style="list-style-type: none"><li>a. 从操作数列表选择一个操作数。</li><li>b. 选择 <b>Contains</b> 或 <b>Is</b> 作为运算符。</li><li>c. 输入一个值，或从可用列表选择一个值。</li></ul>                                                                        |
| 条件组    | <ul style="list-style-type: none"><li>a. 单击“添加条件组”</li><li>b. 从操作数列表选择一个操作数。</li><li>c. 选择 <b>Contains</b> 或 <b>Is</b> 作为运算符。</li><li>d. 输入一个值，或从可用列表选择一个值。</li><li>e. 如果需要，单击“添加条件”以创建更多条件，并对每个条件重复步骤 a 到 d。</li></ul> |

- 7. 单击“添加”。

创建组规则的示例

在“添加组规则”对话框中，执行以下步骤创建组规则，包括配置条件和添加条件组：

步骤

- 1. 指定组规则的名称。
- 2. 选择对象类型作为存储虚拟机 (SVM)。
- 3. 从组列表选择一个组。
- 4. 在条件部分中，选择\*对象名称\*作为操作数。
- 5. 选择 **Contains** 作为运算符。
- 6. 输入值 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 **Contains** 作为运算符。
10. 输入值 `vol`。
11. 单击\*添加条件\*。
12. 重复步骤 8 到 10，步骤 8 中选择 **data-priority** 作为操作数，步骤 9 中选择 **Is** 作为运算符，步骤 10 中选择 **critical** 作为值。
13. 单击“添加”为组规则创建条件。

### 编辑群组规则

您可以编辑组规则来修改条件组和条件组内的条件，以便向特定组添加或从特定组中删除存储对象。

#### 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、关联组名称、条件组和条件。



您不能更改组规则的目标对象类型。

4. 单击“保存”。

### 删除群组规则

当不再需要组规则时，您可以从Active IQ Unified Manager中删除该组规则。

#### 开始之前

您必须具有应用程序管理员或存储管理员角色。

当删除组规则时，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。

### 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您的时间，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\*Group\*菜单中，选择您想要配置操作的组。
5. 从\*操作类型\*菜单中，选择一种操作类型。

对话框展开，使您能够使用所需参数配置所选的操作类型。

6. 输入所需参数的适当值来配置组操作。
7. 单击“添加”。

#### 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、描述、关联组名称和操作类型的参数。

#### 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“群组操作”选项卡中，选择要编辑的群组操作，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、关联组名称和操作类型的参数。
4. 单击“保存”。

#### 为组配置卷健康阈值

您可以为容量、Snapshot 副本、qtree 配额、增长和 inode 配置组级卷健康阈值。

#### 开始之前

您必须具有应用程序管理员或存储管理员角色。

卷健康阈值类型的组操作仅适用于组的卷。

#### 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，选择要配置组操作的组。
5. 选择\*操作类型\*作为卷健康阈值。

6. 选择要设置阈值的类别。
7. 输入健康阈值所需的值。
8. 单击“添加”。

## 删除组操作

当不再需要组操作时，您可以从 Unified Manager 中删除该组操作。

### 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。在存储对象上设置的任何对象级健康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“群组操作”选项卡中，选择要删除的群组操作，然后单击“删除”。
3. 在“警告”对话框中，单击“是”确认删除。

## 重新排序组操作

您可以更改应用于组中存储对象的组操作的顺序。组操作根据存储对象的等级按顺序应用于存储对象。最低等级分配给您最后配置的组操作。您可以根据需要更改团体行动的等级。

### 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，然后执行多次拖放操作来更改组操作的排名。但是，您必须保存更改，以便重新排序能够反映在组操作网格中。

### 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“保存”。

## 使用注释确定存储对象事件的优先级

您可以创建注释规则并将其应用于存储对象，以便您可以根据所应用的注释类型及其优先级来识别和过滤这些对象。

### 了解有关注释的更多信息

了解有关注释的概念有助于您管理与环境中的存储对象相关的事件。



什么是注释

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动态地与存储对象关联。当您将存储对象与预定义注释关联时，您可以过滤和查看与它们相关的事件。您可以将注释应用于集群、卷和存储虚拟机 (SVM)。

每个注释名称可以有多个值；每个名称-值对都可以通过规则与一个存储对象相关联。

例如，您可以创建一个名为“data-center”的注释，其值为“Boston”和“Canada”。然后，您可以将注释“data-center”和值“Boston”应用于卷 v1。当针对标有“data-center”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。

Unified Manager 中的注释规则如何工作

注释规则是您定义的用于注释存储对象（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注释规则。

- 您必须将注释规则与注释关联起来。
- 您必须为注释规则关联一个对象类型；一个注释规则只能关联一种对象类型。
- 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从存储对象中添加或删除注释。
- 一个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。针对特定注释的注释规则还可以使用规则条件中的不同注释来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。您可以在注释的注释规则中应用所有定义的条件组，以便注释存储对象。

条件组内的条件使用逻辑“与”来执行。条件组中的所有条件必须满足。当您创建或修改注释规则时，会创建一个条件，该条件仅应用、选择和注释那些满足条件组中所有条件的存储对象。当您想要缩小要注释的存储对象的范围时，您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来创建具有存储对象的条件。

| 存储对象类型 | 适用操作数                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------|
| 卷      | <ul style="list-style-type: none"><li>• 对象名称</li><li>• 所属集群名称</li><li>• 所属 SVM 名称</li><li>• 标注</li></ul> |
| SVM    | <ul style="list-style-type: none"><li>• 对象名称</li><li>• 所属集群名称</li><li>• 标注</li></ul>                     |

| 存储对象类型 | 适用操作数                                                              |
|--------|--------------------------------------------------------------------|
| 集群     | <ul style="list-style-type: none"> <li>对象名称</li> <li>标注</li> </ul> |

当您选择注释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，将评估条件是否为操作数值与所选操作数提供的值完全匹配。当您选择“包含”运算符时，将评估条件是否满足以下条件之一：

- 操作数值与所选操作数的值完全匹配。
- 操作数值包含为所选操作数提供的值。

### 带条件的注释规则示例

考虑具有一个条件组的注释规则，该规则针对具有以下两个条件的卷：

- 名称包含“vol”
- SVM 名称为“data\_svm”

此注释规则使用选定的注释和注释类型对名称中包含“vol”且托管在名为“data\_svm”的 SVM 上的所有卷进行注释。

### 条件组

条件组使用逻辑或执行，然后应用于存储对象。存储对象必须满足要注释的其中一个条件组的要求。对满足所有条件组条件的存储对象进行注释。您可以使用条件组来增加要注释的存储对象的范围。

### 带有条件组的注释规则示例

考虑一个具有两个卷条件组的注释规则；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”
  - 数据优先级的注释值为“critical” 此条件组将名称中包含“vol”且数据优先级注释值为“critical”的所有卷进行注释。

当包含这两个条件组的注释规则应用于存储对象时，则会注释以下存储对象：

- 名称中包含“vol”且托管在 SVM 上且名称为“data\_svm”的所有卷。
- 所有名称中包含“vol”且数据优先级注释值为“critical”的卷。

数据优先级 是一个预定义注释，其值为任务关键、高和低。这些值使您能够根据存储对象所包含的数据的优先级对其进行注释。您不能编辑或删除预定义的注释值。

- 数据优先级：任务关键

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以被视为任务关键型。

- 数据优先级：高

此注释适用于包含高优先级数据的存储对象。例如，承载业务应用程序的对象可以被视为高优先级。

- 数据优先级：低

此注释适用于包含低优先级数据的存储对象。例如，位于二级存储上的对象（如备份和镜像目标）可能优先级较低。

## 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\*部分中，单击\*添加\*以向注释添加值。
5. 单击“保存”。

### 向注释添加值

您可以向注释添加值，然后将存储对象与特定的注释名称-值对关联。向注释添加值可以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。

您不能向预定义注释添加值。

### 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，选择要添加值的注释，然后单击“值”部分中的“添加”。

3. 在“添加注释值”对话框中，指定注释的值。

您指定的值对于选定的注释必须是唯一的。

4. 单击“添加”。

## 删除注释

当不再需要自定义注释及其值时，您可以删除它们。

### 开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 注释值不得在其他注释或组规则中使用。

### 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。

显示所选注释的详细信息。

3. 单击“操作”>“删除”以删除选定的注释及其值。
4. 在警告对话框中，单击“是”确认删除。

## 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) 动态关联的注释列表。您还可以查看注释的详细信息，例如描述、创建者、创建日期、值、规则以及与注释相关的对象。

### 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。

## 从注释中删除值

当与自定义注释关联的值不再适用于该注释时，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。
- 注释值不得与任何注释规则或组规则相关联。

您不能从预定义注释中删除值。

### 步骤

1. 在左侧导航窗格中，单击“存储管理”>“注释”。
2. 在“注释”选项卡的注释列表中，选择要从中删除值的注释。
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”。

该值已被删除，并且不再显示在所选注释的值列表中。

创建注释规则

您可以创建注释规则，Unified Manager 可以使用该规则动态注释存储对象，例如卷、集群或存储虚拟机 (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。

一旦创建注释规则，就会对当前监控的存储对象进行注释。仅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，指定注释规则的名称。
- 4. 在\*目标对象类型\*字段中，选择要注释的存储对象的类型。
- 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，执行适当的操作来创建条件、条件组或两者：

| 创建... | 操作                                                                                                                                                                                                                         |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 一个条件  | <ul style="list-style-type: none"><li>a. 从操作数列表中选择一个操作数。</li><li>b. 选择 <b>Contains</b> 或 <b>Is</b> 作为运算符。</li><li>c. 输入一个值，或从可用列表中选择一个值。</li></ul>                                                                         |
| 条件组   | <ul style="list-style-type: none"><li>a. 单击“添加条件组”。</li><li>b. 从操作数列表中选择一个操作数。</li><li>c. 选择 <b>Contains</b> 或 <b>Is</b> 作为运算符。</li><li>d. 输入一个值，或从可用列表中选择一个值。</li><li>e. 如果需要，单击“添加条件”以创建更多条件，并对每个条件重复步骤 a 到 d。</li></ul> |

- 7. 单击“添加”。

创建注释规则的示例

在“添加注释规则”对话框中执行以下步骤来创建注释规则，包括配置条件和添加条件组：

步骤

- 1. 指定注释规则的名称。

2. 选择目标对象类型为存储虚拟机 (SVM)。
3. 从注释列表选择一个注释，并指定一个值。
4. 在条件部分中，选择\*对象名称\*作为操作数。
5. 选择 **Contains** 作为运算符。
6. 输入值 `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 **Contains** 作为运算符。
10. 输入值 `vol`。
11. 单击\*添加条件\*。
12. 重复步骤 8 到 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“添加”。

### 手动向各个存储对象添加注释

您可以手动注释选定的卷、集群和 SVM，而无需使用注释规则。您可以注释单个存储对象或多个存储对象，并为注释指定所需的名称-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：

| 要添加注释... | 操作                                                                                             |
|----------|------------------------------------------------------------------------------------------------|
| 集群       | <ol style="list-style-type: none"> <li>a. 单击“存储”&gt;“集群”。</li> <li>b. 选择一个或多个集群。</li> </ol>    |
| 卷        | <ol style="list-style-type: none"> <li>a. 单击“存储”&gt;“卷”。</li> <li>b. 选择一个或多个卷。</li> </ol>      |
| SVM      | <ol style="list-style-type: none"> <li>a. 单击“存储”&gt;“SVM”。</li> <li>b. 选择一个或多个 SVM。</li> </ol> |

2. 单击“注释”并选择一个名称-值对。
3. 单击“应用”。

## 编辑注释规则

您可以编辑注释规则来修改条件组和条件组内的条件，从而向存储对象添加注释或从存储对象中删除注释。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

当您编辑相关的注释规则时，注释将与存储对象解除关联。

### 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“保存”。

## 配置注释规则的条件

您可以配置一个或多个条件来创建 Unified Manager 应用于存储对象的注释规则。满足注释规则的存储对象将被注释为规则中指定的值。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

### 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种对象类型，然后从列表中选择注释名称和值。
5. 在对话框的“条件”部分中，从列表选择一个操作数和一个运算符，然后输入条件值，或者单击“添加条件”来创建新条件。
6. 单击“保存并添加”。

## 配置注释规则条件的示例

考虑对象类型 SVM 的条件，其中对象名称包含“svm\_data”。

在“添加注释规则”对话框中执行以下步骤来配置条件：

### 步骤

1. 输入注释规则的名称。
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 **Contains** 作为运算符。
6. 输入值 `svm_data`。
7. 单击“添加”。

## 删除注释规则

当不再需要注释规则时，您可以从Active IQ Unified Manager中删除这些规则。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

当您删除注释规则时，注释将取消关联并从存储对象中删除。

### 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。

## 重新排序注释规则

您可以更改 Unified Manager 将注释规则应用到存储对象的顺序。注释规则根据存储对象的等级依次应用于存储对象。配置注释规则时，排序最小。但是您可以根据需要更改注释规则的等级。

### 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并执行多次拖放操作来更改注释规则的等级。但是，您必须保存更改，以便重新排序显示在“注释规则”选项卡中。

### 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\*重新排序注释规则\*对话框中，拖放单行或多行以重新排列注释规则的顺序。
4. 单击“保存”。

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

当您遇到的问题需要比AutoSupport消息提供的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 和维护控制台将支持包发送给技术支持。



Unified Manager 一次最多可存储两个完整支持包和三个轻量级支持包。

## 相关信息

### "Unified Manager 用户角色和功能"

将**AutoSupport**消息和支持包发送给技术支持

AutoSupport页面使您能够向技术支持团队发送预定义和按需的AutoSupport消息，以确保您的环境正常运行，并帮助您维护环境的完整性。AutoSupport默认处于启用状态，您不应禁用它，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，甚至生成并发送支持包给技术支持团队。



具有存储管理员角色的用户可以生成并发送按需AutoSupport消息和支持包给技术支持。但是，只有管理员或维护用户可以启用或禁用定期AutoSupport并配置 HTTP 设置，如设置 HTTP 代理服务器部分中所述。在需要使用 HTTP 代理服务器的环境中，应先完成配置，然后存储管理员才能向技术支持发送按需AutoSupport消息和支持包。

## 发送按需**AutoSupport**消息

您可以生成并发送按需消息给技术支持人员，或发送给指定的电子邮件收件人，或同时发送给两者。

### 步骤

1. 导航到 常规 > **AutoSupport**，然后执行以下操作之一或全部两个：
2. 如果您想将AutoSupport消息发送给技术支持，请选中 发送至技术支持 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“保存”。
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。如果禁用，管理员或维护用户可以启用该设置。

### 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，请按照设置 HTTP 代理服务器部分中的说明定义 HTTP 代理服务器的名称、端口和身份验证信息。
4. 单击“保存”。

## 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。

较旧的支持包已从系统中删除。

由于某些类型的支持数据可能会使用大量集群资源或需要很长时间才能完成，因此当您选择完整支持包时，您可以包含或排除特定数据类型以减小支持包的大小。您还可以选择创建一个轻量级支持包，其中仅包含 30 天的日志和配置数据库记录 - 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. 在按需支持包部分，单击\*生成并发送支持包\*。
3. 要向技术支持发送轻量支持包，请在“生成并发送支持包”弹出窗口中选中“生成轻量支持包”复选框。
4. 或者，要发送完整的支持包，请选中“生成完整的支持包”复选框。选择要在支持包中包含或排除的特定数据类型。



即使您未选择任何数据类型，支持包仍会与其他 Unified Manager 数据一起生成。

5. 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。如果您未选中此复选框，则会在 Unified Manager 服务器本地生成并存储捆绑包。生成的支持包可供以后在 VMware 系统的 /support 目录中使用，`/opt/netapp/data/support/` 在 Linux 系统上，`ProgramData\NetApp\OnCommandAppData\ocum\support` 在 Windows 系统上。
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互联网访问，以便将 AutoSupport 内容发送给支持人员。此部分仅供管理员和维护用户使用。

##### • 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。

#### 访问维护控制台

如果 Unified Manager 用户界面未运行，或者您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，维护控制台将注销您。



在 VMware 上安装时，如果您已经通过 VMware 控制台以维护用户身份登录，则无法同时使用安全外壳登录。

步骤

1. 按照以下步骤访问维护控制台：

| 在此操作系统上... | 请按照以下步骤操作...                                                                                                                                                |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VMware     | <div>a. 使用安全外壳连接到 Unified Manager 虚拟设备的 IP 地址或完全限定域名。</div> <div>b. 使用您的维护用户名和密码登录维护控制台。</div>                                                              |
| Linux      | <div>a. 使用安全外壳连接到 Unified Manager 系统的 IP 地址或完全限定域名。</div> <div>b. 使用维护用户 (umadmin) 名称和密码登录到此系统。</div> <div>c. 输入命令 `maintenance_console` 然后按 Enter 键。</div> |
| Windows    | <div>a. 使用管理员凭据登录 Unified Manager 系统。</div> <div>b. 以 Windows 管理员身份启动 PowerShell。</div> <div>c. 输入命令 `maintenance_console` 然后按 Enter 键。</div>               |

显示 Unified Manager 维护控制台菜单。

生成并上传支持包

您可以生成包含诊断信息的支持包，以便将其发送给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将支持包上传到 NetApp。

开始之前

您必须以维护用户身份访问维护控制台。

由于某些类型的支持数据可能会使用大量集群资源或需要很长时间才能完成，因此当您选择完整支持包时，您可以指定要包含或排除的数据类型以减少支持包的大小。您还可以选择创建一个轻量级支持包，其中仅包含 30 天的日志和配置数据库记录 - 它不包括性能数据、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包。较旧的支持包已从系统中删除。

步骤

1. 在维护控制台\*主菜单\*中，选择\*支持/诊断\*。

2. 根据您希望在支持包中拥有的详细程度，选择\*生成轻量支持包\*或\*生成支持包\*。
3. 如果选择完整支持包，请选择或取消选择以下数据类型以在支持包中包含或排除：

- 数据库转储

MySQL 服务器数据库的转储。

- 堆转储

主 Unified Manager 服务器进程状态的快照。此选项默认处于禁用状态，仅应在客户支持要求时选择。

- 采集记录

Unified Manager 与受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，则支持包仍会与其他 Unified Manager 数据一起生成。

4. 类型 g，然后按 Enter 键生成支持包。

由于生成支持包是一项占用大量内存的操作，因此系统会提示您确认是否确定要在此时生成支持包。

5. 类型 y，然后按 Enter 键生成支持包。

如果您现在不想生成支持包，请键入 n，然后按 Enter。

6. 如果您在完整支持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。包含性能统计信息会占用大量时间和空间，因此您也可以转储数据库而不包含性能统计信息：

- a. 以 YYYYMMDD 格式输入开始日期。

例如，输入 `20210101` 截至 2021 年 1 月 1 日。进入 `n` 如果您不想包含性能统计数据。

- b. 输入要包含的统计数据的天数，从指定开始日期的凌晨 12 点开始。

您可以输入 1 到 10 之间的数字。

如果包括性能统计数据，系统将显示将收集性能统计数据的时间段。

7. 创建支持包后，系统会提示您是否要将其上传到 NetApp。类型 y，然后按 Enter。

系统会提示您输入支持案例编号。

8. 如果您已经有案件编号，请输入该编号并按 Enter。否则只需按 Enter 键。

支持包已上传至 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您无法上传支持包，那么您可以检索它并手动发送。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，您可以使用远程桌面 (RDP) 来检索支持包。

生成的支持包位于 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。

相关信息

["Unified Manager 用户角色和功能"](#)

使用 **Windows** 客户端检索支持包

如果您是 Windows 用户，您可以下载并安装一个工具来从 Unified Manager 服务器检索支持包。您可以将支持包发送给技术支持，以便对问题进行更详细的诊断。Filezilla 或 WinSCP 是您可以使用的工具的示例。

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. 下载并安装工具来检索支持包。
- 2. 打开工具。
- 3. 通过 SFTP 连接到您的 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. 选择要复制的支持包，然后使用该工具将文件从 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 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具有可用的支持包名称。

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. 使用以下命令检索支持包并将其复制到本地目录：

| 条件  | 命令                                                                                                                                   |
|-----|--------------------------------------------------------------------------------------------------------------------------------------|
| SCP | <code>scp &lt;maintenance-user&gt;@&lt;vApp-name-or-ip&gt;:/support/support_bundle_file_name.7z &lt;destination-directory&gt;</code> |

| 条件   | 命令                                                                                                     |
|------|--------------------------------------------------------------------------------------------------------|
| SFTP | sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory> |

当您使用维护控制台生成支持包时，会向您提供其名称。

#### 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
```

#### 向技术支持发送支持包

当问题需要比AutoSupport消息提供的更详细的诊断和故障排除信息时，您可以向技术支持发送支持包。

#### 开始之前

您必须具有支持包的访问权限才能将其发送给技术支持。

您必须拥有通过技术支持网站生成的案例编号。

#### 步骤

1. 登录NetApp支持站点。
2. 上传文件。

["如何将文件上传到NetApp"](#)

## 与多个工作流程相关的任务和信息

一些可以帮助您理解和完成工作流程的任务和参考文本对于 Unified Manager 中的许多工作流程都是通用的，包括添加和查看有关事件的注释、分配事件、确认和解决事件以及有关卷、存储虚拟机 (SVM)、聚合等的详细信息。

### 集群组件及其争用的原因

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的性能会变慢，并且其对客户端请求的响应时间（延迟）会增加，从而触发 Unified Manager 中的事件。

存在争用的组件无法达到最佳性能。它的性能已经下降，并且其他集群组件和工作负载（称为“受害者”）的性能可能会增加延迟。要使组件摆脱争用，必须减少其工作负载或提高其处理更多工作的能力，以便性能恢复到正常水平。由于 Unified Manager 以五分钟为间隔收集和分析工作负载性能，因此它仅检测集群组件何时持续过度使用。未检测到在五分钟内仅持续很短时间的过度使用瞬态峰值。

例如，存储聚合可能处于争用状态，因为其上的一个或多个工作负载正在竞争满足其 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，以减少当前聚合上的总体工作负载需求。对于 QoS 策略组，您可以调整吞吐量限制，或将工作负载移至其他策略组，这样工作负载就不会再受到限制。

Unified Manager 监控以下集群组件，并在它们发生争用时提醒您：

- 网络

表示集群上外部网络协议的 I/O 请求的等待时间。等待时间是指集群响应 I/O 请求之前等待“传输就绪”事务完成所花费的时间。如果网络组件处于争用状态，则意味着协议层的高等待时间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的 I/O 处理的软件组件。负责网络处理的节点可能会在检测到事件后发生更改。如果网络处理组件存在争用，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。

在主动-主动配置中使用全 SAN 阵列群集时，将显示两个节点的网络处理延迟值，以便您可以验证节点是否平等地共享负载。

- QoS 限制最大值

表示分配给工作负载的存储服务质量 (QoS) 策略组的最大吞吐量（峰值）设置。如果策略组组件存在争用，则意味着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 限制最小值

表示由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。如果某些工作负载上设置的 QoS 最小值使用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多延迟。

- 集群互连

表示集群节点物理连接的电缆和适配器。如果集群互连组件处于争用状态，则意味着集群互连处 I/O 请求的等待时间过长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与包含工作负载的存储聚合之间的 I/O 处理的软件组件。负责数据处理的节点可能会在检测到事件后发生更改。如果数据处理组件存在争用，则意味着数据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。

- **音量激活**

表示跟踪所有活动卷使用情况的进程。在有超过 1000 个卷处于活动状态的大型环境中，此过程会跟踪有多少个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，一些非关键卷将会出现此处标识的延迟。

- **\* 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的工作负载的高写入吞吐量或链路健康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，则不会显示此图标。

- **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。聚合由所有 HDD 组成，或由 HDD 和 SSD 的混合（Flash Pool 聚合）组成，或由 HDD 和云层的混合（FabricPool聚合）组成。“SSD 聚合”由所有 SSD（全闪存聚合）或 SSD 和云层（FabricPool聚合）的混合组成。

- **云延迟**

表示集群中涉及集群和存储用户数据的云层之间的 I/O 处理的软件组件。如果云延迟组件存在争用，则意味着托管在云层上的卷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，则意味着SnapMirror同步操作的活动正在影响一个或多个工作负载的延迟。

## 音量/健康详情页面

您可以使用卷/健康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。同时，还可以查看有关此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。

- 行动

- 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，该对话框使您能够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 副本中的数据的所有数据都将被删除。

- 还原

用于将数据从一个卷还原到另一个卷。有关信息，请参阅["使用卷/健康详情页面恢复数据"](#)。



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

“容量”选项卡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。该值可以是“已启用”、“已禁用”或“不适用”。对于旧版本 ONTAP 上的卷或不支持逻辑空间报告的卷，将显示“不适用”。

#### ◦ 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。

### • 自动生长

显示卷在空间不足的情况下是否会自动增长。

### • 舱位保证

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 卷根据其大小预留空间。如果FlexCache卷的大小为 100 MB 或更多，则最小空间保证默认为 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）。

- 快照保留

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）。

- 音量阈值

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。

- 其他详情

- 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 Snapshot 副本的数量显示为一个链接。单击该链接将打开“卷上的 Snapshot 副本”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。

- 音量移动

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。

另外，还显示对选定卷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

显示包含该卷的 SVM 的名称。

- 接合路径

显示路径的状态，可以是活动或非活动状态。还会显示 SVM 中卷的挂载路径。您可以点击“历史记录”链接查看连接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。您可以单击该链接查看有关属于 SVM 的卷上启用的导出策略、身份验证协议和访问的详细信息。

- 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

指定是否启用或禁用压缩。

- 重复数据删除

指定是否启用或禁用重复数据删除。

- 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，例如滞后信息、关系类型和关系拓扑。

- 概括

显示选定卷的保护关系（SnapMirror、SnapVault或存储 VM DR）属性。对于任何其他关系类型，仅显示“关系类型”属性。如果选择主卷，则仅显示托管和本地 Snapshot 副本策略。对于 SnapMirror 和 SnapVault 关系，显示的属性包含以下内容：

- 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、异步保险库、异步镜像保险库、StrictSync 和同步。

- 关系状态

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。

- 转移

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 表示默认的异步镜像保护策略，XDPDefault 表示默认的异步保险库策略，DPSyncDefault 表示默认的异步镜像保险库策略。StrictSync表示默认的同步严格保护策略，Sync表示默认的同步策略。您可以单击策略名称来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
- 没有保留设置的 Snapshot 副本在源是数据保护 (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

显示所选卷所使用的保护类型。例如，如果卷受一致性组和SnapMirror卷关系保护，则此字段同时显示SnapMirror和一致性组。该字段还提供一个链接，将您重定向到“关系”页面以查看统一关系状态。该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。

- 观点

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。

双粗线指定异步镜像关系，单粗线指定异步保险库关系，双单线指定异步镜像保险库关系，粗线和非粗线指

定同步关系。下表指示同步关系是 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。问号 (?) 位于卷的左上角，表示该卷丢失或尚未被发现。也可能指示缺少容量信息。将光标置于问号上方可显示其他信息，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

显示卷所用的总容量。将光标置于拓扑中的卷上会在“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滞后持续时间和滞后状态。清除 **Lag** 复选框将隐藏拓扑中所有卷的所有滞后信息。当 **Lag** 复选框变暗时，所选卷的滞后信息将显示在拓扑下方的关系表中，以及所有相关卷的滞后信息。

- Snapshot

显示可用于卷的 Snapshot 副本数量。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 () 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 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。

- 上次成功传输

显示上次成功传输数据的数量、持续时间、时间和日期。当“上次成功传输”复选框变暗时，所选卷的上次成功传输信息将显示在拓扑下方的关系表中，以及所有相关卷的上次成功传输信息。

- 历史

以图形方式显示选定卷的传入 SnapMirror 和 SnapVault 保护关系的历史记录。有三种历史图表可用：传入关系滞后持续时间、传入关系转移持续时间和传入关系转移大小。仅在选择目标卷时才会显示历史记录信息。如果选择主卷，则图表为空，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表类型。也可以通过选择 1 周、1 个月或 1 年来查看特定时间段的详细信息。历史记录图可以帮助您了解趋势：例如在某天或某一周的同一段时间传输大量数据，或者总

是违反滞后警告或滞后错误阈值，则可以采取相应措施。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。

- 关系转移大小

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。

## 历史区

“历史记录”区域显示的几个图提供有关选定卷的容量和空间预留的信息。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。

当卷的数据或状态在一段时间内保持不变时，图表可能为空，并显示消息“未找到数据”。

您可以从历史记录窗格顶部的下拉列表中选择图表类型。也可以通过选择 1 周、1 个月或 1 年来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，如果卷使用情况持续突破“几乎满”阈值，您可以采取适当的措施。

历史记录图显示下列信息：

- 已使用的卷容量

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：

- 严重性

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。

## 相关注释窗格

通过“相关注释”窗格，您可以查看与所选卷相关的注释详细信息。详细信息包括标注名称和应用于卷的标注值。您还可以从“相关注释”窗格中删除手动注释。

## 相关设备窗格

通过“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：

- 存储虚拟机

显示包含选定卷的 SVM 的容量和运行状况。

- 总计的

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。

- 总量

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。

- Qtree

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。

- 中小企业股份

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。

- 家长卷

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

通过“相关组”窗格，您可以查看与所选卷关联的组的列表。

## 相关警报窗格

通过“相关警报”窗格，您可以查看为选定卷创建的警报列表。您也可以单击“添加警报”链接来添加警报，或者单击警报名称来编辑现有警报。

## 存储虚拟机/运行状况详细信息页面

您可以使用存储虚拟机/运行状况详细信息页面查看有关所选存储虚拟机的详细信息，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。您还可以查看有关存储虚拟机的相关对象和相关警报的信息。



您只能监控数据存储虚拟机。

#### 命令按钮

命令按钮使您能够对选定的存储虚拟机执行以下任务：

- 切换到性能视图

使您能够导航到存储虚拟机/性能详细信息页面。

- 行动

- 添加警报

使您能够向选定的存储虚拟机添加警报。

- 标注

使您能够注释选定的存储虚拟机。

- 查看存储虚拟机

使您能够导航到“运行状况：所有存储虚拟机”视图。

#### “健康”标签

“运行状况”选项卡显示有关各种对象（例如卷、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

以图形方式显示对象总数，其中包括具有可用性问题的对象以及没有任何可用性相关问题的对象。图形中的颜色表示问题的不同严重性级别。图表下方的信息提供了有关可用性问题的详细信息，这些问题可能影响或已经影响了存储虚拟机中数据的可用性。例如，显示有关已关闭的 NAS LIF 和 SAN LIF 以及已脱机的卷的信息。

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

以图形方式显示对象总数，其中包括存在容量问题的对象以及没有任何容量相关问题的对象。图形中的颜色表示问题的不同严重性级别。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容量的容量问题的详细信息。例如，有关可能会违反设定阈值的聚合的信息。

- 保护问题

通过以字段对话框的形式显示关系总数（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），快速概览存储虚拟机保护相关的健康状况。您还可以查看所选存储虚拟机的存储虚拟机 DR 关系的状态。存储 VM DR 关系事件显示在此处，单击事件将转到事件详细信息页面。当存在不受保护的卷时，单击链接将转

到“运行状况：所有卷”视图，您可以在其中查看存储虚拟机上不受保护的卷的筛选列表。图形中的颜色表示问题的不同严重性级别。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 副本预留空间接近全满的卷或有关 SnapMirror 关系滞后问题的信息。

## 容量选项卡

容量选项卡显示有关所选 SVM 的数据容量的详细信息。

对于具有 FlexVol volume 或 FlexGroup 卷的存储虚拟机，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

显示存储虚拟机的总容量。

- 已用

显示属于存储虚拟机的卷中数据所使用的空间。

- 保证可用

显示存储虚拟机中卷可用的保证数据空间。

- 无保证

显示为存储虚拟机中精简配置卷分配的数据剩余可用空间。

- 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。

如果卷状态是由某一事件引起的，可以查看有关该事件名称、事件触发时间和日期、负责处理该事件的管理员姓名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。

如果卷状态是由严重性相同的多个事件引起的，则会显示前三个事件，以及事件名称、事件触发时间和日期、负责处理事件的管理员姓名等信息。您可以单击事件名称来查看其中每个事件的更多详细信息，您还可以单击[“查看所有事件”](#)链接来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，例如其集群、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

显示存储虚拟机所属的集群名称。

- 允许的卷类型

显示可以在存储虚拟机中创建的卷的类型。此类型可以是“FlexVol”或“FlexVol/FlexGroup”。

- 根卷

显示存储虚拟机的根卷的名称。

- 允许的协议

显示可在存储虚拟机上配置的协议类型。此外，指示协议是否启动（），向下（），或者未配置（）。

- 数据网络接口

- NAS

显示与存储虚拟机关联的 NAS 接口的数量。此外，指示接口是否已启动（）或向下（）。

- SAN

显示与存储虚拟机关联的 SAN 接口的数量。此外，指示接口是否已启动（）或向下（）。

- FC-NVMe

显示与存储虚拟机关联的 FC-NVMe 接口的数量。此外，指示接口是否已启动 (●) 或向下 (●)。

- 管理网络接口

- 可用性

显示与存储虚拟机关联的管理接口的数量。此外，指示管理接口是否已启动 (●) 或向下 (●)。

- 政策

- Snapshot

显示在存储虚拟机上创建的快照策略的名称。

- 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

- 存储虚拟机灾难恢复

显示所选存储虚拟机是否受保护、目标或不受保护，以及受保护存储虚拟机的目标的名称。如果选定的存储虚拟机是目标，则会显示源存储虚拟机的详细信息。在扇出的情况下，该字段显示受保护的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过滤的存储虚拟机关系网络。

- 受保护的卷

显示选定存储虚拟机上受保护卷的数量（占总卷的数量）。如果您正在查看目标存储虚拟机，则数字链接代表所选存储虚拟机的目标卷。

- 未受保护的卷

显示所选存储虚拟机上未受保护的卷的数量。

- 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“Domain Name System (DNS)”或“Network Information Service (NIS)”。

- 状态

显示服务的状态，可以是“启动” (●)，向下 (●) 或未配置 (●)。

- 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虚拟机上创建的数据网络接口 (LIF) 的详细信息：

- 网络接口

显示在选定存储虚拟机上创建的接口的名称。

- 运营状态

显示接口的运行状态，可以是 Up (↑)，向下 (↓) 或未知 (?)。接口的运行状态由其物理端口的状态决定。

- 行政地位

显示接口的管理状态，可以是 Up (↑)，向下 (↓) 或未知 (?)。接口的管理状态由存储管理员控制，以便更改配置或进行维护。管理状态可以与运行状态不同。但是，如果接口的管理状态为“已关闭”，则运行状态默认为“已关闭”。

- 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”。

- 母港

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。

- 端口设置

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。

#### qtree 选项卡

Qtrees 选项卡显示有关 qtree 及其配额的信息。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”按钮创建一个逗号分隔值 (.csv) 文件，其中包含所有受监控 qtree 的详细信息。导出到 CSV 文件时，您可以选择为当前存储虚拟机、当前集群中的所有存储虚拟机或数据中心中所有集群的所有存储虚拟机创建 qtree 报告。导出的 CSV 文件中会显示一些额外的 qtree 字段。

- 地位

显示 qtree 的当前状态。状态可以是“严重” (❌)，错误 (⚠️)，警告 (⚠️) 或正常 (✅)。

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 状态是由某一事件引起的，可以查看有关该事件名称、事件触发时间和日期、负责处理该事件的管理员姓名以及事件原因等信息。您可以使用\*查看详细信息\*来查看有关该事件的更多信息。

如果 qtree 状态是由严重性相同的多个事件引起的，则会显示前三个事件，以及事件名称、事件触发时间和日期、负责处理事件的管理员姓名等信息。您可以单击事件名称来查看其中每个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。

- 簇

显示 qtree 所在集群的名称。仅显示在导出的 CSV 文件中。

- 存储虚拟机

显示包含 qtree 的存储虚拟机 (SVM) 名称。仅显示在导出的 CSV 文件中。

- 体积

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。

- 配额设置

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。

- 磁盘使用率%

显示已用磁盘空间的百分比。如果设置了磁盘硬限制，则此值以磁盘硬限制为基础。如果设置了配额，而无磁盘硬限制，则此值以卷数据空间为基础。如果未设置配额，或者 qtree 所属卷上的配额已关闭，则网格页面中将显示“不适用”，并且 CSV 导出数据中的字段为空白。

- 磁盘硬限制

显示为 qtree 分配的最大磁盘空间量。当达到此限制并且不允许进一步写入磁盘时，Unified Manager 会生成严重事件。在以下情况下，该值显示为“Unlimited”：如果设置的配额没有磁盘硬限制、未设置配额或 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，该值显示为“Unlimited”：如果设置的配额没有磁盘软限制、未设置配额或 qtree 所属卷上的配额为关闭状态。默认情况下，此列处于隐藏状态。

- 磁盘阈值

显示对磁盘空间设置的阈值。在以下情况下，该值显示为“Unlimited”：如果设置的配额没有磁盘阈值限制、未设置配额或 qtree 所属卷上的配额已关闭。默认情况下，此列处于隐藏状态。

- 使用的文件 %

显示 qtree 中已用文件的百分比。如果设置了文件硬限制，则此值以文件硬限制为基础。如果设置了配额且无文件硬限制，则不显示任何值。如果未设置配额，或者 qtree 所属卷上的配额已关闭，则网格页面中将显示“不适用”，并且 CSV 导出数据中的字段为空白。

- 文件硬限制

显示 qtree 所允许的文件数的硬限制。在以下情况下，该值显示为“Unlimited”：如果设置的配额没有文件硬限制、未设置配额或 qtree 所属卷上的配额已关闭。

- 文件软限制

显示 qtree 所允许的文件数的软限制。在以下情况下，该值显示为“Unlimited”：如果设置了配额而没有文件软限制，如果未设置配额，或者如果 qtree 所属卷上的配额已关闭。默认情况下，此列处于隐藏状态。

#### 用户和组配额选项卡

显示有关所选存储虚拟机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、已用磁盘空间量和文件数量以及磁盘阈值等信息。此外，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。您可以修改该电子邮件地址。如果编辑电子邮件地址字段为空，则使用默认规则为选定的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，为存储虚拟机上配置的用户或用户组配额生成电子邮件地址。当违反配额时，系统会向指定的电子邮件地址发送通知。

- 地位

显示配额的当前状态。状态可以是“严重”（），警告（）或正常（）。

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。

如果配额状态是由某一事件引起的，可以查看有关该事件名称、事件触发时间和日期、负责处理该事件的管理员姓名以及事件原因等信息。您可以使用\*查看详细信息\*来查看有关该事件的更多信息。

如果配额状态是由严重性相同的多个事件引起的，则会显示前三个事件，以及事件名称、事件触发时间和日期、负责处理事件的管理员姓名等信息。您可以单击事件名称来查看其中每个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，该值显示为“未知”。

- 类型

指定配额针对用户还是用户组。

- 卷或 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。

- 磁盘使用率%

显示已用磁盘空间的百分比。如果配额设置时没有磁盘硬限制，则该值显示为“不适用”。

- 磁盘硬限制

显示为配额分配的最大磁盘空间量。当达到此限制并且不允许进一步写入磁盘时，Unified Manager 会生成

严重事件。如果配额设置没有磁盘硬限制，则该值显示为“无限制”。

- 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。如果配额设置时没有磁盘软限制，则该值显示为“无限制”。默认情况下，此列处于隐藏状态。

- 磁盘阈值

显示对磁盘空间设置的阈值。如果配额设置没有磁盘阈值限制，则该值显示为“无限制”。默认情况下，此列处于隐藏状态。

- 使用的文件 %

显示 qtree 中已用文件的百分比。如果设置的配额没有文件硬限制，则该值显示为“不适用”。

- 文件硬限制

显示配额所允许的文件数的硬限制。如果配额设置没有文件硬限制，则该值显示为“无限制”。

- 文件软限制

显示配额所允许的文件数的软限制。如果配额设置时没有文件软限制，则该值显示为“无限制”。默认情况下，此列处于隐藏状态。

- 电子邮件

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。在下列条件下，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。

- 地位

显示 NFS 共享的当前状态。状态可以是错误 (❗) 或正常 (✅)。

- 连接路径

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。

- 连接路径已启用

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。

- 卷或 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。

- 音量状态

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。

- 出口政策

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信息，例如身份验证协议和访问权限。



## SMB 共享选项卡

显示有关所选存储虚拟机上的 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。



文件夹中的共享不会显示在 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。

您可以查看存储虚拟机的用户映射的详细信息。

- 显示 **ACL** 命令按钮

启动共享的访问控制对话框。

您可以查看选定共享的用户和权限详细信息。

- 地位

显示共享的当前状态。状态可以是正常 (✓) 或错误 (!)。

- 共享名称

显示 SMB 共享的名称。

- 小路

显示创建共享的接合路径。

- 连接路径已启用

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“详细信息”页面中查看包含对象的详细信息。如果父对象是 qtree，将为 qtree 和卷显示链接。

- 音量状态

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。

- 出口政策

显示适用于共享的导出策略的名称。如果没有为存储虚拟机指定导出策略，则该值显示为未启用。

您可以单击链接查看有关与导出策略关联的规则的信息，例如访问协议和权限。如果所选存储虚拟机的导出策略被禁用，则该链接也会被禁用。

- **NFS 等效**

指定共享是否存在 NFS 等效对象。

## **SAN 选项卡**

显示有关所选存储虚拟机的 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，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。您可以查看有关 LUN 名称、LUN 状况（联机或脱机）、LUN 所在文件系统（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。

还可以查看有关是否在 LUN 上启用了精简配置以及 LUN 是否映射到启动程序组的信息。如果映射到启动器

，则可以查看映射到选定 LUN 的启动器组和启动器。

- 发起者组选项卡

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。

- 普通的

启动程序组连接到多个访问路径。

- 单路径

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。

- 发起者标签

显示选定存储虚拟机的启动器的名称和类型以及映射到该启动器的启动器组总数。

```
initiator groups that are mapped to the selected initiator group.
```

#### 相关注释窗格

通过“相关注释”窗格，您可以查看与所选存储虚拟机相关的注释详细信息。详细信息包括注释名称和应用用于存储虚拟机的注释值。您还可以从“相关注释”窗格中删除手动注释。

#### 相关设备窗格

通过“相关设备”窗格，您可以查看与存储虚拟机相关的集群、聚合和卷：

- 簇

显示存储虚拟机所属集群的健康状态。

- 聚合

显示属于所选存储虚拟机的聚合数量。此外，系统还将基于最高严重性级别显示聚合的运行状况。例如，如果存储虚拟机包含十个聚合，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

显示分配给存储虚拟机的聚合数量。此外，系统还将基于最高严重性级别显示聚合的运行状况。

- 卷

显示属于所选存储虚拟机的卷的数量和容量。此外，系统还将基于最高严重性级别显示卷的运行状况。当存储虚拟机中存在FlexGroup卷时，计数还包括 FlexGroup；但不包括FlexGroup组成部分。

#### 相关组窗格

通过“相关组”窗格，您可以查看与所选存储虚拟机关联的组列表。

#### 相关警报窗格

通过“相关警报”窗格，您可以查看为所选存储虚拟机创建的警报列表。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。

#### 集群/健康详情页面

集群/健康详情页面提供有关所选集群的详细信息，例如健康、容量和配置详情。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

命令按钮使您能够对选定的集群执行以下任务：

- 切换到性能视图

使您能够导航到集群/性能详细信息页面。

- 行动

- 添加警报：打开添加警报对话框，您可以向选定的集群添加警报。
- 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 重新获取缓存数据（如果有）。

重新发现操作启动后，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：使您能够注释选定的集群。

- 查看集群

使您能够导航到“健康状况：所有集群”视图。

#### “健康”标签

显示有关各种集群对象（例如节点、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表来查看对象的过滤列表。例如，您可以单击显示警告的 SVM 容量图表来查看经过筛选的 SVM 列表。此列表包含具有容量问题且严重级别为“警告”的卷或 qtree 的 SVM。您还可以单击显示警告的 SVM 可用性图表，查看存在严重级别为“警告”的可用性问题的 SVM 列表。

## 可用性問題

以图形方式显示对象的总数，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。图形中的颜色表示问题的不同严重性级别。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。所有其他条形图显示的数据都是根据生成的事件计算的。

## 容量問題

以图形方式显示对象的总数，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。图形中的颜色表示问题的不同严重性级别。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，有关可能会违反设定阈值的聚合的信息。

### 容量选项卡

显示有关所选集群容量的详细信息。

### 容量

显示有关所有已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

未应用ONTAP存储效率技术节省的数据在该集群的所有聚合上存储的实际数据大小。这包括 Snapshot 副本。

- 数据缩减

显示不包含 Snapshot 副本且带有两个有效数字的比率，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。这包括用于奇偶校验、正确大小调整和预留的容量。

- 可用

显示可用的数据容量。

- 备用

显示所有备用磁盘中可供存储的可存储容量。

- 已配置

显示为所有底层卷配置的容量。

## 详细信息

显示有关已用容量和可用容量的详细信息。该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、正确大小调整和预留的容量。

- 可用

显示可用的数据容量。

- 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供存储的可存储容量。

## 云层

显示已使用的云层总容量，以及集群上启用FabricPool的聚合的每个连接的云层所使用的容量。 FabricPool可以是已授权的，也可以是未授权的。

## 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”选项卡中查看有关磁盘类型的更多信息。

- 总可用容量

显示数据盘的可用容量和剩余容量。

- HDD

图形化展示集群中所有HDD数据盘的已用容量和可用容量。虚线表示HDD中数据盘的剩余容量。

- 闪存

- SSD数据

图形化展示集群中SSD数据盘的已用容量和可用容量。

- 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

显示集群中未分配的磁盘数。

## 具有容量问题的聚合列表

以表格形式显示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

表示聚合具有一定严重程度容量相关问题。

您可以将指针移到状态上以查看有关聚合生成的事件的更多信息。

如果聚合的状态由单个事件决定，则可以查看事件名称、触发事件的时间和日期、分配事件的管理员的姓名以及事件的原因等信息。您可以点击“查看详细信息”按钮查看有关该事件的更多信息。

如果聚合的状态由多个相同严重程度事件决定，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分配事件的管理员的姓名等信息。您可以单击事件名称来查看其中每个事件的更多详细信息，您还可以单击“查看所有事件”链接来查看生成的事件列表。



一个聚合可以具有多个严重程度相同或不同的容量相关事件。但是，系统将仅显示最高严重性。例如，如果聚合具有两个事件，其严重性级别分别为“错误”和“严重”，则仅显示“严重”严重性。

- 聚合

显示聚合的名称。

- 已用数据容量

以图形方式显示有关总容量使用情况的信息（百分比）。

- 达到全满前的天数

显示聚合达到满负荷之前预计剩余的天数。

## “配置”选项卡

显示有关所选集群的详细信息，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。还显示接口的运行状态。

- 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

显示集群的完全限定域名 (FQDN)。

- 操作系统版本

显示集群正在运行的ONTAP版本。如果集群中的节点运行不同版本的ONTAP，则显示最早的ONTAP版本。

- 联系方式

显示有关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

确定这是否是全 SAN 阵列配置的集群。

## 远程集群概述

提供有关MetroCluster配置中远程集群的详细信息。仅针对MetroCluster配置显示此信息。

- 集群

显示远程集群的名称。点击集群名称，可以跳转到该集群的详情页面。

- 主机名或 IP 地址

显示远程集群的 FQDN、简称或 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。仅针对 FC 或 IP 配置的MetroCluster显示此信息。

- 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：

#### 对于 FC

- 使用 SAS 缆线的延伸型配置
- 使用 FC-SAS 桥接器的延伸配置
- 使用 FC 交换机的光纤配置



对于四节点MetroCluster，仅支持具有 FC 交换机的结构配置。

#### 对于 IP

- 使用以太网交换机的 IP 配置（L2 或 L3，取决于集群的配置方式）
  - 自动计划外切换 (AUSO)

显示本地集群是否启用了自动计划外切换。默认情况下，Unified Manager 中双节点MetroCluster配置中的所有集群均启用 AUSO。您可以使用命令行界面来更改 AUSO 设置。此功能仅支持 FC 上的MetroCluster。

- 切换模式

显示MetroCluster over IP 配置的切换模式。可用的值有：Active，Negotiated Switchover，和 Automatic Unplanned Switchover。

#### 节点

- 可用性

显示已启动的节点数 (●) 或向下 (●) 在集群中。

- 操作系统版本

显示节点正在运行的ONTAP版本以及运行特定版本ONTAP的节点数。例如，9.6 (2), 9.3 (1) 指定两个节点正在运行ONTAP 9.6，一个节点正在运行ONTAP 9.3。

#### 存储虚拟机

- 可用性

显示已启动的 SVM 数量 (●) 或向下 (●) 在集群中。

#### 网络接口

- 可用性

显示已启动的非数据 LIF 的数量 (●) 或向下 (●) 在集群中。

- 集群管理接口

显示集群管理 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列表。数据协议包括 iSCSI、CIFS、NFS、NVMe 和 FC/FCoE。

## 保护

- 调解器

显示集群是否支持中介以及中介的连接状态。它指示中介是否已配置，如果已配置，则显示中介的状态。

- 不适用

当集群不支持中介时显示。

- 未配置

当集群支持中介但未配置中介时显示。

- IP 地址

当集群支持调解器并且调解器已配置时显示。调解员状态通过颜色表示。绿色表示调解器状态可达。红色表示调解器状态不可达。

## 云层

列出此集群所连接的云层的名称。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 配置中的集群组件的问题和连接状态。当集群的灾难恢复伙伴出现问题时，集群将显示在红色框中。



仅对于采用 FC 上的MetroCluster配置的集群，才会显示MetroCluster连接选项卡。

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来查看组件的详细信息。例如，点击集群中节点的计数链接，即可显示该集群详情页中的节点标签。单击远程集群中磁盘的数量链接，将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，无法在另一对 HA 上显示本地货架。

您可以将指针移到组件上，以查看出现问题时集群的详细信息和连接状态，并查看有关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决定，您可以查看事件名称、触发事件的时间和日期、分配事件的管理员的姓名以及事件的原因等信息。查看详细信息按钮提供有关该事件的更多信息。

如果组件之间的连接问题的状态由多个相同严重程度的事件决定，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分配事件的管理员的姓名等信息。您可以单击事件名称来查看其中每个事件的更多详细信息，您还可以单击“查看所有事件”链接来查看生成的事件列表。

#### MetroCluster “复制”选项卡

显示通过 FC 配置在MetroCluster中复制的数据的状态。您可以使用MetroCluster Replication 选项卡通过与已经对等的集群同步镜像数据来确保数据保护。当集群的灾难恢复伙伴出现问题时，集群将显示在红色框中。



仅对于采用 FC 上的MetroCluster配置的集群，才会显示MetroCluster复制选项卡。

在MetroCluster环境中，您可以使用此选项卡来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期间可能出现的问题。

在MetroCluster Replication 选项卡中，本地集群提供所选集群的详细图形表示，而MetroCluster伙伴集群指的是远程集群。

#### 网络接口选项卡

显示在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 (↑)，向下 (↓) 或未知 (?)。网络接口的运行状态由其物理端口的状态决定。

##### 管理状态

显示接口的管理状态，可以是 Up (↑)，向下 (↓) 或未知 (?)。当您更改配置或进行维护时，您可以控制接口的管理状态。管理状态可以与运行状态不同。但是，如果 LIF 的管理状态为 Down，则操作状态默认为 Down。

## IP 地址

显示接口的 IP 地址。

## 角色

显示接口的角色。可能的角色是集群管理 LIF、节点管理 LIF、集群 LIF 和集群间 LIF。

## 母港

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。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。

## 节点选项卡

显示有关所选集群中的节点的信息。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 状态和 HA 对中节点的健康状况的图形表示。节点的健康状态通过以下颜色表示：

- 绿色的

节点处于工作状态。

- 黄色的

该节点已接管伙伴节点或该节点正面临一些环境问题。

- 红色的

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，会显示以下消息：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的连接性。您还可以查看事件触发的时间。

您可以查看其他与节点相关的信息，例如型号。

如果有单节点集群，还可以查看节点的详细信息。

## 磁盘架

显示有关 HA 对中磁盘架的信息。

您还可以查看磁盘架和环境组件生成的事件以及事件触发的时间。

- 货架编号

显示磁盘所在机架的 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：

- 绿色的

环境组件运行正常。

- 灰色的

没有关于环境成分的数据。

- 红色的

一些环境因素已经下降。

- 状态

显示磁盘架的状态。可能的状态有离线、在线、无状态、需要初始化、丢失和未知。

- 模型

显示磁盘架的型号。

- 本地磁盘架

指示磁盘架位于本地集群还是远程集群。此列仅对 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

显示有关关联的 FC、FCoE 和以太网端口的信息。您可以通过单击端口图标来查看有关端口和关联 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，端口名称可以是 e0M、e0a 和 e0b。

- 角色

显示端口的角色。可能的角色有集群、数据、集群间、节点管理和未定义。

- 类型

显示端口使用的物理层协议。可能的类型有以太网、光纤通道和 FCoE。

- WWPN

显示端口的全球端口名称 (WWPN)。

- 固件修订版

显示 FC/FCoE 端口的固件修订版。

- 状态

显示端口的当前状态。可能的状态包括“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

显示有关所选集群中磁盘的详细信息。可以查看已使用磁盘数、备用磁盘数、损坏磁盘数、未分配磁盘数等磁盘相关信息。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

显示磁盘数量（按有效类型（FCAL、SAS、SATA、MSATA、SSD、NVMe SSD、SSD CAP、Array LUN 和 VMDISK）分类）和磁盘状态。您还可以查看其他详细信息，例如聚合、共享磁盘、备用磁盘、损坏磁盘、未分配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 组

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。

## 状态

显示磁盘的状态：聚合、共享、备用、损坏、未分配、不受支持或未知。默认情况下，此列按以下顺序排序显示状态：损坏、未分配、不受支持、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群集还是远程群集。此列仅对MetroCluster配置中的集群显示。

## 位置

根据磁盘的容器类型显示磁盘的位置：例如，副本、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到影响的聚合数量。您可以将指针移到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”视图中查看受影响聚合的列表。

对于下列情况，此列不显示任何值：

- 对于损坏的磁盘，当包含此类磁盘的集群添加到 Unified Manager 时
- 当没有故障磁盘时

## 存储池

显示 SSD 所属的存储池的名称。将鼠标悬停在存储池名称上，可以查看该存储池的详细信息。

## 可存储容量

显示可用的磁盘容量。

## 原始容量

显示正确调整大小和 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ONTAP分配的磁盘类型。

对于创建和添加聚合以及备用管理而言，某些ONTAP磁盘类型被视为等效的。ONTAP为每种磁盘类型分配一种有效的磁盘类型。

#### 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，以百分比显示已用 SSD 寿命的估计值。大于 99 的值表示已消耗了估计的耐久度，但可能并不表示 SSD 故障。如果值未知，则省略磁盘。

#### 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

显示磁盘所在机架的 ID。

#### 托架

显示磁盘所在托架的ID。

#### 相关注释窗格

使您能够查看与所选集群相关的注释详细信息。详细信息包括注释名称和应用于集群的注释值。您还可以从“相关注释”窗格中删除手动注释。

#### 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、数量和健康状态。您可以点击计数链接对该特定设备进行进一步分析。

您可以使用MetroCluster合作伙伴窗格来获取远程MetroCluster合作伙伴及其相关集群组件（例如节点、聚合和SVM）的数量和详细信息。MetroCluster合作伙伴窗格仅针对MetroCluster配置中的集群显示。

通过“相关设备”窗格，您可以查看并导航到与集群相关的节点、SVM 和聚合：



## MetroCluster 配对集群

显示MetroCluster伙伴的健康状况。使用计数链接，您可以进一步导航并获取有关集群组件的健康和容量的信息。

### 节点

显示属于所选集群的节点的数量、容量和健康状态。容量表示可用容量与可用容量之比。

### 存储虚拟机

显示属于选定集群的 SVM 的数量。

### 聚合

显示属于所选集群的聚合的数量、容量和运行状况。

### 相关组窗格

使您能够查看包含所选集群的组列表。

### 相关警报窗格

通过“相关警报”窗格，您可以查看所选集群的警报列表。您也可以单击“添加警报”链接来添加警报，或者单击警报名称来编辑现有警报。

### 相关信息

["卷页面" "查看集群列表和详细信息"](#)

### 聚合/健康详情页面

您可以使用聚合/健康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FabricPool的聚合时，此页面上的已提交值和过量提交值仅与本地或性能层容量相关。云层中可用的空间量未反映在超额承诺的值中。类似地，聚合阈值仅与本地性能层相关。

命令按钮使您能够对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。

- 行动

- 添加警报

使您能够向选定的聚合添加警报。

- 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“健康状况：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生成这些事件的设置。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

未应用ONTAP存储效率技术节省的成本，聚合上存储的数据的实际大小。

- 已用

聚合中数据使用的物理容量。

- 已过量提交

当聚合中的空间被过度使用时，图表会显示一个带有过度使用量的标志。

- 警告

在设置警告阈值的位置显示一条虚线；表示聚合中的空间已快满。如果违反此阈值，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一条实线；表示聚合中的空间已满。如果违反此阈值，则会生成“空间已满”事件。

- Snapshot 副本图

只有已使用的 Snapshot 容量或 Snapshot 预留不为零时，才会显示此图形。

如果已使用的快照容量超过快照预留，则两个图表都会显示快照容量超过快照预留的容量。

- 云层

显示启用FabricPool的聚合的云层中数据所使用的空间。FabricPool可以是已授权的，也可以是未授权的。

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这里。

- 细节

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快照容量。

- 已过量提交的容量

显示总过量承诺。聚合过量使用使您能够提供比给定聚合实际可用的更多的存储空间，只要当前并非所有存储空间都正在被使用。使用精简配置时，聚合中卷的总大小可能会超过聚合的总容量。



如果您过度使用了聚合，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FabricPool的聚合的云层中数据所使用的空间。FabricPool可以是已授权的，也可以是未授权的。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这里

- 总缓存空间

显示添加到 Flash Pool 聚合的固态硬盘 (SSD) 或分配单元的总空间。如果您已为聚合启用 Flash Pool 但尚未添加任何 SSD，则缓存空间将显示为 0 KB。



如果为聚合禁用了 Flash Pool，则此字段将被隐藏。

- 聚合阈值

显示以下聚合容量阈值：

- 接近全满阈值

指定聚合接近满的百分比。

- 全满阈值

指定聚合已满的百分比。

- 接近过量提交阈值

指定聚合接近过度承诺的百分比。

- 过量提交阈值

指定聚合过度承诺的百分比。

- 其他详情：每日增长率

如果最后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，如果某个聚合在下午 2 点使用 10 GB 磁盘空间，在下午 6 点使用 12 GB 磁盘空间，则该聚合的每日增长率 (GB) 为 2 GB。

- 卷移动

显示当前正在进行的卷移动操作的数量：

- 卷移出

显示正在移出聚合的卷的数量和容量。

您可以单击该链接查看更多详细信息，例如卷名称、卷移动到的聚合、卷移动操作的状态以及预计结束时间。

- 卷移入

显示正在移动到聚合中的卷的数量和剩余容量。

您可以单击该链接查看更多详细信息，例如卷名称、移动卷的聚合、卷移动操作的状态以及预计结束时间。

- Estimated used capacity after volume move

显示卷移动操作完成后估计的已用空间总量（以百分比表示，单位为 KB、MB、GB 等）。

- 容量概览 - 卷

显示提供有关聚合中包含的卷容量的信息的图表。显示卷已使用的空间量（已用容量）和卷中可用空间量（可用容量）。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）。

您可以从下拉列表中选择要查看的图表。您可以对图表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、每日最快增长率和最慢增长率等详细信息。您可以根据包含聚合中的卷的存储虚拟机 (SVM) 来过滤数据。您还可以查看精简配置卷的详细信息。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。默认情况下，图表显示总体排名前 30 的过滤卷。

## 磁盘信息选项卡

显示有关选定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 组以及所用的磁盘类型（例如 SAS、ATA、FCAL、SSD 或 VMDISK）。您可以将光标放在奇偶校验磁盘和数据磁盘上来查看更多信息，例如磁盘的托架、架子和旋转速度。

- 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，显示共享磁盘的图形详细信息。当数据盘包含专用盘和共享盘时，会同时显示专用盘和共享盘的图形详情。

- **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

显示聚合中的 RAID 组的数量。

- 使用的磁盘

- 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，不会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，不会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

显示选定聚合中节点可用的备用数据磁盘的有效类型、数量和容量。



当聚合故障转移到配对节点时，Unified Manager 不会显示与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。

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

显示聚合中的 RAID 组的数量。

- 使用的磁盘

- 有效类型

表示聚合中用于缓存的磁盘类型为 SSD。

- 数据磁盘

显示分配给缓存聚合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

显示选定聚合中可用于缓存的节点的备用磁盘的有效类型、数量和容量。



当聚合故障转移到配对节点时，Unified Manager 不会显示与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。您可以将指针移到存储池名称上来查看以下详细信息：

- 状态

显示存储池的状态，可以是健康或不健康。

- 总分配量

显示存储池中的分配单元总数和大小。

- 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量。如果存储池列中的磁盘数量与该存储池的“磁盘信息”选项卡中显示的磁盘数量不匹配，则表示一个或多个磁盘损坏，存储池不健康。

- 已用分配量

显示聚合使用的分配单元的数量和大小。您可以单击聚合名称来查看聚合详细信息。

- 可用分配量

显示节点可用的分配单元的数量和大小。您可以单击节点名称来查看聚合详细信息。

- 分配的缓存

显示聚合使用的分配单元的大小。

- 分配单位

显示聚合使用的分配单元数。

- 磁盘

显示存储池中包含的磁盘数量。

- 细节

- 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

如果您已配置启用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，两个云层的详细信息都会显示在这里

## “配置”选项卡

配置选项卡显示有关所选聚合的详细信息，例如其集群节点、块类型、RAID 类型、RAID 大小和 RAID 组数量：

- 概述

- 节点

显示包含选定聚合的节点的名称。

- 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 组

显示聚合中的 RAID 组的数量。

- SnapLock 类型

显示聚合的SnapLock类型。

- 云层

如果这是启用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的不同而不同。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这里。

- 提供程序

显示存储提供商的名称，例如StorageGRID、Amazon S3、IBM Cloud Object Storage、Microsoft Azure Cloud、Google Cloud Storage 或 Alibaba Cloud Object Storage。

- 名称

显示由ONTAP创建云层时的名称。

- 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

显示云层的访问密钥或帐户。

- 容器名称

显示云层的存储桶或容器名称。

- SSL

显示是否为云层启用了 SSL 加密。

## 历史区

历史记录区域显示提供有关所选聚合容量的信息的图表。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。

您可以从历史记录窗格顶部的下拉列表中选择图表类型。也可以通过选择 1 周、1 个月或 1 年来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，如果总体使用情况持续突破“接近满”阈值，您可以采取适当的措施。



历史记录图显示下列信息：

- 已用总容量 (%)

以百分比形式在垂直 (y) 轴上显示已使用的容量总量和基于使用历史记录容量总量的使用趋势（折线图）。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，当您单击“已用容量”图例时，“已用容量”图形线将被隐藏。

- 已用总容量与总容量

根据使用历史记录显示聚合容量的使用趋势，以及已用容量和总容量，以折线图形式在垂直 (y) 轴上以字节、千字节、兆字节等单位显示。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。

- 已用总容量 (%) 与已承诺容量 (%)

根据使用历史记录显示聚合容量的使用趋势，并以折线图的形式显示已提交空间（以百分比表示，位于垂直 (y) 轴上）。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，当您单击“已承诺空间”图例时，“已承诺空间”图形线将被隐藏。

## 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：

- 严重性

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。如果时间超过一周，则会显示事件生成的时间戳。

## 相关设备窗格

通过“相关设备”窗格，您可以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。容量表示可用容量与可用容量之比。

- 节点中的聚合

显示包含选定聚合的集群节点中所有聚合的数量和容量。此外，系统还将基于最高严重性级别显示聚合的运行状况。例如，如果一个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

显示聚合中的FlexVol卷和FlexGroup卷的数量和容量；该数量不包括FlexGroup组成部分。此外，系统还将基于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

通过“相关警报”窗格，您可以查看为选定聚合创建的警报列表。您也可以单击“添加警报”链接来添加警报，或者单击警报名称来编辑现有警报。

#### 相关信息

["查看存储池详细信息"](#)

# 保护和恢复数据

## 创建、监控和排除保护关系故障

Unified Manager 使您能够创建保护关系、监控和排除托管集群上存储的数据的镜像保护和备份库保护故障，以及在数据被覆盖或丢失时恢复数据。

### 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。SnapMirror保护的所有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。

在传统的SnapMirror关系中，镜像操作的执行速度比在替代SnapMirror关系中更快，因为镜像操作基于块复制。但是，传统的SnapMirror保护要求目标卷在与同一主要版本中的源卷相同或更高版本的ONTAP软件下运行（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，因为目标正在运行早期主要版本。

#### SnapMirror异步保护，具有版本灵活的复制

SnapMirror异步保护与版本灵活的复制功能可在源卷和目标卷之间提供逻辑复制镜像保护，即使这些卷在不同版本的ONTAP 8.3 或更高版本软件下运行（例如，版本 8.3 到 8.3.1、8.3 到 9.1 或 9.2.2 到 9.2）。

在具有版本灵活复制的SnapMirror关系中，镜像操作的执行速度不如传统SnapMirror关系中那么快。

由于执行速度较慢，具有版本灵活复制保护的SnapMirror不适合在以下任一情况下实施：

- 源对象包含超过 1000 万个需要保护的文件。
- 受保护数据的恢复点目标是两小时或更短。（也就是说，目标必须始终包含镜像的、可恢复的数据，且这些数据的保存时间不能比源数据早两个小时。）

在列出的任何一种情况下，都需要基于更快的块复制执行默认SnapMirror保护。

#### SnapMirror异步保护，具有版本灵活的复制和备份选项

SnapMirror异步保护具有版本灵活的复制和备份选项，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从源到目标镜像哪些 Snapshot 副本，还可以指定在目标保留这些副本多长时间，即使它们在源被删除。

在具有版本灵活复制和备份选项的SnapMirror关系中，镜像操作的执行速度不如传统SnapMirror关系中那么快。

## 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，统一数据保护在第一次调用时执行基线传输。默认统一数据保护策略“MirrorAndVault”下的基线传输会对源卷进行快照复制，然后将该副本及其引用的数据块传输到目标卷。与SnapVault一样，统一数据保护不包括基线中的旧 Snapshot 副本。

### SnapMirror同步保护，严格同步

SnapMirror同步保护采用“严格”同步，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失败，则客户端对主卷的 I/O 将会中断。

### SnapMirror同步保护与定期同步

SnapMirror同步保护采用“常规”同步，不要求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 将继续到主卷。



从“健康状况：所有卷”视图或“卷/健康状况详细信息”页面监控同步保护关系时，“恢复”按钮和“关系操作”按钮不可用。

### SnapMirror主动同步

SnapMirror主动同步功能在ONTAP 9.8 及更高版本中可用，您可以使用它来保护带有 LUN 的应用程序，使应用程序能够透明地进行故障转移，确保在发生灾难时业务连续性。

它允许您从 Unified Manager 发现和监控集群和存储虚拟机上可用的一致性组 (CG) 的同步SnapMirror关系。AFF集群或所有 SAN 阵列 (ASA ) 集群均支持SnapMirror主动同步，其中主集群和辅助集群可以是AFF或ASA。SnapMirror主动同步使用 iSCSI 或 FCP LUN 保护应用程序。

当您查看受SnapMirror主动同步关系保护的卷和 LUN 时，您可以获得保护关系、卷清单中的一致性组的统一视图，查看一致性组关系的保护拓扑，查看长达一年的一致性组关系的历史数据。您也可以下载该报告。您还可以查看一致性组关系的摘要、搜索一致性组关系的支持，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主动同步的更多信息，请参阅["Snapmirror 主动同步（以前称为 SM-BC）的ONTAP 9 文档"](#)。

## 在 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，您必须执行几个步骤。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须在两个集群或两个 Storage Virtual Machine (SVM) 之间建立对等关系。
- OnCommand Workflow Automation必须与 Unified Manager 集成：
  - ["设置OnCommand Workflow Automation"](#)。
  - ["验证工作流自动化中的 Unified Manager 数据源缓存"](#)。

## 步骤

1. 根据您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，请根据要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"。

## 配置工作流自动化和 **Unified Manager** 之间的连接

您可以在OnCommand Workflow Automation (WFA) 和 Unified Manager 之间配置安全连接。连接到工作流自动化使您能够使用保护功能（例如SnapMirror和SnapVault配置工作流）以及用于管理SnapMirror关系的命令。

### 开始之前

- 安装的工作流自动化版本必须为 5.1.1P6 或更高版本。



WFA 5.1.1P6 中包含“用于管理 Clustered Data ONTAP 的WFA 包”，因此无需像过去那样从 NetAppStorage Automation Store 下载此包并将其单独安装到 WFA 服务器上。 ["用于管理ONTAP 的WFA 包"](#)

- 您必须拥有在 Unified Manager 中创建的数据库用户的名称才能支持 WFA 和 Unified Manager 连接。  
必须已为该数据库用户分配集成模式用户角色。
- 您必须被分配工作流自动化中的管理员角色或架构师角色。
- 您必须拥有工作流自动化设置的主机地址、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”>“工作流自动化”。
2. 在“工作流自动化页面”的“数据库用户”区域中，选择名称并输入您创建的用于支持 Unified Manager 和工作流自动化连接的数据库用户的密码。
3. 在页面的\*工作流自动化凭据\*区域中，输入主机名或 IP 地址（IPv4 或 IPv6）以及工作流自动化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“保存”。
5. 如果您使用自签名证书，请单击“是”授权安全证书。

显示工作流自动化页面。

6. 单击“是”重新加载 Web UI，并添加工作流自动化功能。

["NetApp文档： OnCommand Workflow Automation （当前版本）"](#)

### 在工作流自动化中验证 **Unified Manager** 数据源缓存

您可以通过检查工作流自动化中的数据源获取是否成功来确定 Unified Manager 数据源缓存是否正常工作。您可以在将工作流自动化与 Unified Manager 集成时执行此操作，以确保集成后工作流自动化功能可用。

#### 开始之前

您必须被分配工作流自动化中的管理员角色或架构师角色才能执行此任务。

#### 步骤

1. 从工作流自动化 UI 中，选择 **执行 > 数据源**。
2. 右键单击 Unified Manager 数据源的名称，然后选择 **立即获取**。
3. 验证获取是否成功且无错误。

必须解决获取错误才能使工作流自动化与 Unified Manager 成功集成。

### 重新安装或升级**OnCommand Workflow Automation**时会发生什么情况

在重新安装或升级OnCommand Workflow Automation之前，您必须首先删除OnCommand Workflow Automation与 Unified Manager 之间的连接，并确保所有当前正在运行或计划的OnCommand Workflow Automation作业都已停止。

您还必须从OnCommand Workflow Automation中手动删除 Unified Manager。

重新安装或升级OnCommand Workflow Automation后，您必须再次建立与 Unified Manager 的连接。

### 从 **Unified Manager** 中删除**OnCommand Workflow Automation**设置

当您不再想使用工作流自动化时，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\*>\*工作流自动化\*。
2. 在\*工作流自动化\*页面中，单击\*删除设置\*。

### 执行保护关系故障转移和故障回复

当保护关系中的源卷由于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/写，并故障转移到该卷，直到源再次联机；然后，当原始源

可用于提供数据时，您可以故障恢复到原始源。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须设置OnCommand Workflow Automation才能执行此操作。

步骤

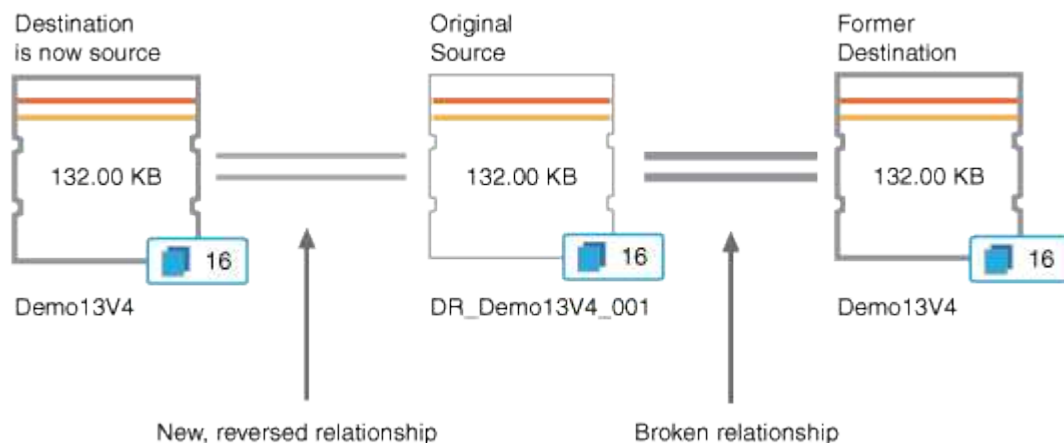
1. "断开 SnapMirror 关系"。

您必须先中断该关系，然后才能将目标从数据保护卷转换为读/写卷，然后才能逆转该关系。

2. "反转保护关系"。

当原始源卷再次可用时，您可能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，您必须将其与写入先前目标的数据同步。您可以使用反向重新同步操作来创建新的保护关系，方法是反转原始关系的角色并将源卷与之前的目标同步。为新的关系创建一个新的基线 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以再次提供数据时，使用中断操作来中断反转关系。

4. "删除关系"。

当不再需要逆转的关系时，您应该先删除该关系，然后再重新建立原始关系。

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。

从卷/运行状况详细信息页面断开**SnapMirror**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。目标卷更改为读写卷。您不能破坏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。
- 您必须已经设置了工作流自动化。

#### 步骤

1. 在“**Volume / Health**”详细信息页面的“**Protection**”选项卡中，从拓扑中选择要中断的SnapMirror关系。
2. 右键单击目标并从菜单中选择\*Break\*。

将显示“中断关系”对话框。

3. 单击“继续”即可断开关系。
4. 在拓扑中，验证关系是否已中断。

#### 从卷/健康详情页面反转保护关系

当灾难导致保护关系中的源卷失效时，您可以在修复或更换源卷的同时，将目标卷转换为读/写卷，以提供数据。当源再次可以接收数据时，您可以使用反向重新同步操作来建立反向关系，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。
- 您必须已经设置了工作流自动化。
- 该关系不能是SnapVault关系。
- 保护关系必须已经存在。
- 保护关系必须被打破。
- 源和目标都必须在线。
- 源不能是另一个数据保护卷的目标。
- 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相同。

如果不存在策略和计划，则创建它们。

#### 步骤

1. 从“**Volume / Health**”详细信息页面的“**Protection**”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\*。

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您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关闭，作业链接显示在卷/健康详情页面顶部。

4. \*可选：\*单击“卷/健康”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。



显示经过筛选的作业列表。

5. \*可选：\*单击浏览器上的\*后退\*箭头返回到\*音量/健康\*详细信息页面。

当所有作业任务成功完成后，反向重新同步操作就完成了。

#### 从卷/健康详情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，当您想要使用不同的目标创建关系时。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。
- 您必须已经设置了工作流自动化。

##### 步骤

1. 在“**Volume / Health**”详细信息页面的“**Protection**”选项卡中，从拓扑中选择要删除的SnapMirror关系。
2. 右键单击目的地的名称，然后从菜单中选择“删除”。

将显示“删除关系”对话框。

3. 单击“继续”以删除关系。

该关系已从卷/健康详细信息页面中删除。

#### 从卷/健康详情页面重新同步保护关系

您可以重新同步已中断的SnapMirror或SnapVault关系上的数据，然后将目标设置为读/写，以便源上的数据与目标上的数据匹配。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，您可能还需要重新同步。

##### 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“**Volume / Health**”详细信息页面的“**Protection**”选项卡中，在拓扑中找到要重新同步的保护关系并右键单击它。
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\*以重新同步您当前正在查看详细信息的关系。

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“源快照副本”；然后在“快照副本”列中单击“默认”。

系统弹出“选择源Snapshot副本”对话框。

5. 如果您想指定现有的 Snapshot 副本而不是传输默认的 Snapshot 副本，请单击“现有 **Snapshot** 副本”并从列表选择一个 Snapshot 副本。
6. 单击“提交”。

您将返回到“重新同步”对话框。

7. 如果您选择了多个要重新同步的源，请单击“默认”以选择要为其指定现有 Snapshot 副本的下一个源。
8. 单击“提交”开始重新同步作业。

重新同步作业已启动，您将返回到卷/健康详细信息页面，并且页面顶部会显示作业链接。

9. \*可选：\*单击“卷/健康详情”页面上的“查看作业”以跟踪每个重新同步作业的状态。

显示经过筛选的作业列表。

10. \*可选：\*单击浏览器上的\*后退\*箭头返回到\*音量/健康\*详细信息页面。

当所有作业任务成功完成后，重新同步作业即完成。

## 解决保护作业失败

此工作流程提供了一个示例，说明如何从 Unified Manager 仪表板识别和解决保护作业失败。

### 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来查看您的保护作业是否存在任何问题。在“保护事件”区域，您会注意到有一个“作业终止”事件，显示卷上出现“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。



事件的链接文本以以下形式编写 `object_name:/object_name - Error Name`，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。

看[“识别问题并对失败的保护作业执行纠正措施”](#)。

### 识别问题并对失败的保护作业执行纠正措施

您在“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，您可以进入“音量/健康详细信息”页面来收集更多信息。

开始之前

您必须具有应用程序管理员角色。

事件详细信息页面上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。

该作业涉及源卷之间的保护关系 `cluster2_src_vol2` 在虚拟服务器上 `cluster2_src_svm` 以及目标卷 `managed_svc2_vol3` 在名为 `cluster3_dst_svm`。

- Snapshot 复制作业失败 `0426cluster2_src_vol2snap` 在源卷上 `cluster2_src_svm:/cluster2_src_vol2`。

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，解决故障需要您访问系统管理器 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，您选择不这样做。

2. 您决定尝试解决该事件，因此执行以下操作：

- a. 单击“分配给”按钮并从菜单中选择“我”。
- b. 如果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. 您还可以选择添加有关该事件的注释。

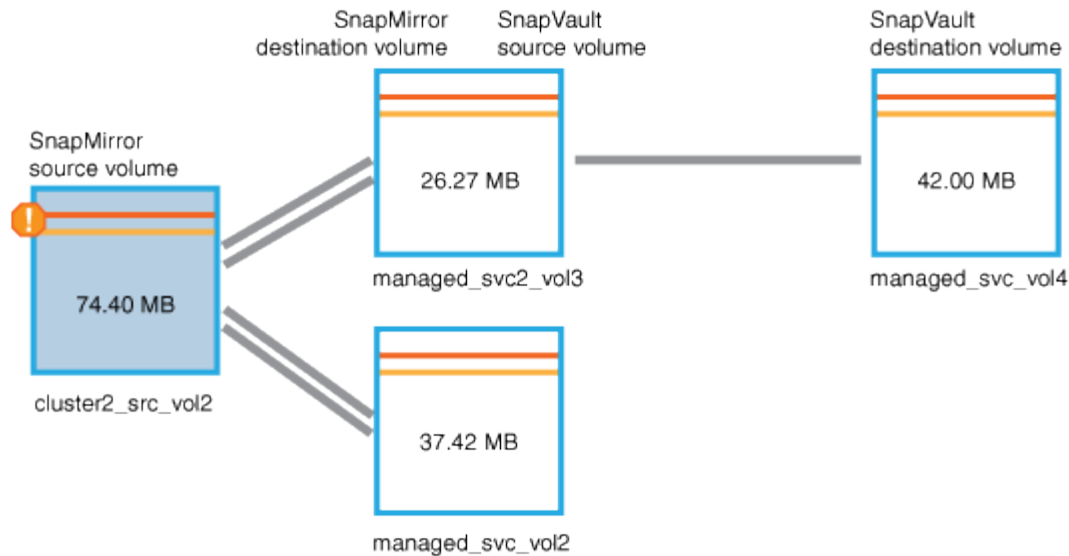
3. 单击“摘要”窗格中的“源”字段可查看有关源卷的详细信息。

**Source** 字段包含源对象的名称：在本例中，即计划执行 Snapshot 复制作业的卷。

音量/健康详情页面显示 `cluster2_src_vol2`，显示“保护”选项卡的内容。

4. 查看保护拓扑图，您会看到与拓扑中第一个卷关联的错误图标，该卷是 SnapMirror 关系的源卷。

您还会看到源卷图标中的水平条，表示为该卷设置的警告和错误阈值。



5. 将光标放在错误图标上，可以看到显示阈值设置的弹出对话框，并看到卷已超过错误阈值，表明存在容量问题。
6. 单击“容量”选项卡。

有关卷的容量信息 `cluster2\_src\_vol2` 显示。

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该卷设置的阈值水平。
8. 在容量图下方，您可以看到卷自动增长已被禁用，并且已设置卷空间保证。

您可以决定启用自动增长，但出于此场景的目的，您决定在决定如何解决容量问题之前进一步调查。

9. 您向下滚动到“事件”列表，会看到生成了“保护作业失败”、“卷满天数”和“卷空间满”事件。
10. 在\*事件\*列表中，单击\*卷空间已满\*事件以获取更多信息，并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，您可以阅读该事件的“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，您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，因此您不会看到针对所有类型事件的此区域。

单击可执行的建议操作列表来解决卷空间已满事件：

- 在此卷上启用自动增长。
- 调整卷大小。
- 在此卷上启用并运行重复数据删除。
- 在此卷上启用并运行压缩。

13. 您决定在卷上启用自动增长，但要做到这一点，您必须确定父聚合上的可用空间和当前卷增长率：
  - a. 查看父聚合， `cluster2_src_aggr1` ，在“相关设备”窗格中。



您可以单击聚合的名称以获取有关聚合的更多信息。

您确定聚合具有足够的空间来启用卷自动增长。

- b. 在页面顶部，查看表示关键事件的图标并查看图标下方的文本。

您确定“满员天数：少于一天 | 每日增长率：5.4%”。

14. 转至系统管理器或访问ONTAP CLI 以启用 `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 \*事件\*详细信息页面并将事件标记为已解决。

## 解决滞后问题

此工作流程提供了如何解决滞后问题的示例。在这种情况下，您是管理员或操作员，访问 Unified Manager Dashboard 页面来查看您的保护关系是否存在问题，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“仪表板”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关系滞后错误并单击它。

将显示滞后错误事件的事件详细信息页面。

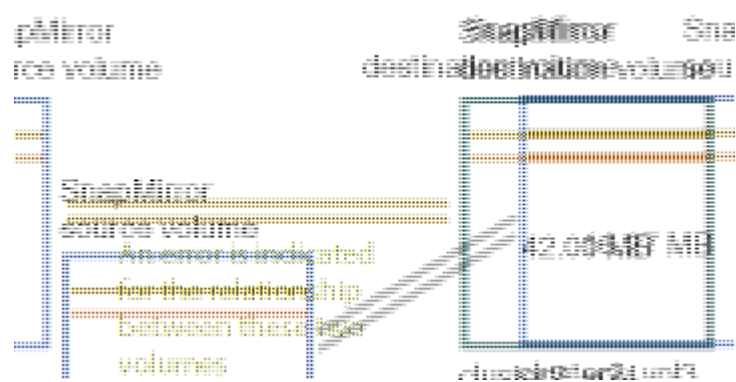
2. 您可以在“\*活动\*详细信息”页面中执行以下一项或多项任务：
  - 查看“摘要”区域的“原因”字段中的错误消息，以确定是否有任何建议的纠正措施。
  - 单击摘要区域的源字段中的对象名称（在本例中为卷）以获取有关该卷的详细信息。
  - 查找可能已添加的有关此事件的注释。
  - 为事件添加注释。
  - 将事件分配给特定用户。
  - 确认或解决该事件。
3. 在这种情况下，您单击“**Summary**”区域的“Source”字段中的对象名称（在本例中为卷）以获取有关该卷的详细信息。

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。

您注意到，具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勾勒，源卷的双

橙色线表示SnapMirror关系错误。



5. 单击SnapMirror级联中的每个卷。

当您选择每个卷时，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会发生变化，以显示与所选卷相关的详细信息。

6. 您查看\*摘要\*区域并将光标放在每个卷的\*更新计划\*字段中的信息图标上。

在此场景中，您注意到SnapMirror策略为 DPDefault，并且SnapMirror计划每小时在整点后的五分钟更新一次。您意识到关系中的所有卷都在尝试同时完成SnapMirror传输。

7. 为了解决滞后问题，您可以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

Active IQ Unified Manager使您能够创建保护关系、监控和排除托管集群上的SnapMirror和SnapVault关系故障，以及在数据被覆盖或丢失时恢复数据。

对于SnapMirror操作，有两种复制类型：

- 异步

从主卷到辅助卷的复制由计划决定。

- 同步

复制在主卷和辅助卷上同时执行。

您可以同时执行最多 10 项保护作业，而不会对性能产生任何影响。当您同时运行 11 到 30 个作业时，可能会遇到一些性能影响。不建议同时运行超过 30 个作业。

### 查看卷保护状态

数据保护页面提供了单个集群中所有受保护卷或数据中心中所有集群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. 根据您是否要查看所有受监控集群或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部的右箭头。显示“数据保护”页面。

根据您在数据中心中选择的是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，同时显示未受保护卷的数量。

从\*单个集群\*列表选择一个集群将显示该集群中受保护卷的 Snapshot 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”链接来查看事件管理库存页面中的所有活动保护事件。您可以将鼠标悬停在屏幕上来查看相应的计数和图例。您可以点击：

- 未受保护的卷和受 Snapshot 副本保护的卷的条形图，可转到“卷”页面并查看详细信息。
- 所有关系的条形图都转到“关系”页面，其中详细信息由源集群过滤。

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 副本保护和未受 Snapshot 副本保护的卷总数。
- 正在使用或超出 Snapshot 副本的预留空间的卷总数。

\*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 小时内发生的事件。
- 受 Snapshot 副本保护和未受 Snapshot 副本保护的卷的详细图表。
- 卷正在使用、未使用以及超出预留的 Snapshot 副本容量。
- 卷的分解是根据其 Snapshot 副本的数量进行的。

**Snapshot** 副本注意事项

- 为了计算受 Snapshot 副本保护的卷数，需要同时考虑源卷和目标卷。
- 返回的 Snapshot 副本数仅适用于处于在线状态且可用的卷。
- Snapshot 副本数量的图表范围是动态的。它是根据所选集群中存在的快照数量生成的。
- 为了将卷视为受保护的，应启用该卷的 Snapshot 副本计划。
- Snapshot 副本的预留空间值对于查看已利用的磁盘空间量或计算删除一个或多个 Snapshot 副本时可以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策略保护的卷的数量，例如卷SnapMirror关系、存储 VM 灾难恢复 (SVM-DR) 及其组合。
- 根据滞后状态，经历恢复点目标 (RPO) 滞后的SnapMirror关系总数。
- SnapMirror分析\* 详细说明了以下信息：

- 针对SnapMirror关系引发的单个事件，包括过去 24 小时内引发的事件
- 每种SnapMirror策略保护的卷数。
- SnapMirror关系类型保护的关系数，例如异步镜像、异步保险库、异步 MirrorVault、StricxtSync、SnapMirror活动同步一致性组和同步。
- 健康和 unhealthy 关系的数量。
- 分解成交量关系计数。您可以按 RPO 滞后时间和状态切换图表。
- 非管理关系的滞后阈值。您可以点击设置图标 (  ) 配置滞后阈值设置。有关详细信息，请参阅 ["配置非托管保护关系的滞后阈值设置"](#)。

#### SnapMirror关系注意事项

- 为了计算SnapMirror关系的数量，将计算已启用读取和写入的源卷。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的数量。
- 数据复制中 RPO 滞后的滞后持续时间基于SnapMirror关系。状态分类为 ok, warning, 或者 error, 基于关系阈值的设置。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。
- 如果卷具有多个SnapMirror关系，则每种关系类型都会计入 RPO 滞后。
- 如果源和目标之间的数据复制存在问题（例如，当关系中断时），则卷关系被视为不健康。

#### 查看受MetroCluster配置保护的集群

数据保护\*页面上的 MetroCluster保护\*面板显示您的站点上通过 FC 或 IP 配置受MetroCluster保护或未受保护的集群数量。单击此面板上的条形图将转到“集群”页面，其中将根据受保护或不受保护的集群来过滤集群详细信息。有关监控MetroCluster配置的信息，请参阅["监控MetroCluster配置"](#)。

#### 查看卷保护关系

从“关系：所有关系”视图和“卷关系”页面中，您可以查看现有卷SnapMirror和SnapVault关系的状态。您还可以检查有关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、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。

您还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“存储”>“卷”。
2. 从“视图”菜单中，选择“关系”>“所有关系”。

关系：显示所有关系视图。

3. 选择以下方式之一来查看卷保护详细信息：



- 要查看有关所有卷关系的当前信息，请保留默认的“所有关系”页面。
- 要查看一段时间内卷转移趋势的详细信息，请在“查看”菜单中选择“关系：过去 1 个月的转移状态视图”。
- 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。

## 监控一致性组关系中的 LUN

如果您的ONTAP环境支持SnapMirror主动同步来保护具有 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 SAN 环境中故障转移期间的零恢复时间目标 (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 和从 LUN 是复合 LUN，或者具有相同 UUID 和序列号的副本 LUN 对。这些复合 LUN 上的源站点和目标站点之间的 I/O 操作（读取和写入）均进行多路复用，以确保透明度。

要查看复合 LUN，应在 Unified Manager 上添加和发现具有一致性组关系一部分的 LUN 的主集群和辅助集群。仅支持 iSCSI 和 FCP LUN。

有关SnapMirror主动同步的信息，请参阅["SnapMirror主动同步（以前称为 SM-BC）的ONTAP 9 文档"](#)。

要查看您环境中的复合 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. 从“查看”菜单中，选择“关系”>“所有 LUN”。

关系：显示所有 LUN 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、一致性组和合作伙伴 LUN。您可以单击每个组件来深入了解详细视图。单击一致性组将转到关系页面。

单击合作伙伴 LUN 后，您可以在托管合作伙伴 LUN 的存储虚拟机的“存储虚拟机详细信息”页面的“SAN”选项卡上查看其配置详细信息。显示启动器、启动器组以及合作伙伴 LUN 的其他方面的信息。

您可以对环境中受保护的 LUN 执行标准网格级功能，包括排序、筛选、生成和上传报告。

## 从“Health: All Volumes”视图创建SnapVault保护关系

您可以使用“运行状况：所有卷”视图为同一存储虚拟机上的一个或多个卷创建SnapVault关系，以启用数据备份来保护数据。

### 开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已经设置了工作流自动化。

在下列情况下不会显示“保护”菜单：

- 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“存储”>“卷”。
2. 在\*Health: All Volumes\*视图中，选择要保护的卷，然后单击\*Protect\*。

或者，要在同一个存储虚拟机 (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\*。

启动“配置保护”对话框。

4. 单击 \* SnapVault\* 查看 \* SnapVault\* 选项卡并配置二级卷信息。
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. 完成“SnapVault”选项卡中的“目标信息”区域和“关系设置”区域。
7. 单击“应用”。

您将返回到“健康状况：所有卷”视图。

8. 单击“**Health: All Volumes**”视图顶部的保护配置作业链接。

如果您只创建一个保护关系，则会显示“作业详细信息”页面；但是，如果您创建多个保护关系，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：
  - 如果您只有一项作业，请单击“刷新”以更新与保护配置作业相关的任务列表和任务详细信息，并确定作业何时完成。
  - 如果您有多个工作：
    - i. 单击作业列表中的一项作业。
    - ii. 单击“刷新”以更新与保护配置作业相关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”按钮返回到过滤列表并查看另一项工作。

## 从卷/运行状况详细信息页面创建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，以便启用数据备份来保护卷。

#### 开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须设置工作流自动化才能执行此任务。

在下列情况下不会显示“保护”菜单：

- 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“**Volume / Health**”详细信息页面的“**Protection**”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\*。

启动“配置保护”对话框。

3. 单击“\* SnapVault\*”查看“\* SnapVault\*”选项卡，配置二级资源信息。
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. 完成“配置保护”对话框中的“目标信息”区域和“关系设置”区域。
6. 单击“应用”。

您将返回到“音量/健康”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。

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相关的任务列表和任务详细信息，并确定作业何时完成。

当作业任务完成时，新的关系将显示在卷/健康详细信息页面拓扑视图中。

## 从“**Health: All Volumes**”视图创建**SnapMirror**保护关系

使用“运行状况：所有卷”视图，您可以通过在同一存储虚拟机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。
- 您必须已经设置了工作流自动化。

在下列情况下不会显示“保护”菜单：

- 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\*Health:All Volumes\*视图中，选择要保护的卷。

或者，要在同一个 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”。

弹出“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”根据需要设置空间保证，然后单击“应用”。
4. 完成“\* SnapMirror\*”选项卡中的“目标信息”区域和“关系设置”区域。
5. 单击“应用”。

您将返回到“健康状况：所有卷”视图。

6. 单击“健康：所有卷视图”顶部的保护配置作业链接。

如果您只创建一个保护关系，则会显示“作业详细信息”页面；但是，如果您创建多个保护关系，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：

- 如果您只有一项作业，请单击“刷新”以更新与保护配置作业相关的任务列表和任务详细信息，并确定作业何时完成。
- 如果您有多个工作：
  - i. 单击作业列表中的一项作业。
  - ii. 单击“刷新”以更新与保护配置作业相关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”按钮返回到过滤列表并查看另一项工作。

根据您在配置期间指定的目标 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化之一：

- 如果您指定的目标 SVM 在与源卷相同或更新版本的ONTAP下运行，则基于块复制的SnapMirror关系是默认结果。
- 如果您指定的目标 SVM 在与源卷相同或更新版本的ONTAP下运行，但在高级设置中启用了版本灵活复制，则会产生具有版本灵活复制的SnapMirror关系。
- 如果您指定的目标 SVM 在比源卷更早的ONTAP版本下运行，并且早期版本支持版本灵活复制，则会自动产生具有版本灵活复制的SnapMirror关系。

## 从卷/运行状况详细信息页面创建SnapMirror保护关系

您可以使用卷/运行状况详细信息页面创建SnapMirror关系，以便启用数据复制来保护目的。 SnapMirror复制使您能够在源卷上发生数据丢失时从目标卷恢复数据。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已经设置了工作流自动化。

在下列情况下不会显示“保护”菜单：

- 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

您可以同时执行最多 10 项保护作业，而不会对性能产生任何影响。当您同时运行 11 到 30 个作业时，可能会遇到一些性能影响。不建议同时运行超过 30 个作业。

## 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保护的卷的名称。
2. 从菜单中选择\*保护\* > \* SnapMirror\*。

弹出“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”根据需要设置空间保证，然后单击“应用”。
5. 完成“配置保护”对话框中的“目标信息”区域和“关系设置”区域。
6. 单击“应用”。

您将返回到“音量/健康”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相关的任务列表和任务详细信息，并确定作业何时完成。
9. 当作业任务完成后，单击浏览器上的\*返回\*即可返回到\*Volume / Health\*详细信息页面。

新的关系显示在卷/健康详细信息页面拓扑视图中。

根据您在配置期间指定的目标 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化之一：

- 如果您指定的目标 SVM 在与源卷相同或更新版本的ONTAP下运行，则基于块复制的SnapMirror关系是默认结果。
- 如果您指定的目标 SVM 在与源卷相同或更新版本的ONTAP下运行，但在高级设置中启用了版本灵活复制，则会产生具有版本灵活复制的SnapMirror关系。
- 如果您指定的目标 SVM 在ONTAP的早期版本或高于源卷的版本下运行，并且早期版本支持版本灵活复制，则会自动产生具有版本灵活复制的SnapMirror关系。

## 创建具有版本灵活复制的SnapMirror关系

您可以创建具有版本灵活复制的SnapMirror关系。即使源卷和目标卷在不同版本的ONTAP下运行，版本灵活的复制也使您能够实施SnapMirror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。
- 您必须已经设置了工作流自动化。
- 源 SVM 和目标 SVM 都必须启用SnapMirror许可证。
- 源 SVM 和目标 SVM 必须分别在支持版本灵活复制的ONTAP软件版本下运行。

具有版本灵活复制功能的SnapMirror使您即使在并非所有存储都在一个版本的ONTAP下运行的异构存储环境中也能实施SnapMirror保护；但是，在具有版本灵活复制功能的SnapMirror下执行的镜像操作的执行速度不如在传

统块复制SnapMirror下那么快。

#### 步骤

1. 显示您想要保护的卷的“配置保护”对话框。
  - 如果您正在查看“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”。弹出“配置保护”对话框。
2. 单击 \* SnapMirror\* 以查看 \* SnapMirror\* 选项卡。
3. 完成“配置保护”对话框中的“目标信息”区域和“关系设置”区域。

如果您指定的目标 SVM 在比要保护的源卷更早的ONTAP版本下运行，并且该早期版本支持版本灵活的复制，则此任务会自动使用版本灵活的复制配置SnapMirror。

4. 如果您指定的目标 SVM 与源卷运行在相同的ONTAP版本下，但仍想使用版本灵活的复制配置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”。

您将返回到“音量/健康”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相关的任务列表和任务详细信息，并确定作业何时完成。
8. 当作业任务完成后，单击浏览器上的\*返回\*即可返回到\*Volume / Health\*详细信息页面。

新的关系显示在卷/健康详细信息页面拓扑视图中。

## 使用备份选项创建具有版本灵活复制的SnapMirror关系

您可以创建具有版本灵活复制和备份选项功能的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。
- 您必须已经设置了工作流自动化。
- 源 SVM 和目标 SVM 都必须启用SnapMirror许可证。
- 源 SVM 和目标 SVM 都必须启用SnapVault许可证。
- 源 SVM 和目标 SVM 必须分别在支持版本灵活复制的ONTAP软件版本下运行。

配置具有备份选项功能的SnapMirror使您能够使用SnapMirror灾难恢复功能（例如卷故障转移功能）保护您的数据，同时提供SnapVault功能（例如多个备份副本保护）。

#### 步骤

1. 显示您想要保护的卷的“配置保护”对话框。
  - 如果您正在查看“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“健康状况：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”。弹出“配置保护”对话框。
2. 单击 \* SnapMirror\* 以查看 \* SnapMirror\* 选项卡。
3. 完成“配置保护”对话框中的“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“**Version-Flexible Replication**”复选框，请立即选中它。
6. 选中“使用备份选项”复选框以启用备份选项功能；然后单击“应用”。
7. 单击“应用”。

您将返回到“音量/健康”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相关的任务列表和任务详细信息，并确定作业何时完成。
10. 当作业任务完成后，单击浏览器上的\*返回\*即可返回到\*Volume / Health\*详细信息页面。

新的关系显示在卷/健康详细信息页面拓扑视图中。

## 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。当您想要最大化目标卷或辅助卷的空间利用率时，可以使用这些设置。

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，效率设置与源卷的设置相匹配，但SnapVault关系中的压缩设置除外，该设置默认情况下处于禁用状态。

步骤

1. 根据您正在配置的关系类型，单击“配置保护”对话框中的“\* SnapMirror\*”选项卡或“\* SnapVault\*”选项卡。
2. 单击“目标信息”区域中的“高级”。

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、压缩、自动增长和空间保证的效率设置。
4. 单击“应用”保存您的选择并返回“配置保护”对话框。

## 创建SnapMirror和SnapVault计划

您可以创建基本或高级SnapMirror和SnapVault计划，以在源卷或主卷上启用自动数据保护传输，以便传输更频繁或更少地进行，具体取决于卷上数据更改的频率。

### 开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已经完成了配置保护对话框中的目标信息区域。
- 您必须设置工作流自动化才能执行此任务。

### 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。

弹出“创建计划”对话框。

2. 在“计划名称”字段中，输入您想要赋予计划的名称。

3. 选择下列选项之一：

- 基本的

如果您想创建基本间隔式时间表，请选择。

- 先进的

如果您想要创建 cron 风格的计划，请选择。

4. 单击“创建”。

新的计划将显示在SnapMirror计划或SnapVault计划下拉列表中。

## 创建级联或扇出关系，以扩展现有保护关系的保护

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对现有关系的保护。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，您可能会这样做。

您可以使用一致性组将保护扩展到卷，一致性组是一个包含多个卷的容器，以便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。
- 您必须已经设置了工作流自动化。

### 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. 根据您正在创建的保护关系类型，选择“使用SnapMirror”或“使用SnapVault”。

将显示“配置保护”对话框。



这可以从统一关系/卷关系和卷/健康详细信息页面实现。

6. 按照“配置保护”对话框中的指示填写信息。

## 从卷关系页面编辑保护关系

您可以编辑现有的保护关系来更改最大传输速率、保护策略或保护计划。您可以编辑关系以减少用于传输的带宽，或者增加计划传输的频率，因为数据经常变化。

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。当选择源卷、负载共享卷或非SnapMirror或SnapVault关系目标的卷时，您无法编辑关系。

步骤

1. 在“卷关系”页面中，在卷列表中选择同一 SVM 中要编辑关系设置的一个或多个卷，然后从工具栏中选择“编辑”。

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”。

更改将应用于选定的关系。

## 从卷/健康详情页面编辑保护关系

您可以编辑现有的保护关系来更改当前的最大传输速率、保护策略或保护计划。您可以编辑关系以减少用于传输的带宽，或者增加计划传输的频率，因为数据经常变化。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已经安装并配置了工作流自动化。

所选卷必须是保护关系目标。当选择源卷、负载共享卷或非SnapMirror或SnapVault关系目标的卷时，您无法编辑关系。

步骤

1. 从\*Volume / Health\*详细信息页面的\*Protection\*选项卡中，在拓扑中找到要编辑的保护关系并右键单击它。

2. 从菜单中选择\*编辑\*。

或者，从\*操作\*菜单中，选择\*关系\*>\*编辑\*来编辑您当前正在查看详细信息的关系。

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”。

更改将应用于选定的关系。

## 创建**SnapMirror**策略以最大程度提高传输效率

您可以创建SnapMirror策略来指定保护关系的SnapMirror传输优先级。 SnapMirror策略允许您通过分配优先级来最大程度地提高从源到目标的传输效率，以便将较低优先级的传输安排在正常优先级的传输之后运行。

### 开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已经设置了工作流自动化。
- 此任务假定您已经完成了“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。

系统弹出“创建SnapMirror策略”对话框。

2. 在“策略名称”字段中，输入您想要赋予策略的名称。
3. 在\*转移优先级\*字段中，选择您想要分配给策略的转移优先级。
4. 在“注释”字段中，输入该策略的可选注释。
5. 单击“创建”。

新策略显示在SnapMirror策略下拉列表中。

## 创建**SnapVault**策略以最大程度提高传输效率

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程度地提高保护关系中从主节点到次节点的传输效率。

### 开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已经设置了工作流自动化。
- 您必须已经完成了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。

将显示SnapVault选项卡。

2. 在“策略名称”字段中，输入您想要赋予该策略的名称。
3. 在“转移优先级”字段中，选择您想要分配给策略的转移优先级。
4. \*可选：\*在“注释”字段中，输入该政策的注释。
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“创建”。

新策略显示在“创建策略”下拉列表中。

## 从卷关系页面中止活动数据保护传输

当您想要停止正在进行的SnapMirror复制时，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启检查点。当传输与其他操作（例如卷移动）冲突时，您可能会中止传输。



您不能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。
- 您必须已经设置了工作流自动化。

在下列情况下不会显示中止操作：

- 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

您无法清除基线传输的重启检查点。

### 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”。

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”对话框关闭，中止作业的状态显示在“卷关系”页面顶部，同时显示作业详细信息的链接。

4. 可选：\*单击“\*查看详细信息”链接转到“工作”详细信息页面以获取更多详细信息并查看工作进度。

## 从卷/健康详情页面中止活动数据保护传输

当您想要停止正在进行的SnapMirror复制时，可以中止活动数据保护传输。如果不是基线

传输，您还可以清除传输的重启检查点。当传输与其他操作（例如卷移动）冲突时，您可能会中止传输。



您不能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。
- 您必须已经设置了工作流自动化。

在下列情况下不会显示中止操作：

- 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

您无法清除基线传输的重启检查点。

#### 步骤

1. 在“**Volume / Health**”详细信息页面的“**Protection**”选项卡中，右键单击拓扑视图中要中止的数据传输的关系，然后选择“**Abort**”。

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”。

中止传输对话框关闭，中止操作的状态显示在卷/健康详细信息页面的顶部，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“工作”详细信息页面以获取更多详细信息并查看工作进度。
5. 单击每个作业任务即可查看其详细信息。
6. 单击浏览器上的“后退”箭头返回到\*Volume / Health\*详细信息页面。

当所有作业任务成功完成后，中止操作就完成了。

## 从卷关系页面停止保护关系

在“卷关系”页面中，您可以暂停保护关系以暂时阻止数据传输的发生。当您想要创建包含数据库的 SnapMirror 目标卷的 Snapshot 副本时，您可能会停顿关系，并且您希望确保其内容在 Snapshot 副本操作期间保持稳定。

#### 开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已经设置了工作流自动化。

在下列情况下不会显示静默操作：

- 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
- 当您尚未配对 Workflow Automation 和 Unified Manager 时

#### 步骤

1. 要使一个或多个保护关系的传输处于静止状态，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“静止”。

将显示“静默”对话框。

2. 单击“继续”。

静默作业的状态显示在卷/健康详情页面的顶部，同时显示作业详情的链接。

3. 单击“查看详细信息”链接转到“工作”详细信息页面，查看更多详细信息和工作进度。
4. \*可选：\*单击浏览器上的\*后退\*箭头返回到\*卷关系\*页面。

当所有作业任务成功完成后，静默作业即完成。

### 从卷/健康详情页面暂停保护关系

您可以停止保护关系以暂时阻止数据传输的发生。当您想要创建包含数据库的 SnapMirror 目标卷的 Snapshot 副本时，您可能会停顿关系，并且您希望确保其内容在 Snapshot 副本期间保持稳定。

#### 开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已经设置了工作流自动化。

在下列情况下不会显示静默操作：

- 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
- 当您尚未配对 Workflow Automation 和 Unified Manager 时

#### 步骤

1. 在“**Volume / Health**”详细信息页面的“**Protection**”选项卡中，右键单击拓扑视图中要静止的保护关系的关系。
2. 从菜单中选择\*静默\*。
3. 单击“是”继续。

静默作业的状态显示在卷/健康详情页面的顶部，同时显示作业详情的链接。

4. 单击“查看详细信息”链接转到“工作”详细信息页面，查看更多详细信息和工作进度。
5. 可选：\*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后，静默作业即完成。

## 从卷关系页面断开SnapMirror关系

您可以中断保护关系以停止SnapMirror关系中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。目标卷更改为读/写卷。您不能破坏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。
- 您必须已经设置了工作流自动化。

### 步骤

1. 从“卷关系”页面中，选择一个或多个具有保护关系且要停止数据传输的卷，然后在工具栏上单击“中断”。

将显示“中断关系”对话框。

2. 单击“继续”即可断开关系。
3. 在“卷关系”页面中，在“关系状态”列中验证关系是否已中断。

关系状态列默认是隐藏的，因此您可能需要在显示/隐藏列列表中选择它。

## 从卷关系页面中删除保护关系

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，当您想要使用不同的目标创建关系时。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。
- 您必须已经设置了工作流自动化。

### 步骤

1. 从“卷关系”页面中，选择一个或多个要删除的具有保护关系的卷，然后在工具栏上单击“删除”。

将显示“删除关系”对话框。

2. 单击“继续”以删除关系。

该关系已从卷关系页面中删除。

## 从卷关系页面恢复静止关系上的计划传输

在您停止关系以停止发生计划的传输后，您可以使用\*恢复\*重新启用计划的传输，以便保护源或主卷上的数据。如果存在检查点，则在下一个预定的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。

- 您必须已经设置了工作流自动化。

您可以选择最多 10 个静止关系来恢复传输。

#### 步骤

1. 从卷\*关系\*页面中，选择一个或多个具有静止关系的卷，然后在工具栏上单击\*恢复\*。
2. 在“恢复”对话框中，单击“继续”。

您将返回到卷关系页面。

3. 要查看相关的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相关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相关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预定的传输间隔恢复。

### 从卷/健康详情页面恢复已暂停关系的预定传输

在您停止关系以停止发生计划的传输后，您可以使用卷/健康详细信息页面上的\*恢复\*重新启用计划的传输，以便保护源或主卷上的数据。如果存在检查点，则在下一个预定的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。
- 您必须已经设置了工作流自动化。

#### 步骤

1. 在“**Volume / Health**”详细信息页面的“**Protection**”选项卡中，在拓扑视图中右键单击要恢复的静止关系。

或者，从 操作 > 关系 菜单中选择 恢复。

2. 在“恢复”对话框中，单击“继续”。

您将返回到“音量/健康”详细信息页面。

3. 要查看相关的工作任务并跟踪其进度，请单击“**Volume / Health**”详细信息页面顶部显示的作业链接。
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相关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预定的传输间隔恢复。

## 从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，或者如果关系已经初始化并且您想要执行手动、非计划增量更新以立即传输，则可以更新关系。



您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”页面上，右键单击一个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”。

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“源快照副本”；然后在“快照副本”列中单击“默认”。

系统弹出“选择源 Snapshot 副本”对话框。

4. 如果您想指定现有的 Snapshot 副本而不是传输默认的 Snapshot 副本，请单击“现有 **Snapshot** 副本”并从列表选择一个 Snapshot 副本。
5. 单击“提交”。

您将返回到\*初始化/更新\*对话框。

6. 如果您选择了多个源进行初始化或更新，请单击“默认”以选择要为其指定现有 Snapshot 副本的下一个源。
7. 单击“提交”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，并且作业链接将显示在页面顶部。

8. \*可选：\*单击\*Health: All Volumes\*视图上的\*View Jobs\*来跟踪每个初始化或更新作业的状态。

显示经过筛选的作业列表。

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\*箭头返回到\*卷关系\*页面。

当所有任务成功完成后，初始化或更新操作就完成了。

## 从卷/健康详情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，或者如果关系已经初始化并且您想要执行手动、非计划增量更新以立即传输数据，则更新关系。



注意：您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“**Volume / Health**”详细信息页面的“**Protection**”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\*来初始化或更新您当前正在查看详细信息的关系。

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“源快照副本”；然后在“快照副本”列中单击“默认”。

系统弹出“选择源Snapshot副本”对话框。

5. 如果您想指定现有的 Snapshot 副本而不是传输默认的 Snapshot 副本，请单击“现有 **Snapshot** 副本”并从列表选择一个 Snapshot 副本。
6. 单击“提交”。

您将返回到初始化/更新对话框。

7. 如果您选择了多个源进行初始化或更新，请单击“默认”以选择下一个要为其指定现有 Snapshot 副本的读/写源。

您不能为数据保护卷选择不同的 Snapshot 副本。

8. 单击“提交”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/健康详细信息页面，并且页面顶部会显示作业链接。

9. \*可选：\*单击“卷/健康”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。

显示经过筛选的作业列表。

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“**Volume / Health**”详细信息页面。

当所有作业任务成功完成后，初始化或更新操作就完成了。

#### 从卷关系页面重新同步保护关系

在“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，或者当您想要将当前源更改为其他卷时。

#### 开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 您必须已经设置了工作流自动化。

#### 步骤

1. 从“卷关系”页面中，选择一个或多个具有静止关系的卷，然后从工具栏中单击“重新同步”。

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“源快照副本”；然后在“快照副本”列中单击“默认”。

系统弹出“选择源Snapshot副本”对话框。

4. 如果您想指定现有的 Snapshot 副本而不是传输默认的 Snapshot 副本，请单击“现有 **Snapshot** 副本”并从列表选择一个 Snapshot 副本。
5. 单击“提交”。

您将返回到“重新同步”对话框。

6. 如果您选择了多个要重新同步的源，请单击“默认”以选择要为其指定现有 Snapshot 副本的下一个源。
7. 单击“提交”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，并且页面顶部会显示作业链接。

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。

显示经过筛选的作业列表。

9. \*可选：\*单击浏览器上的\*后退\*箭头返回到\*卷关系\*页面。

当所有作业任务成功完成后，重新同步操作就完成了。

## 从“卷关系”页面反向保护关系

当灾难导致保护关系中的源卷失效时，您可以在修复或更换源卷的同时，将目标卷转换为读/写卷，以提供数据。当源再次可以接收数据时，您可以使用反向重新同步操作来建立反向关系，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。
- 您必须已经设置了工作流自动化。
- 该关系不能是SnapVault关系。
- 保护关系必须已经存在。
- 保护关系必须被打破。

- 源和目标都必须在线。
- 源不能是另一个数据保护卷的目标。
- 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相同。

如果不存在策略和计划，则创建它们。

#### 步骤

1. 从“卷关系”页面中，选择一个或多个要反转关系的卷，然后在工具栏上单击“反转重新同步”。

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您要执行反向重新同步操作的关系，然后单击“提交”。

反向重新同步操作启动后，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。

显示与此操作相关的作业的过滤列表。

4. \*可选：\*单击浏览器上的\*后退\*箭头返回到\*卷关系\*页面。

当所有作业任务成功完成后，反向重新同步操作就完成了。

## 使用卷和卷/健康详情页面恢复数据

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 副本还原被覆盖或删除的文件、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：

- 您不能还原 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. 从左侧导航窗格，转到\*存储>卷\*。
2. 选择卷并单击“恢复”按钮。或者，单击卷转到\*卷/健康详情>操作>恢复\*。系统弹出“恢复”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. 选择要将选定项目恢复到的位置：原始位置\*或\*备用现有位置。

#### 6. 如果选择备用现有位置，请执行以下操作之一：

- 在“恢复路径”文本字段中，键入要恢复数据的位置的路径，然后单击“选择目录”。
- 单击“浏览”启动“浏览目录”对话框并完成以下步骤：
  - i. 选择要还原到的目标集群、存储虚拟机 (SVM) 和卷。
  - ii. 在名称表中，选择要恢复的目录名称。
  - iii. 单击“选择目录”。

#### 7. 单击“恢复”。

还原过程将开始。在后端创建一个作业来完成恢复过程。

#### 8. 如果您想查看作业进度，请从左侧导航窗格导航到\*保护>作业\*，从作业列表中查看还原作业的状态。



如果Cloud Volumes ONTAP HA 集群之间的还原操作因 NDMP 错误而失败，则可能需要在目标集群中添加明确的 AWS 路由，以便目标可以与源系统的集群管理 LIF 进行通信。您可以使用NetApp Console执行此配置步骤。

## 什么是资源池

资源池是由存储管理员使用 Unified Manager 创建的聚合组，用于为合作伙伴应用程序提供备份管理的配置。

您可以根据性能、成本、物理位置或可用性等属性来汇集资源。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独的单元进行监控和配置。这简化了这些资源的管理，并允许更灵活、更有效地使用存储。

在二级存储配置期间，Unified Manager 使用以下标准确定资源池中最适合保护的聚合：

- 该聚合是数据聚合（不是根聚合）并且处于在线状态。
- 聚合位于目标集群节点上，其ONTAP版本与源集群主版本相同或更高。
- 该聚合具有资源池中所有聚合中最大的可用空间。
- 配置目标卷后，聚合空间处于为聚合定义的接近满和接近过量使用的阈值内（全局或本地阈值，以适用者为准）。
- 目标节点上的FlexVol卷数量不得超过平台限制。

## 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用于配置目的。

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集群的聚合，但同一个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中。

## 编辑资源池

当您想要更改资源池名称和描述时，您可以编辑现有的资源池。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

仅当选择一个资源池时，“编辑”按钮才可用。如果选择了多个资源池，则“编辑”按钮将被禁用。

## 步骤

1. 在左侧导航窗格中，单击“保护”>“资源池”。
2. 从列表选择一个资源池。
3. 单击“编辑”。

将显示“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“保存”。

资源池列表中显示新的名称和描述。

## 查看资源池清单

您可以使用资源池页面查看资源池库存并监控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”。

显示资源池库存。

## 添加资源池成员

资源池由多个成员聚合组成。您可以将聚合添加到现有资源池，以增加可用于二级卷配置的空间量。

开始之前

您必须具有应用程序管理员或存储管理员角色。

一次最多可以向资源池添加 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”列表选择一个资源池。

资源池成员显示在资源池列表下方区域。

3. 在资源池成员区，单击\*添加\*。

将显示“聚合”对话框。

4. 选择一个或多个聚合。
5. 单击“添加”。

对话框关闭并且聚合显示在所选资源池的成员列表中。

## 从资源池中移除聚合

您可以从现有资源池中删除聚合：例如，当您想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。

\*删除\*按钮已启用。

4. 单击“删除”。

此时将显示警告对话框。

5. 单击“是”继续。

选定的聚合将从成员窗格中删除。

## 删除资源池

当不再需要资源池时，您可以删除它。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，从而使原始资源池变得过时。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

仅当选择至少一个资源池时，“删除”按钮才可用。

### 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“删除”。

该资源池从资源池列表中删除，其聚合也从成员列表中删除。

## 监控存储虚拟机灾难恢复保护关系

Active IQ Unified Manager支持监控存储虚拟机灾难恢复关系，从而以存储虚拟机级别提供灾难恢复。存储虚拟机灾难恢复可以恢复存储虚拟机组成卷中存在的数据以及恢复存储虚拟机配置。

从源存储虚拟机到目标存储虚拟机创建存储虚拟机 DR 关系，以提供异步灾难恢复。您可以根据集群设置选择复制存储虚拟机配置的全部或部分（不包括网络和协议配置）以及数据卷。

配置存储虚拟机灾难恢复关系后，当源存储虚拟机由于硬件故障或环境灾难而变得不可用时，目标存储虚拟机将启动，以提供对数据访问的最小中断。类似地，当源存储虚拟机可用时，它会与目标存储虚拟机重新同步，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虚拟机灾难恢复关系。

### 使用“关系”页面监控存储虚拟机

您可以从 INVENTORY 的 PROTECTION 部分中的关系页面监控存储 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过滤器。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

您可以使用过滤器来查看存储虚拟机灾难恢复关系。

### 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、一致性组和存储虚拟机关系。

2. 单击“过滤器”，然后选择“关系对象类型”和“存储虚拟机”以仅查看存储虚拟机灾难恢复关系。
3. 单击“应用过滤器”。



您应该清除组成关系过滤器以查看所有保护关系。

该页面仅展示存储虚拟机容灾关系。

从存储虚拟机页面查看保护关系

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的状态。

开始之前

您必须具有应用程序管理员或存储管理员角色。

您还可以检查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。您可以安排报告或以所需的格式下载现有报告。使用“显示/隐藏”按钮可以将所需的列添加到报告中，因为默认情况下它们不会显示。

步骤

- 1. 在左侧导航窗格中，单击“存储”>“存储虚拟机”。
- 2. 从 **VIEW** 菜单中，选择 **Relationship > All Relationships**。

关系：所有关系视图显示所有已配置的存储虚拟机。

根据保护状态查看存储虚拟机

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。

存储虚拟机视图中添加了一个新的列“保护角色”，提供有关存储虚拟机是否受保护或不受保护的信息。



如果未将源集群添加到Active IQ Unified Manager，则与该集群相关的所有信息在网格中均不可用。

步骤

- 1. 在左侧导航窗格中，单击“存储”>“存储虚拟机”。
- 2. 从 **VIEW** 菜单中，选择 **Health > All Storage VMs**。

显示健康状况：所有存储虚拟机。

- 3. 单击“筛选器”可查看以下存储虚拟机之一。

| 查看         | 过滤值            |
|------------|----------------|
| 受保护的存储虚拟机  | 保护角色 是 受保护     |
| 未受保护的存储虚拟机 | 保护角色*处于*未受保护状态 |





您不能同时查看受保护和不受保护的存储虚拟机。您需要清除现有过滤器才能重新应用新的过滤器选项。

#### 4. 单击“应用过滤器”。

未保存视图根据您的筛选器选择显示所有受存储虚拟机灾难恢复保护或不受保护的存储虚拟机。

## 了解存储虚拟机关联

存储虚拟机（存储 VM）关联是从源存储 VM 到目标存储 VM 的映射，合作伙伴应用程序使用它来进行资源选择和辅助卷配置。

无论目标存储虚拟机是二级目标还是三级目标，都会在源存储虚拟机和目标存储虚拟机之间建立关联。您不能使用二级目标存储虚拟机作为源来创建与三级目标存储虚拟机的关联。

作为应用程序管理员或存储管理员，您可以在\*保护\* > \*存储虚拟机关联\*页面上查看您环境中的存储虚拟机关联。

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 以及将来创建的任何 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的一个或多个目标 SVM。
- 关联特定存储虚拟机：您可以在特定源存储虚拟机和一个或多个特定目标 SVM 之间创建关联。例如，如果您为许多客户端提供存储服务，而这些客户端的数据必须彼此分开，则可以选择此选项将特定的源存储虚拟机与仅分配给该客户端的特定目标存储虚拟机关联。
- 与外部存储虚拟机关联：您可以在源存储虚拟机和目标存储虚拟机的外部灵活卷之间创建关联。

## 创建存储虚拟机关联

创建存储虚拟机关联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选择哪些资源。dd

### 开始之前

- 您要关联的存储虚拟机必须已经存在。
- 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，您只能在每个目标集群上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“存储虚拟机关联”页面上，单击“创建”。

\*创建存储虚拟机关联\*向导已启动。

### 3. 选择以下源之一：

- 任何

当您想要在任何主存储 VM 源和一个或多个目标存储 VM 之间创建关联时，请选择此选项。这意味着当前需要保护的所有现有存储虚拟机以及将来创建的任何存储虚拟机都与指定的目标存储虚拟机相关联。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的一个或多个目标存储虚拟机。

- 单身的

当您想要选择与一个或多个目标存储虚拟机关联的特定源存储虚拟机时，请选择此选项。例如，如果您要为许多客户端提供存储服务，而这些客户端的数据必须彼此分开，请选择此选项将特定的存储 VM 源与仅分配给该客户端的特定存储 VM 目标相关联。

- 无（外部）

当您想要在源存储虚拟机和目标存储虚拟机的外部灵活卷之间创建关联时，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. 选择一个或多个存储虚拟机保护目标。

### 7. 单击“完成”。

## 删除存储虚拟机关联

您可以删除合作伙伴应用程序的存储虚拟机关联，以删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想要创建新的存储虚拟机保护关联时，您可能会执行此操作。

### 开始之前

您必须具有应用程序管理员或存储管理员角色。

在选择至少一个存储虚拟机关联之前，“删除”按钮将被禁用。使用“Delete”和“Create”功能更改关联时，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. 选择至少一个存储虚拟机关联。

\*删除\*按钮已启用。

#### 3. 单击“删除”。

此时将显示警告对话框。

#### 4. 单击“是”继续。

选定的存储虚拟机关联将从列表中删除。

## 支持存储服务的 **SVM** 和资源池要求

如果您观察到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中的一致性：例如，当您关联 SVM 并在 Unified Manager 中创建资源池以支持合作伙伴应用程序提供的存储服务中的保护拓扑时。

一些应用程序与 Unified Manager 服务器合作，提供在源卷和二级或三级位置的保护卷之间自动配置和执行 SnapMirror 或 SnapVault 备份保护的服务。为了支持这些保护存储服务，您必须使用 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 或位于二级或三级位置的 SnapVault 备份卷），请遵守以下要求：

- 必须在包含 SnapMirror 源或 SnapVault 主卷的 SVM 与任何二级卷或三级卷所在的 SVM 之间配置 SVM 关联。
  - 例如，要支持源卷 Vol\_A 位于 SVM\_1 上、SnapMirror 二级目标卷 Vol\_B 位于 SVM\_2 上、三级 SnapVault 备份卷 Vol\_C 位于 SVM\_3 上的保护拓扑，您必须使用 Unified Manager Web UI 在 SVM\_1 和 SVM\_2 之间配置 SnapMirror 关联，并在 SVM\_1 和 SVM\_3 之间配置 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 备份关联都不是必需的，也不会使用。

- 要支持源卷 Vol\_A 和 SnapMirror 目标卷 Vol\_B 都位于 SVM\_1 上的保护拓扑，您必须在 SVM\_1 和 SVM\_1 之间配置 SnapMirror 关联。
- 资源池必须包含可供关联 SVM 使用的集群聚合资源。

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二级目标和三级目标节点。

## 什么是作业

作业是您可以使用 Unified Manager 监控的一系列任务。查看作业及其相关任务使您能够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）、当您执行数据恢复任务时、当您登录到集群时等等时，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”页面来监控该作业以及相关作业任务的进度。

## 监控作业

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”。

将显示“作业”页面。

2. 查看\*状态\*列以确定当前正在运行的作业的状态。
3. 单击工作名称即可查看有关该特定工作的详细信息。

将显示“作业详细信息”页面。

## 查看职位详情

开始一项工作后，您可以从“工作详情”页面跟踪其进度，并监控相关任务是否存在错误。

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相关的任务列表。
3. 单击某个任务即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。

## 中止作业

如果某项作业花费的时间太长、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。仅当作业的状态和类型允许时，您才可以中止作业。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项作业，然后单击“中止”。
3. 在确认提示下，单击“是”以中止所选作业。

## 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。

每次只能重试一项失败的作业。选择多个作业将禁用“重试”按钮。仅可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，选择单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”。

工作重新开始。

## 保护关系窗口和对话框说明

您可以查看和管理与保护相关的详细信息，例如资源池、SVM 关联和保护作业。您可以使用适当的“健康阈值”页面来配置聚合、卷和关系的全局健康阈值。

### 资源池页面

资源池页面显示现有的资源池及其成员，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：

- 创造

启动“创建资源池”对话框，您可以使用该对话框创建资源池。

- 编辑

使您能够编辑所创建的资源池的名称和描述。

- 删除

使您能够删除一个或多个资源池。

### 资源池列表

资源池列表显示（以表格形式）现有资源池的属性。

- 资源池

显示资源池的名称。

- 描述

描述资源池。

- \* SnapLock类型\*

显示资源池中聚合正在使用的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 等单位）。

- 已用容量

显示资源池中使用的空间量（以 MB、GB 等单位）。

- 可用容量

显示资源池中可用的空间量（以 MB、GB 等单位）。

- 用过的 %

显示资源池中已使用的空间百分比。

#### 成员列表命令按钮

成员列表命令按钮使您能够执行以下任务：

- 添加

使您能够向资源池添加成员。

- 删除

使您能够从资源池中删除一个或多个成员。

#### 成员名单

选择资源池后，成员列表会显示（表格格式）资源池成员及其属性。

- 地位

显示成员聚合的当前状态。状态可以是“严重”（）， 错误（）， 警告（）或正常（）。

- 聚合名称

显示成员聚合的名称。

- 状态

显示聚合的当前状态，可以是以下之一：

- 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写访问。

- 受限

允许有限的操作（例如奇偶校验重建），但不允许数据访问。

- 正在创建

正在创建聚合。

- 正在销毁

聚合体正在被破坏。

- 失败

聚合无法联机。

- 已冻结

聚合（暂时）不处理请求。

- 不一致

该聚合已被标记为损坏；您应该联系技术支持。

- 受 Iron 限制

诊断工具无法在聚合上运行。

- 正在安装

骨料正在安装过程中。

- 部分

至少为聚合找到了一个磁盘，但缺少两个或更多磁盘。

- 正在暂停

总体已处于静止状态。

- 已暂停

总体已静止。

- 已还原

聚合的恢复已完成。

- 已卸载

聚合已被卸载。

- 正在卸载

聚合正在脱机。

- 未知

已发现聚合，但 Unified Manager 服务器尚未检索聚合信息。

默认情况下，此列处于隐藏状态。

- 簇

显示聚合所属集群的名称。

- 节点

显示聚合所在节点的名称。

- 总容量

显示聚合的总容量（以 MB、GB 等单位）。

- 已用容量

显示聚合中使用的空间量（以 MB、GB 等单位）。

- 可用容量

显示聚合中可用的空间量（以 MB、GB 等单位）。

- 用过的 %

显示聚合中使用的空间百分比。

- 磁盘类型

显示 RAID 配置类型，可以是以下之一：

- RAID0：所有 RAID 组均为 RAID0 类型。
- RAID4：所有 RAID 组均为 RAID4 类型。
- RAID-DP：所有 RAID 组均为 RAID-DP 类型。
- RAID-TEC：所有 RAID 组都属于RAID-TEC类型。
- 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。

## 创建资源池对话框

您可以使用“创建资源池”对话框来命名和描述新的资源池，以及向该资源池添加聚合和从中删除聚合。



#### 资源池名称

文本框使您能够添加以下信息来创建资源池：

使您能够指定资源池名称。

#### 描述

使您能够描述资源池。

#### 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，以便您可以将特定集群中的聚合添加到资源池。您可以从不同的集群添加聚合，但不能将相同的聚合添加到多个资源池。

- 消除

使您能够从资源池中删除选定的聚合。

- 创造

创建资源池。直到在资源池名称或描述字段中输入信息后，此按钮才会启用。

- 取消

放弃更改并关闭“创建资源池”对话框。

#### 编辑资源池对话框

您可以使用“编辑资源池”对话框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，您可以更改它们以使其更精确。

#### 文本框

您可以使用文本框更改所选资源池的以下信息：

- 资源池名称

使您能够输入新名称。

- 描述

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：

- 节省

保存对资源池名称和描述的更改。

- 取消

放弃更改并关闭“编辑资源池”对话框。

## 聚合对话框

您可以使用“聚合”对话框来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

将选定的聚合添加到资源池。至少选择一个聚合后，“添加”按钮才会启用。

- 取消

放弃更改并关闭“聚合”对话框。

## 聚合列表

聚合列表显示（以表格形式）受监控聚合的名称和属性。

- 地位

显示卷的当前状态。状态可以是“严重”（）， 错误（）， 警告（）或正常（）。

您可以将指针移到状态上来查看有关该卷生成的事件的更多信息。

- 聚合名称

显示聚合的名称。

- 状态

显示聚合的当前状态，可以是以下之一：

- 脱机

不允许读取或写入访问。

- 受限

允许有限的操作（例如奇偶校验重建），但不允许数据访问。

- 联机

允许对该聚合上托管的卷进行读写访问。

- 正在创建

正在创建聚合。

- 正在销毁

聚合体正在被破坏。

- 失败

聚合无法联机。

- 已冻结

聚合（暂时）不处理请求。

- 不一致

该聚合已被标记为损坏；您应该联系技术支持。

- 受 Iron 限制

诊断工具无法在聚合上运行。

- 正在安装

骨料正在安装过程中。

- 部分

至少为聚合找到了一个磁盘，但缺少两个或更多磁盘。

- 正在暂停

总体已处于静止状态。

- 已暂停

总体已静止。

- 已还原

聚合的恢复已完成。

- 已卸载

聚合处于离线状态。

- 正在卸载

聚合正在脱机。

- 未知

已发现聚合，但 Unified Manager 服务器尚未检索聚合信息。

- 簇

显示聚合所在集群的名称。

- 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 等单位）。默认情况下，此列处于隐藏状态。

- 承诺容量

显示聚合中所有卷的已提交总空间（以 MB、GB 等单位）。默认情况下，此列处于隐藏状态。

- 已用容量

显示聚合中使用的空间量（以 MB、GB 等单位）。

- 可用容量

显示可用于聚合中的数据的空间量（以 MB、GB 等单位）。默认情况下，此列处于隐藏状态。

- 可用的 %

显示聚合中可用于数据的空间百分比。默认情况下，此列处于隐藏状态。

- 用过的 %

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。

## 工作页面

通过“作业”页面，您可以查看所有正在运行的合作伙伴应用程序保护作业以及已完成的作业的当前状态和其他信息。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

中止选定的作业。仅当选定的作业正在运行时此选项才可用。

- 重试

重新启动保护配置或保护关系操作类型失败的作业。每次只能重试一项失败的作业。如果选择了多个失败的作业，则“重试”按钮将被禁用。您无法重试失败的存储服务作业。

- 刷新

刷新作业列表及其相关信息。

## 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，列表仅显示过去一周内生成的作业。您可以使用列排序和过滤来自定义要显示的作业。

- 地位

显示作业的当前状态。状态可以是错误 (❗) 或正常 (✅)。

- 职位编号

显示作业的识别号。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。您可以通过在列过滤器提供的文本框中输入职位标识号来搜索特定职位。

- 姓名

显示作业的名称。

- 类型

显示作业类型。工作类型如下：

- 集群获取

工作流自动化作业正在重新发现集群。

- 保护配置

保护作业正在启动工作流自动化工作流，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 workflow 链

workflow 自动化作业正在执行多个 workflow。

- 恢复

恢复作业正在运行。

- 清理

这项工作正在清理不再需要用于恢复目的的存储服务成员工件。

- 符合

这项工作是检查存储服务成员的配置以确保它们符合要求。

- 破坏

这项工作正在破坏存储服务。

- 进口

该作业正在将非托管存储对象导入现有存储服务。

- 调整

该作业正在修改现有存储服务的属性。

- 订阅

这项工作是为会员订阅存储服务。

- 取消订阅

这项工作是取消会员的存储服务订阅。

- 更新

保护更新作业正在运行。

- **WFA 配置**

workflow 自动化作业正在推送集群凭证并同步数据库缓存。

- 状态

显示作业的运行状态。状态选项如下：

- 已中止

工作已中止。

- 中止

此项工作正在中止。

- 完全的

工作已经完成了。

- 跑步

工作正在运行。

- 提交时间

显示作业提交的时间。

- 期间

显示完成作业所花费的时间。默认显示此列。

- 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。

## 职位详情页面

通过“作业详细信息”页面，您可以查看正在运行、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。

## 工作摘要

作业摘要显示以下信息：

- 作业 ID
- 类型
- 状态
- 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

刷新任务列表和与每个任务相关的属性。

- 查看职位

返回“工作”页面。

作业任务列表在表中显示与特定作业相关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，最近的任务显示在列的顶部，较旧的任务显示在底部。

- 类型

显示任务的类型。

- 状态

特定任务的状态：

- 完全的

任务已完成。

- 排队

任务即将运行。

- 跑步

任务正在运行。

- 等待

作业已提交，一些相关任务正在等待排队和执行。

- 地位

显示任务状态：

- 错误 ()

任务失败。

- 普通的 ()

任务成功。

- 跳过 ()

某项任务失败，导致后续任务被跳过。

- 期间

显示任务开始以来经过的时间。

- 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。该列可以进行排序和过滤。默认情况下，此列处于隐藏状态。

- 依赖顺序

显示一个表示图表中任务序列的整数，其中第一个任务分配零。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附加信息，包括任务名称、任务描述以及失败的原因（如果任务失败）。

- 任务消息窗格

显示特定于选定任务的消息。消息可能包括错误的原因和解决错误的建议。并非所有任务都会显示任务消息。

## 高级辅助设置对话框

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复制、多副本备份和空间相关设置。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。

与空间相关的设置可最大限度地增加存储的数据量，包括：重复数据删除、数据压缩、自动增长和空间保证。

该对话框包括以下字段：

- 启用版本灵活复制

启用具有版本灵活复制功能的SnapMirror。即使目标卷运行的ONTAP版本低于源卷的版本，版本灵活的复制也能为源卷提供SnapMirror保护。

- 启用备份

如果启用了版本灵活复制，还可以将SnapMirror源数据的多个 Snapshot 副本传输到SnapMirror目标并保留在该目标。

- 启用重复数据删除

在SnapVault关系中的二级卷上启用重复数据删除，以便消除重复的数据块，从而节省空间。当空间节省至少 10% 并且数据覆盖率不是很快时，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，每次传输后都会启动此操作。

- 启用数据压缩

启用透明数据压缩。当空间节省至少 10%、潜在开销可以接受、并且在非高峰时段有足够的系统资源来完成压缩时，您可以使用压缩。在SnapVault关系中，此设置默认处于禁用状态。仅当选择重复数据删除时才可以启用压缩。

- 实时数据压缩

通过在将数据写入磁盘之前压缩数据来立即节省空间。当您的系统在高峰时段的利用率不超过 50% 时，以及当系统在高峰时段可以容纳新的写入和额外的 CPU 时，您可以使用内联压缩。仅当选择“启用压缩”时，此设置才可用。

- 启用自动增长

当可用空间百分比低于指定阈值时，只要关联聚合上有可用空间，您就可以自动增加目标卷。

- 最大尺寸

设置卷可以增长的最大百分比。默认值比源卷大小大 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。仅当启用自动增长设置时，此字段才可用。

- 增加尺寸

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。

- 舱位保证

确保在辅助卷上分配足够的空间，以便数据传输始终成功。空间保证设置可以是以下之一：

- 文件
- 卷
- 无 + 例如，您可能有一个 200 GB 的卷，其中包含总计 50 GB 的文件；但是，这些文件仅包含 10 GB 的数据。无论源卷上的内容如何，卷保证都会为目标卷分配 200 GB。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的文件数据实际使用的空间分配 10 GB。

空间保证默认设置为卷。

## 命令按钮

这些命令按钮可用来执行下列任务：

- 申请

保存选定的效率设置，并在单击“配置保护”对话框中的“应用”时应用这些设置。

- 取消

放弃您的选择并关闭“高级目标设置”对话框。

## 高级目标卷设置对话框

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。当源上禁用空间保证但希望在目标上启用它时，您可能会选择高级设置。 SnapMirror关系中的重复数据删除、压缩和自动增长设置从源卷继承，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。空间保证设置可以是以下之一：

- 文件
- 卷
- 无

例如，您可能有一个 200 GB 的卷，其中包含总计 50 GB 的文件；但是，这些文件仅包含 10 GB 的数据。无论源卷上的内容如何，卷保证都会为目标卷分配 200 GB。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实际使用的空间分配 10 GB。

空间保证默认设置为卷。

## 还原对话框

您可以使用“还原”对话框将数据从特定的 Snapshot 副本还原到卷。

### 还原自

“恢复自”区域可让您指定要从哪里恢复数据。

- 体积

指定要从中恢复数据的卷。默认情况下，选择您启动还原操作的卷。您可以从下拉列表中选择不同的卷，该列表包含与您启动还原操作的卷具有保护关系的所有卷。

- 快照副本

指定要使用哪个 Snapshot 副本来还原数据。默认情况下，选择最新的 Snapshot 副本。您还可以从下拉列表中选择不同的 Snapshot 副本。Snapshot 副本列表根据所选卷而变化。

- 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。如果您想查看选定卷内的所有对象，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。

### 选择要恢复的项目

通过“选择要还原的项目”区域，您可以选择要还原的整个卷或特定文件和文件夹。您最多可以选择 10 个文件、文件夹或两者的组合。当选择了最大项目数时，项目选择复选框将被禁用。

- 路径字段

显示要恢复的数据的路径。您可以导航到要恢复的文件夹和文件，也可以键入路径。在您选择或输入路径之前，此字段为空。点击  选择路径后，您将在目录结构中向上移动一级。

- 文件夹和文件列表

显示您输入的路径的内容。默认情况下，首先显示根文件夹。单击文件夹名称即可显示该文件夹的内容。

您可以按如下方式选择要恢复的项目：

- 当您在路径字段中输入具有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。

- 当您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，并且您最多可以选择 10 个文件、文件夹或两者的组合进行还原。

如果文件夹包含超过 995 个项目，则会显示一条消息，指示项目太多而无法显示，如果继续执行该操作，则会恢复指定文件夹中的所有项目。如果您想查看所选卷内的所有对象，可以取消选中“列出最多 995 个文件和目录”复选框。



您不能还原 NTFS 文件流。

#### 还原至

恢复至区域可让您指定要恢复数据的位置。

- **Volume\_Name** 中的原始位置

将选定的数据还原到最初备份数据的源目录中。

- 备用地点

将选定的数据恢复到新位置：

- 恢复路径

指定用于恢复选定数据的备用路径。该路径必须已经存在。您可以使用\*浏览\*按钮导航到要恢复数据的位置，也可以使用格式 `cluster://svm/volume/path` 手动输入路径。

- 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 将使用目标上的以下目录结构恢复数据：`/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

放弃您的选择并关闭“还原”对话框。

- 恢复

应用您的选择并开始恢复过程。

#### 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。

- 簇

列出可以恢复到的可用集群目标。默认情况下，选择原始源卷的集群。

- **SVM** 下拉列表

列出选定集群可用的 SVM。默认情况下，选择原始源卷的 SVM。

- 体积

列出选定 SVM 中的所有读/写卷。您可以按名称和可用空间过滤卷。具有最大空间的卷将首先列出，依此类推，按降序排列。默认情况下，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经存在。

- 姓名

显示选定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（如果存在）。文件夹中包含的文件不会显示。单击  选择文件夹后，您将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。如果没有选择目录，则此按钮将被禁用。

- 取消

放弃您的选择并关闭“浏览目录”对话框。

#### 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

显示您正在创建的关系的视觉表示。拓扑中的源默认突出显示。

- 来源信息

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

显示所有选定源卷的总大小。

- 累计已用卷大小

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 Compliance、Enterprise 和 Non- SnapLock。

- 快照复制

显示用于基线传输的 Snapshot 副本。如果源卷是读/写的，则 Snapshot 副本列中的 Default 值表示默认创建一个新的 Snapshot 副本，并用于基线传输。如果源卷是数据保护卷，则 Snapshot 副本列中的值 Default 表示不会创建新的 Snapshot 副本，并且所有现有的 Snapshot 副本都将传输到目标。单击 Snapshot 副本值将显示 Snapshot 副本列表，您可以从中选择一个现有 Snapshot 副本用于基线传输。如果源类型是数据保护，则不能选择不同的默认 Snapshot 副本。

## SnapMirror选项卡

使您能够在创建SnapMirror关系时指定保护关系的目标集群、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视觉表示。拓扑中的SnapMirror目标资源默认突出显示。

- 目的地信息

使您能够选择保护关系的目标资源：

- 高级链接

创建SnapMirror关系时启动“高级目标设置”对话框。

- 集群

列出可作为保护目标主机的集群。此字段是必需的。

- 存储虚拟机 (SVM)

列出选定集群上可用的 SVM。必须先选择一个集群，然后才能填充 SVM 列表。此字段是必需的。

- 聚合

列出选定 SVM 上可用的聚合。必须先选择一个集群，然后才能填充聚合列表。此字段是必需的。汇总表显示以下信息：

- 排名

当多个聚合满足目标的所有要求时，排名表示聚合列出的优先级，根据以下条件：

- A. 最好使用与源卷节点位于不同节点上的聚合来实现故障域分离。
    - B. 优先选择具有较少卷的节点上的聚合，以便在集群中的节点之间实现负载平衡。
    - C. 为了实现容量平衡，优先选择比其他聚合具有更多可用空间的聚合。排名为 1 表示根据这三个标准，该集合是最受欢迎的。

- 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。您可以接受提供的命名约定，也可以创建自定义的命名约定。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，则命名约定字段将以红色突出显示。单击“预览名称”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，会在目标名称后附加 001 至 999 之间的后缀，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。如果您选择不使用最大转移率，则关系之间的基线转移是无限限制的。

- SnapMirror 策略

指定该关系的ONTAP SnapMirror策略。默认值为 DPDefault。

- 创建策略

启动“创建SnapMirror策略”对话框，在此可以创建和使用新的SnapMirror策略。

- SnapMirror 计划

指定该关系的ONTAP SnapMirror策略。可用的时间表包括无、5 分钟、8 小时、每天、每小时和每周。默认值为 None，表示没有与该关系关联的计划。没有时间表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，在此可以创建新的SnapMirror计划。

## SnapVault选项卡

使您能够在创建SnapVault关系时指定保护关系的二级集群、SVM 和聚合，以及二级卷的命名约定。您还可以指定SnapVault策略和计划。

- 拓扑视图

显示您正在创建的关系的视觉表示。拓扑中的SnapVault二级资源默认突出显示。

- 次要信息

使您能够选择保护关系的辅助资源：

- 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集群。此字段是必需的。

- 存储虚拟机 (SVM)

列出选定集群上可用的 SVM。必须先选择一个集群，然后才能填充 SVM 列表。此字段是必需的。

- 聚合

列出选定 SVM 上可用的聚合。必须先选择一个集群，然后才能填充聚合列表。此字段是必需的。汇总表显示以下信息：

- 排名

当多个聚合满足目标的所有要求时，排名表示聚合列出的优先级，根据以下条件：

- A. 最好使用与主卷节点位于不同节点上的聚合来实现故障域分离。
- B. 优先选择具有较少卷的节点上的聚合，以便在集群中的节点之间实现负载平衡。
- C. 为了实现容量平衡，优先选择比其他聚合具有更多可用空间的聚合。排名为 1 表示根据这三个标



准，该集合是最受欢迎的。

- 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，也可以创建自定义的命名约定。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，则命名约定字段将以红色突出显示。单击“预览名称”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。如果输入无效值，无效信息将在预览区域中显示为红色问号。创建关系时，会在辅助名称后附加 001 至 999 之间的后缀，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。如果您选择不使用最大转移率，则关系之间的基线转移是无限制的。

- SnapVault策略

指定该关系的ONTAP SnapVault策略。默认值为 XDPDefault。

- 创建策略

启动“创建SnapVault策略”对话框，您可以创建并使用新的SnapVault策略。

- SnapVault计划

指定关系的ONTAP SnapVault计划。可用的时间表包括无、5 分钟、8 小时、每天、每小时和每周。默认值为 None，表示没有与该关系关联的计划。没有时间表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，在此可以创建SnapVault计划。

## 命令按钮

这些命令按钮可用来执行下列任务：

- 取消

放弃您的选择，并关闭“配置保护”对话框。

- 申请

应用您的选择并开始保护过程。

## 创建计划对话框

使用“创建计划”对话框可以为SnapMirror和SnapVault关系传输创建基本或高级保护计划。您可以创建一个新的计划来增加数据传输的频率（因为数据更新频繁），或者当数据不频繁更改时，您可以创建一个不太频繁的计划。

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的名称。

- 日程表名称

您为计划提供的名称。计划名称可以由字符 A 到 Z、a 到 z、0 到 9 以及以下任何特殊字符组成：! @#\$%{插入符号}&\*()\_。计划名称不得包含以下字符：< >。

- 基础版或高级版

您想要使用的计划模式。

基本模式包含以下元素：

- 重复

预定的转移发生的频率。选择包括每小时、每天和每周。

- 天

当选择每周重复时，传输将在星期几发生。

- 时间

当选择每日或每周时，传输发生的时间是一天中的时间。

高级模式包括以下内容：

- 个月

以逗号分隔的数字列表，代表一年中的月份。有效值为 0 到 11，其中零代表一月，依此类推。此元素是

可选的。将此字段留空表示每月都会发生转账。

- 天

以逗号分隔的数字列表，表示月份中的日期。有效值为 1 至 31。此元素是可选的。将该字段留空意味着每月每天都会发生转账。

- 工作日

以逗号分隔的数字列表，表示一周中的每一天。有效值为 0 到 6，其中 0 代表星期日，依此类推。此元素是可选的。将该字段留空意味着每周每天都会发生转账。如果指定了星期几，但未指定月份中的某天，则转移仅在指定的星期几发生，而不是每天发生。

- 小时

以逗号分隔的数字列表，表示一天的小时数。有效值为 0 到 23，其中 0 代表午夜。此元素是可选的。

- 分钟

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。

## 创建 **SnapMirror** 策略对话框

通过“创建SnapMirror策略”对话框，您可以创建策略来设置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标的传输效率。

- 目标集群

您在“配置保护”对话框的SnapMirror选项卡中选择的集群的名称。

- 目标 **SVM**

您在“配置保护”对话框的SnapMirror选项卡中选择的 SVM 的名称。

- 政策名称

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。

- 转移优先权

传输对于异步操作的运行优先级。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先于具有指定低传输优先级的策略的传输关系运行。

- 评论

可选字段，您可以在其中添加有关该政策的评论。

- 重新开始传输

指示当传输因中止操作或任何类型的故障（例如网络中断）而中断时要采取的重新启动操作。您可以选择以下选项之一：

- 总是

指定在重新开始传输之前创建一个新的 Snapshot 副本，然后（如果存在）从检查点重新开始传输，接着从新创建的 Snapshot 副本进行增量传输。

- 从不

指定中断的传输永远不会重新启动。

#### 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。

- 申请

应用您的选择并开始保护过程。

#### 创建 SnapVault 策略对话框

通过“创建SnapVault策略”对话框，您可以创建策略来设置SnapVault传输的优先级。您可以使用策略来最大程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的名称。

- 目标 **SVM**

您在“配置保护”对话框的SnapVault选项卡中选择的 SVM 的名称。

- 政策名称

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。

- 转移优先权

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的策略的传输关系先于具有指定低传输优先级的策略的传输关系运行。默认设置为正常。

- 评论

可选字段，您可以在其中添加有关SnapVault策略的最多 255 个字符的注释。

- 忽略访问时间

指定是否忽略仅访问时间发生变化的文件的增量传输。

- 复制标签

在表中列出与ONTAP选择的在策略中具有特定复制标签的 Snapshot 副本关联的规则。还可以提供以下信息和操作：

- 命令按钮

命令按钮使您能够执行以下操作：

- 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。保留计数必须是 1 到 251 之间的数字。所有规则的保留计数总和不能超过 251。

- 删除

使您能够删除现有的 Snapshot 副本标签。

- Snapshot 副本标签

显示 Snapshot 副本标签。如果您选择一个或多个具有相同本地 Snapshot 副本策略的卷，则会显示该策略中每个标签的条目。如果您选择具有两个或更多本地 Snapshot 副本策略的多个卷，则该表将显示所有策略的所有标签

- 计划

显示与每个 Snapshot 副本标签关联的计划。如果某个标签关联有多个计划，则该标签的计划将显示在以逗号分隔的列表中。如果选择具有相同标签但具有不同计划的多个卷，则计划将显示“各种”以指示有多个计划与所选卷相关联。

- 目标保留数量

显示保留在SnapVault辅助节点上的具有指定标签的 Snapshot 副本的数量。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。如果您选择具有两个或更多本地 Snapshot 副本策略的多个卷，则保留计数为空。

## 编辑关系对话框

您可以编辑现有的保护关系来更改最大传输速率、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

指定基线数据通过网络在集群之间传输的最大速率。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，然后选择每秒千字节 (KBps)、每秒兆字节 (MBps)、每秒千兆字节 (GBps) 或每秒太字节 (TBps)。您指定的最大传输速率必须大于 1 KBps 且小于 4 TBps。如果您选择不使用最大转移率，则关系之间的基线转移是无限制的。如果主集群和辅助集群相同，则此设置被禁用。

- SnapMirror 策略

指定该关系的ONTAP SnapMirror策略。默认值为 DPDefault。

- 创建策略

启动“创建SnapMirror策略”对话框，在此可以创建和使用新的SnapMirror策略。

- SnapMirror 计划

指定该关系的ONTAP SnapMirror策略。可用的时间表包括无、5 分钟、8 小时、每天、每小时和每周。默认值为 None，表示没有与该关系关联的计划。没有时间表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，在此可以创建新的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。

## 初始化/更新对话框

初始化/更新对话框使您能够对新的保护关系执行首次基线传输，或者在关系已经初始化并且您想要执行手动、非计划、增量更新的情况下更新关系。

## 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。

- 转移优先权

传输运行的优先级。您可以选择正常或低。指定正常传输优先级的策略关系在指定低传输优先级的策略关系之前运行。默认选择“正常”。

- 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。如果您选择不使用最大转移率，则关系之间的基线转移是无限制的。如果选择具有不同最大传输速率的多个关系，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

选择后，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。仅当初始化或更新具有不同传输速率的多个关系时，此字段才可用。

- 无限制

表示关系之间的传输没有带宽限制。仅当初始化或更新具有不同传输速率的多个关系时，此字段才可用。

- 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，然后选择每秒千字节 (KBps)、每秒兆字节 (MBps)、每秒千兆字节 (GBps) 或每秒太字节 (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。

- 目标音量

显示选定目标卷的名称。

- 来源类型

显示卷类型。类型可以是读/写或数据保护。

- 快照副本

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，您可以在其中根据您拥有的保护关系类型和正在执行的操作选择要传输的特定 Snapshot 副本。对于数据保护类型源，指定不同 Snapshot 副本的选项不可用。

## 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

保存您的选择并开始初始化或更新作业。

## 重新同步对话框

通过重新同步对话框，您可以重新同步之前已断开且随后目标变为读/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，您可能还需要重新同步。

## 重新同步选项选项卡

通过“重新同步选项”选项卡，您可以设置正在重新同步的保护关系的传输优先级和最大传输速率。

- 转移优先权

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的策略的关系先于具有指定低传输优先级的策略的关系运行。

- 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，然后选择每秒千字节 (KBps)、每秒兆字节 (MBps)、每秒千兆字节 (GBps) 或 TBps。如果您选择不使用最大转移率，则关系之间的基线转移是无限制的。

## 源 Snapshot 副本选项卡

“源 Snapshot 副本”选项卡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。

- 目标音量

显示选定目标卷的名称。

- 来源类型

显示卷类型：读/写或数据保护。

- 快照副本

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，您可以在其中根据您拥有的保护关系类型和正在执行的操作选择要传输的特定 Snapshot 副本。



## 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

取消您的选择并关闭“重新同步”对话框。

## 选择源 **Snapshot** 副本对话框

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**SnapMirror**还是**SnapVault**。

### 默认

使您能够选择默认行为来确定使用哪个 **Snapshot** 副本来初始化、更新和重新同步**SnapVault**和**SnapMirror**关系的传输。

如果您正在执行**SnapVault**传输，则每个操作的默认行为如下：

| 操作   | 源为读/写时的默认 <b>SnapVault</b> 行为                              | 源为数据保护 (DP) 时的默认 <b>SnapVault</b> 行为 |
|------|------------------------------------------------------------|--------------------------------------|
| 初始化  | 创建新的 <b>Snapshot</b> 副本并传输它。                               | 传输最后导出的 <b>Snapshot</b> 副本。          |
| 更新   | 仅传输策略中指定的标记的 <b>Snapshot</b> 副本。                           | 传输最后导出的 <b>Snapshot</b> 副本。          |
| 重新同步 | 传输在最新的通用 <b>Snapshot</b> 副本之后创建的所有带标签的 <b>Snapshot</b> 副本。 | 传输最新的标记 <b>Snapshot</b> 副本。          |

如果您正在执行**SnapMirror**传输，则每个操作的默认行为如下：

| 操作  | 默认 <b>SnapMirror</b> 行为                                                          | 当关系是 <b>SnapMirror</b> 到 <b>SnapMirror</b> 级联中的第二跳时，默认的 <b>SnapMirror</b> 行为 |
|-----|----------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| 初始化 | 创建新的 <b>Snapshot</b> 副本并传输该副本以及在该新 <b>Snapshot</b> 副本之前创建的所有 <b>Snapshot</b> 副本。 | 从源传输所有 <b>Snapshot</b> 副本。                                                   |
| 更新  | 创建新的 <b>Snapshot</b> 副本并传输该副本以及在该新 <b>Snapshot</b> 副本之前创建的所有 <b>Snapshot</b> 副本。 | 传输所有 <b>Snapshot</b> 副本。                                                     |

|      |                                        |                                                                              |
|------|----------------------------------------|------------------------------------------------------------------------------|
| 操作   | 默认 <b>SnapMirror</b> 行为                | 当关系是 <b>SnapMirror</b> 到 <b>SnapMirror</b> 级联中的第二跳时，默认的 <b>SnapMirror</b> 行为 |
| 重新同步 | 创建新的 Snapshot 副本，然后从源传输所有 Snapshot 副本。 | 将所有 Snapshot 副本从二级卷传输到三级卷，并删除在创建最新通用 Snapshot 副本后添加的任何数据。                    |

#### 现有 Snapshot 副本

如果该操作允许选择 Snapshot 副本，则您可以从列表中选择现有的 Snapshot 副本。

- 快照副本

显示现有的 Snapshot 副本，您可以从中选择要传输的副本。

- 创建日期

显示创建 Snapshot 副本的日期和时间。快照副本按从最新到最早的顺序列出，最新的副本位于列表顶部。

如果您正在执行SnapVault传输，并且想要选择一个现有的 Snapshot 副本从源传输到目标，则每个操作的行为如下：

| 操作   | 指定 <b>Snapshot</b> 副本时的 <b>SnapVault</b> 行为 | 在级联中指定 <b>Snapshot</b> 副本时的 <b>SnapVault</b> 行为 |
|------|---------------------------------------------|-------------------------------------------------|
| 初始化  | 传输指定的 Snapshot 副本。                          | 数据保护卷不支持源 Snapshot 副本选择。                        |
| 更新   | 传输指定的 Snapshot 副本。                          | 数据保护卷不支持源 Snapshot 副本选择。                        |
| 重新同步 | 传输选定的 Snapshot 副本。                          | 数据保护卷不支持源 Snapshot 副本选择。                        |

如果您正在执行SnapMirror传输，并且想要选择一个现有的 Snapshot 副本从源传输到目标，则每个操作的行为如下：

| 操作  | 指定 <b>Snapshot</b> 副本时的 <b>SnapMirror</b> 行为 | 在级联中指定 <b>Snapshot</b> 副本时的 <b>SnapMirror</b> 行为 |
|-----|----------------------------------------------|--------------------------------------------------|
| 初始化 | 传输源上的所有 Snapshot 副本，直至指定的 Snapshot 副本。       | 数据保护卷不支持源 Snapshot 副本选择。                         |
| 更新  | 传输源上的所有 Snapshot 副本，直至指定的 Snapshot 副本。       | 数据保护卷不支持源 Snapshot 副本选择。                         |

| 操作   | 指定 <b>Snapshot</b> 副本时的 <b>SnapMirror</b> 行为                          | 在级联中指定 <b>Snapshot</b> 副本时的 <b>SnapMirror</b> 行为 |
|------|-----------------------------------------------------------------------|--------------------------------------------------|
| 重新同步 | 将所有 Snapshot 副本从源传输到选定的 Snapshot 副本，然后删除在创建最新的通用 Snapshot 副本后添加的任何数据。 | 数据保护卷不支持源 Snapshot 副本选择。                         |

#### 命令按钮

这些命令按钮可用来执行下列任务：

- 提交

提交您的选择并关闭“选择源 Snapshot 副本”对话框。

- 取消

放弃您的选择并关闭“选择源 Snapshot 副本”对话框。

#### 反向重新同步对话框

当由于源卷被禁用且目标变为读/写卷而导致保护关系中断时，反向重新同步可让您反转关系的方向，以便目标成为新的源，源成为新的目标。

当灾难导致保护关系中的源卷失效时，您可以使用目标卷将数据转换为读/写形式来提供数据，同时修复或更换源、更新源并重新建立关系。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

显示反向重新同步操作之前关系的源和目标。

- 源卷

反向重新同步操作之前源卷的名称和位置。

- 目标音量

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。

- 目标音量

反向重新同步操作后目标卷的名称和位置。

#### 命令按钮

命令按钮使您能够执行以下操作：

- 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。

#### 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，显示的报告包括卷和存储虚拟机的顶级保护关系。页面顶部的控件使您能够选择特定视图、执行搜索以定位特定对象、创建和应用过滤器以缩小显示数据的列表、添加/删除/重新排序页面上的列以及将页面上的数据导出为 .csv、.pdf 或 .xlsx 文件。在自定义此页面后，您可以将结果保存为一个自定义视图，然后为此数据制定报告计划，以便定期生成此报告并发送电子邮件。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虚拟机的保护关系。您可以使用\*过滤器\*选项仅查看选定的存储系统，例如仅卷或仅存储虚拟机。相同的报告显示在存储页面中，并且仅针对选定的存储实体。如果要查看卷或存储虚拟机关系，您可以访问 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 过滤器 中的 关系对象类型 选项仅过滤掉卷或存储虚拟机数据。

列出所有保护关系的关系页面具有目标集群的链接\*在系统管理器中查看\*，可让您在ONTAP系统管理器中查看相同的对象。

- 地位

显示保护关系的当前状态。

状态可以是错误 (❗)，警告 (⚠)，或确定 (✅)。

- 源存储虚拟机

显示源 SVM 的名称。您可以单击源 SVM 名称来查看有关此源 SVM 的更多详细信息。

如果集群上存在 SVM 但尚未添加到 Unified Manager 清单，或者 SVM 是在集群上次刷新后创建的，则此字段将为空。您必须确保 SVM 存在，或者在集群上执行重新发现以刷新资源列表。

- 来源

根据您的选择显示受保护的源卷或源存储虚拟机。您可以通过单击卷或存储虚拟机名称来查看有关源卷或存储虚拟机的更多详细信息。

如果消息 `Resource-key not discovered` 显示，这可能表明该卷存在于集群上，但尚未添加到 Unified Manager 库存中，或者该卷是在集群上次刷新后创建的。您必须确保卷存在，或者对集群执行重新发现以刷新资源列表。

- 目标存储虚拟机

显示目标 SVM 的名称。您可以单击目标 SVM 名称来查看有关此目标 SVM 的更多详细信息。

- 目的地

根据您的选择显示目标卷或存储虚拟机的名称。您可以通过单击相应的对象名称来查看有关目标卷或存储虚拟机的更多详细信息。

- 关系对象类型

显示关系中使用的对象类型，例如存储虚拟机、卷和一致性组。对于一致性关系中的对象，关系源和目标显示一致性组，单击它们将转到 LUN 页面查看关系。

- 政策

显示 SnapMirror 关系的保护策略的名称。您可以单击策略名称来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 ONTAP 在无法同步某个同步关系时执行的操作。如果与辅助卷同步失败，StrictSync 关系将限制对主卷的访问。如果与辅助服务器同步失败，同步关系不会限制对主服务器的访问。

- 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，滞后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。

- 组成关系

显示选定对象中是否有任何卷。

- 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
- 严格同步
- 同步
- 转移状态

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。

- 转移

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。

- 最后转接时长

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，因为传输应该是同时的。

- 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。

- 调解员

显示调解员状态。

- 不适用

如果集群不支持 SnapMirror 主动同步。

- 未配置

如果未配置，或者已配置但仅添加了目标集群而未在 Unified Manager 中添加源集群。

- 中介 IP 地址

如果已配置，则源集群和目标集群都会添加到 Unified Manager 中。

- 状态

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

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。

- 转移优先权

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。

- 日程

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。

- 源集群 **FQDN**

显示 SnapMirror 关系中的源集群的名称。

- 源节点

显示卷的 SnapMirror 关系的源节点名称链接的名称，并在对象为存储虚拟机或一致性组时显示 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，您可以查看并扩展这些一致性组的卷所属的 SnapMirror 主动同步关系的存储对象的保护。

当您单击节点数链接时，它会将您带到与该关系相关联的各个节点的节点页面。当节点数为 0 时，由于没有与关系关联的节点，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，并在对象为存储虚拟机或一致性组时显示 SnapMirror 关系节点计数链接。

当您单击节点数链接时，它会将您带到与该关系相关联的各个节点的节点页面。当节点数为 0 时，由于没有与关系关联的节点，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

- 存储虚拟机灾难恢复
- SnapMirror、存储虚拟机灾难恢复
- 一致性组
- SnapMirror，一致性组。

## 相关信息

- 有关 关系： **MetroCluster** 视图的信息，请参阅["监控MetroCluster配置"](#)。
- 有关\*关系：过去 1 个月转移状态\*视图的信息，请参阅["关系：最近 1 个月的转移状态视图"](#)。
- 有关“关系：所有关系”视图的信息，请参阅["关系：过去 1 个月的转移率视图"](#)。

## 关系：最近 1 个月的转移状态视图

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的卷和存储虚拟机在一段时间内的传输趋势。此页面还显示传输是否成功或失败。

页面顶部的控件可让您执行搜索以定位特定对象、创建和应用过滤器以缩小显示的数据列表、添加/删除/重新排序页面上的列以及将页面上的数据导出到 .csv， .pdf， 或者 .xlsx 文件。在自定义此页面后，您可以将结果保存为一个自定义视图，然后为此数据制定报告计划，以便定期生成此报告并发送电子邮件。您可以使用\*过滤器\*选项仅查看选定的存储系统，例如仅卷或仅存储虚拟机。相同的报告显示在存储页面中，并且仅针对选定的存储实体。例如，如果您想查看卷关系，您可以从 存储 > 存储虚拟机 > 关系：过去 1 个月的传输状态 菜单或 保护 > 关系 > 关系：过去 1 个月的传输状态 菜单访问存储虚拟机的关系：过去 1 个月的传输状态报告，然后使用 过滤器 仅查看卷的数据。

- 源卷

显示源卷名称。

- 目标音量

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。

- 转机开始时间

显示卷传输开始时间。

- 转移结束时间

显示卷传输结束时间。

- 转移时长

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）。

- 来源 **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，请参阅[“关系：所有关系视图”](#)。
- 有关 关系： **MetroCluster** 视图的信息，请参阅[“监控MetroCluster配置”](#)。
- 有关“关系：所有关系”视图的信息，请参阅[“关系：过去 1 个月的转移率视图”](#)。

## 关系：过去 1 个月的转移率视图

关系：过去 1 个月的传输率视图使您能够分析异步关系中每天传输的数据量。此页面还提供有关每日传输的详细信息以及完成卷和存储虚拟机的传输操作所需的时间。

页面顶部的控件使您能够执行搜索以定位特定对象、创建和应用过滤器以缩小显示数据的列表、添加/删除/重新排序页面上的列，以及将页面上的数据导出到 .csv、.pdf 或 .xlsx 文件。在自定义此页面后，您可以将结果保存为一个自定义视图，然后为此数据制定报告计划，以便定期生成此报告并发送电子邮件。例如，如果您想查看卷关系，您可以访问 存储 > 卷 > 关系：过去 1 个月的传输率 菜单或访问 保护 > 关系 > 关系：过去 1 个月的传输率 菜单，然后使用 过滤器 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）。

- 天

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，请参阅["监控MetroCluster配置"](#)。
- 有关\*关系：过去 1 个月转移状态\*视图的信息，请参阅["关系：最近 1 个月的转移状态视图"](#)。
- 有关“关系：所有关系”视图的信息，请参阅["关系：过去 1 个月的转移率视图"](#)

# 生成自定义报告

## 统一管理器报告

Active IQ Unified Manager（以前称为OnCommand Unified Manager）提供查看、自定义、下载和安排ONTAP存储系统报告的功能。报告可以提供有关存储系统容量、健康状况、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 版中已淘汰的先前报告引擎。

报告提供网络的不同视图，提供有关容量、健康、性能、安全性和保护数据的可操作情报。您可以通过显示、隐藏和重新排列列、过滤数据、排序数据和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，并将它们安排为定期报告以通过电子邮件分发。

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、分层过滤器、数据透视表和图表。当对生成的 Excel 报告满意时，您可以上传 Excel 文件以供每次安排和共享报告时使用。

除了从用户界面生成报告之外，您还可以使用以下附加方法从 Unified Manager 中提取运行状况、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 以返回您感兴趣的信息

从此版本的Active IQ Unified 管理器开始，对报告进行了以下增强：

- 根据配置的时间表发送报告电子邮件。即使您生成按需报告，您也会收到一封电子邮件。
- 报告的文件名和报告的元数据包括生成报告的主机名。即使任何人更改了文件名，您仍然可以通过此增强功能识别生成报告的主机名。

## 生成报告的接入点

您可以在 Unified Manager 中收集有关集群的信息，以便从 UI、MySQL 数据库查询和 REST API 创建报告。

这些部分描述了通过 UI 进行 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 中的库存页面提取数据。
- 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 以返回您想要查看的信息。

这些部分描述了通过 UI 进行 Unified Manager 报告和调度。

可访问 **Unified Manager** 数据库以进行自定义报告

Unified Manager 使用 MySQL 数据库来存储其正在监控的集群的数据。数据保存在 MySQL 数据库的不同架构中。

支持访问以下数据库的所有数据表：

| 数据库                | 描述                                          |
|--------------------|---------------------------------------------|
| netapp_model       | ONTAP 控制器上的对象数据。                            |
| netapp_model_view  | 有关ONTAP控制器上对象的数据，适用于报告工具消耗。                 |
| netapp_performance | 集群特定的性能计数器。                                 |
| ocum               | 统一管理器应用程序数据和信息，支持UI过滤、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   | 库存配置和容量相关数据的视图，适用于报告工具消耗。                   |
| opm                | 性能配置设置和阈值信息。                                |
| scalemonitor       | 有关 Unified Manager 应用程序健康和性能问题的数据。          |
| vmware_model       | NetApp存储上托管的数据存储区的 VMware 对象数据。             |
| vmware_model_view  | NetApp存储上托管的数据存储区的 VMware 对象数据视图，适用于报告工具使用。 |
| VMware性能           | NetApp存储上托管的数据存储区的 VMware 性能计数器数据。          |

报告用户（具有报告模式角色的数据库用户）能够访问这些表中的数据。该用户可以直接从 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，此用户无权访问任何包含用户数据或集群凭据信息的表。

可用于报告的 **Unified Manager REST API**

您可以使用 REST API 查看 Unified Manager 捕获的运行状况、容量、性能和安全信息，从而帮助管理集群。

REST API 通过 Swagger 网页公开。您可以访问 Swagger 网页来显示 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 帮助 按钮，然后选择 **API** 文档。有关 Unified Manager REST API 的信息，请参阅["Active IQ Unified Manager REST API 入门"](#)。

您必须具有操作员、存储管理员或应用程序管理员角色才能访问 REST API。

## 了解报告

报告显示有关存储、网络、服务质量和保护关系的详细信息，帮助您在问题发生之前识别并解决潜在问题。

自定义视图时，您可以使用唯一的名称保存它以供将来使用。您可以根据该视图安排报告定期运行并与他人共享。您还可以下载 Excel 中的视图以使用高级 Excel 功能对其进行自定义，然后将该文件上传回 Unified Manager。如果您使用该视图安排报告，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”页面管理所有已安排的报告。



您必须具有应用程序管理员或存储管理员角色才能管理报告。

您可以将报告下载为逗号分隔值 (CSV)、Excel 或 PDF 文件。

## 了解视图和报告关系

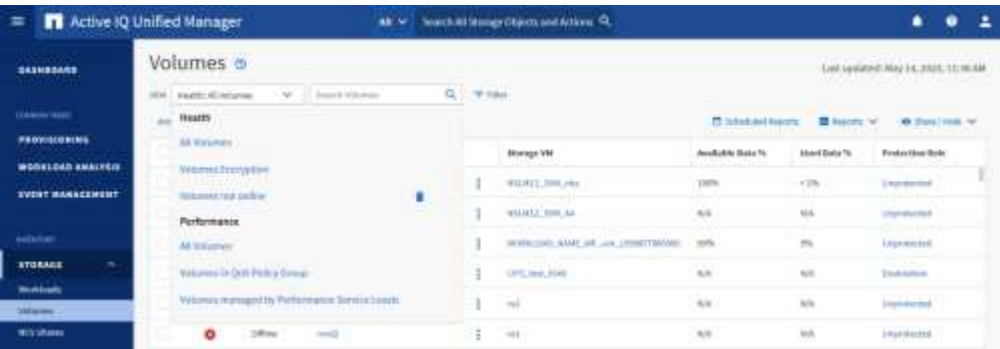
当您下载或安排视图和库存页面时，它们将成为报告。

您可以自定义和保存视图和库存页面以供重复使用。几乎您可以在 Unified Manager 中查看的所有内容都可以保存、重复使用、自定义、安排和共享为报告。

在视图下拉菜单中，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。默认视图不能被修改或删除。



- 如果从列表中删除自定义视图，则也会删除使用该视图的所有 Excel 文件或计划报告。
- 如果您更改自定义视图，则使用该视图的报告将在下次生成报告并根据报告计划通过电子邮件发送时反映更改。更改视图时，请确保您的更改与用于报告的任何相关 Excel 自定义兼容。如果需要，您可以下载 Excel 文件，进行必要的更改，然后将其作为视图的新 Excel 自定义上传，以更新该文件。



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。

报告类型

此表提供了可作为报告使用的视图和库存页面的综合列表，您可以自定义、下载和安排这些报告。

Active IQ Unified Manager报告

| 类型   | 存储或网络对象                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------|
| 容量   | 集群<br><br>聚合<br><br>卷<br><br>qtree                                                                        |
| 运行状况 | 集群<br><br>节点<br><br>聚合<br><br>Storage VM<br><br>卷<br><br>SMB/CIFS 共享<br><br>NFS 共享                        |
| 性能   | 集群<br><br>节点<br><br>聚合<br><br>Storage VM<br><br>卷<br><br>LUN<br><br>NVMe 命名空间<br><br>网络接口 (LIF)<br><br>端口 |



| 类型             | 存储或网络对象      |
|----------------|--------------|
| 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（可从卷页面获取） | 所有关系         |
|                | 最近 1 个月的转账状态 |
|                | 过去 1 个月的转账费率 |
| 安全性            | Storage VM   |
|                | 集群           |

## 报告限制

您应该注意，新的Active IQ Unified Manager报告功能存在一些限制。

### Unified Manager 先前版本的现有报告

您只能编辑在 Unified Manager 9.5 及更早版本中创建和导入（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，则这些自定义报告将不会导入到新的报告工具中。

如果您需要编辑从 .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安排报告（首选）
- 将鼠标悬停在报告上，复制 SQL，然后使用外部工具提取数据

默认视图可以生成为报告，无需任何定制。您可以使用新的报告解决方案来重新创建任何自定义报告。

### 日程与报告关系

您可以为每个已保存的报告创建许多不同的时间表，并可任意组合收件人。但是，您不能将该计划重复用于多个报告。

### 报告保护

任何具有适当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已保存的视图或时间表。

### 活动报告

虽然您可以自定义事件视图并以 CSV 格式下载生成的报告，但您无法安排重复事件报告的生成和分发。

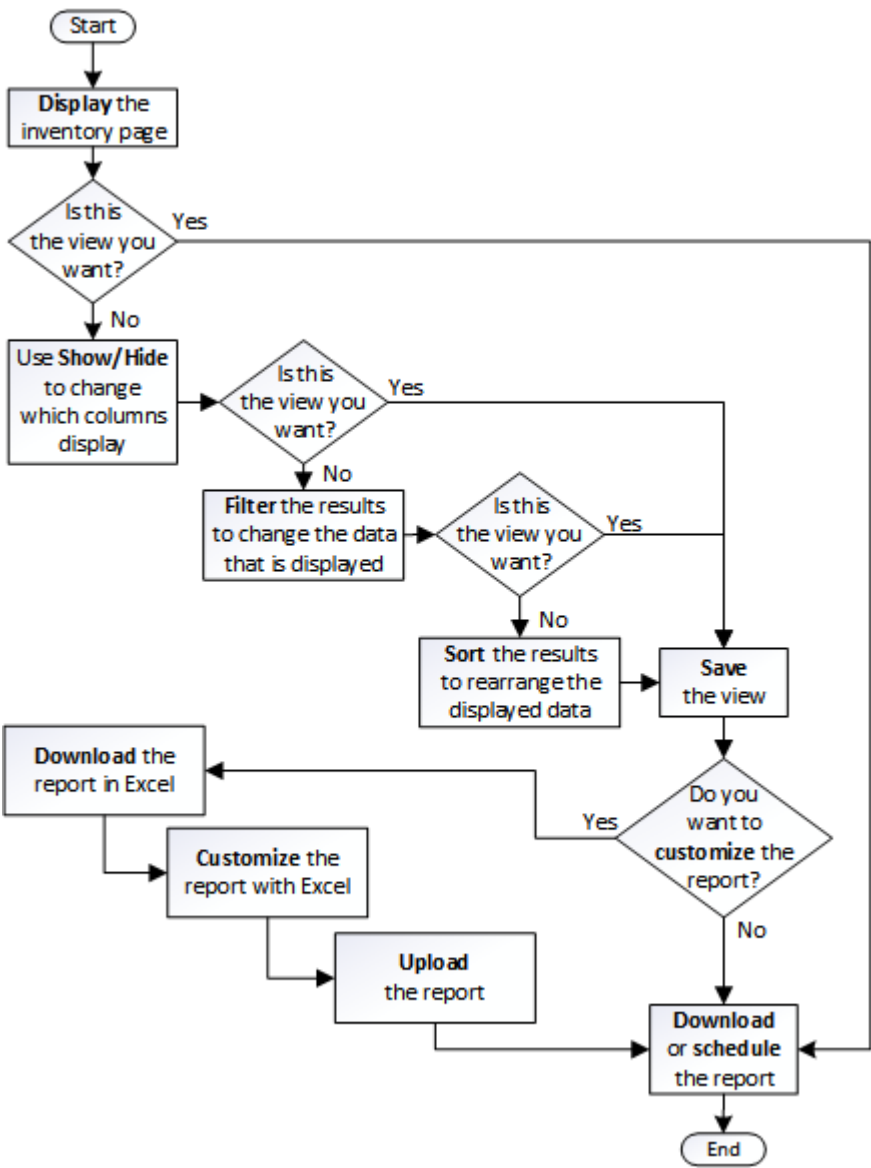
报告不能以电子邮件正文的形式发送。相反，报告仅以 PDF、Excel 或 CSV 附件的形式发送。

## 使用报告

了解如何查找库存页面视图并将其自定义为可共享的计划报告。

### 报告工作流程

描述报告工作流程的决策树。



### 报告快速入门

您可以创建一个示例自定义报告，以了解如何查看视图以及创建报告计划。此快速入门报告有助于您确定存在大量非活动（冷）数据的卷列表，这些卷可能需要移至云层。您将打

开“性能：所有卷”视图，使用过滤器和列自定义视图，将自定义视图保存为报告，并安排报告每周共享一次。

开始之前

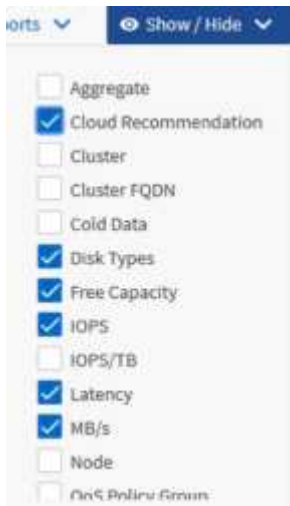
- 您必须具有应用程序管理员或存储管理员角色。
- 您必须事先已配置 FabricPool 聚合，并且这些聚合包含一些卷。

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“存储”>“卷”。
2. 在“查看”菜单中，选择“性能”>“所有卷”。
3. 单击“显示/隐藏”以确保“磁盘类型”列出现在视图中。



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“磁盘类型”列拖到“云推荐”列旁边。
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
  -

Filter

Disk Types contains fabricpool

Cloud Recommendation contains tier

Cold Data greater than 1 GB

+ Add Filter

Reset

Apply Filter

冷数据大于 10 GB

请注意，各个筛选器会通过逻辑“与”进行联接，以使返回的所有卷都符合所有条件。您最多可以添加五个过滤器。

- 单击“冷数据”列的顶部对结果进行排序，以便具有最多冷数据的卷出现在视图的顶部。
- 当视图自定义时，视图名称为未保存的视图。命名视图以反映视图所显示的内容，例如“Vols change tiering policy”。完成后，单击复选标记或按 **Enter** 以新名称保存视图。

Volumes - Performance / Vols change tiering policy Last updated: Feb 8, 2019, 12:26 PM

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View: Vols change tiering policy

| Volume     | Cold Data | Tiering Policy | Disk Types       | Cloud Recommendation | Free Capacity | Total Capacity |
|------------|-----------|----------------|------------------|----------------------|---------------|----------------|
| nfs_vol4   | 38 GB     | Snapshot Only  | SSD (FabricPool) | Tier                 | 2.62 TB       | 3 TB           |
| kjagntsdst | 28 GB     | Snapshot Only  | SSD (FabricPool) | Tier                 | 121 GB        | 150 GB         |

- 在安排或共享之前，将报告下载为 **CSV**、**Excel** 或 **PDF** 文件以查看输出。

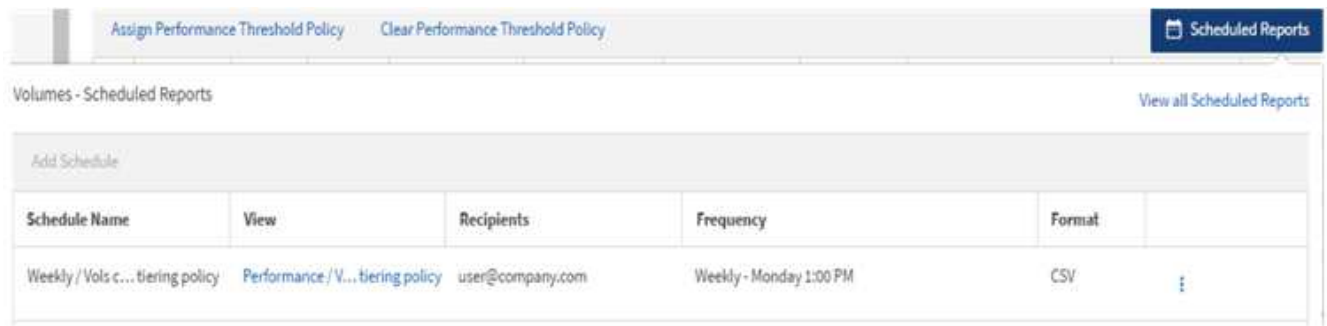
使用已安装的应用程序（例如 Microsoft Excel（CSV 或 Excel）或 Adobe Acrobat（PDF））打开文件，或保存文件。



您可以通过将视图下载为 Excel 文件，使用复杂的过滤器、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，此文件及其自定义内容将应用于视图。

有关使用 Excel 自定义报告的更多信息，请参阅 [\\_Microsoft Excel 报告示例\\_](#)。

- 单击库存页面上的“计划报告”按钮。此时会在列表中显示与此对象（此处为卷）相关的所有已计划报告。



10. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
11. 输入报告名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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：

|   | A                                                                                                                                                                    | B          | C         | D          | E         | F         | G          | H       | I          | J       | K       | L         | M            | N | O | P | Q |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------|------------|-----------|-----------|------------|---------|------------|---------|---------|-----------|--------------|---|---|---|---|
| 1 | Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:52 PM - March 28, 2019, 12:52 PM) |            |           |            |           |           |            |         |            |         |         |           |              |   |   |   |   |
| 2 | Generated At: March 28, 2019, 12:52 PM                                                                                                                               |            |           |            |           |           |            |         |            |         |         |           |              |   |   |   |   |
| 3 |                                                                                                                                                                      |            |           |            |           |           |            |         |            |         |         |           |              |   |   |   |   |
| 4 | Status                                                                                                                                                               | Volume     | Volume Id | Tiering Po | Cold Data | Free Capa | Total Capa | Cluster | Cluster Id | Node    | Node Id | Aggregate | Aggregate Id |   |   |   |   |
| 5 | Ok                                                                                                                                                                   | kjagnfsds1 | 101510    | Snapshot   | 28.01     | 121.32    | 150        | ocum-mo | 99001      | ocum-mo | 99018   | aggr5_vs  | 99040        |   |   |   |   |
| 6 | Ok                                                                                                                                                                   | nfs_vol4   | 102294    | Snapshot   | 379.64    | 2676.57   | 3072       | ocum-mo | 99001      | ocum-mo | 99113   | aggr4     | 99141        |   |   |   |   |

以下示例报告采用 PDF 格式：

| Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:51 PM - March 28, 2019, 12:51 PM) |            |                |                |                    |                     |         |         |           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------------|----------------|--------------------|---------------------|---------|---------|-----------|
| Generated At: March 28, 2019, 12:51 PM                                                                                                                               |            |                |                |                    |                     |         |         |           |
| Status                                                                                                                                                               | Volume     | Tiering Policy | Cold Data (GB) | Free Capacity (GB) | Total Capacity (GB) | Cluster | Node    | Aggregate |
| Ok                                                                                                                                                                   | kjagnfsds1 | Snapshot Data  | 28.01          | 121.32             | 150                 | ocum-mo | ocum-mo | aggr5_vs  |
| Ok                                                                                                                                                                   | nfs_vol4   | Snapshot Data  | 379.64         | 2676.57            | 3072                | ocum-mo | ocum-mo | aggr4     |

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“自动”或“全部”，以将更多冷数据卸载到云层。

## 搜索计划报告

您可以按名称、视图名称、对象类型或收件人搜索计划报告。

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。

| 要查找报告... | 尝试 ...                           |
|----------|----------------------------------|
| 计划名称     | 输入报告计划名称的一部分。                    |
| 视图名称     | 输入报告视图名称的一部分。默认视图和自定义视图出现在视图列表中。 |
| 接受者      | 输入部分电子邮件地址。                      |

|          |                       |
|----------|-----------------------|
| 要查找报告... | 尝试 ...                |
| 文件类型     | 输入“PDF”、“CSV”或“XLSX”。 |

- 您可以单击列标题，按该列的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

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。

从默认库存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、过滤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 中的视图以使用高级功能对其进行自定义。完成后，上传定制的 Excel 文件。如果您使用该视图安排报告，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 自定义报告的更多信息，请参阅 [\\_Microsoft Excel 报告示例\\_](#)。



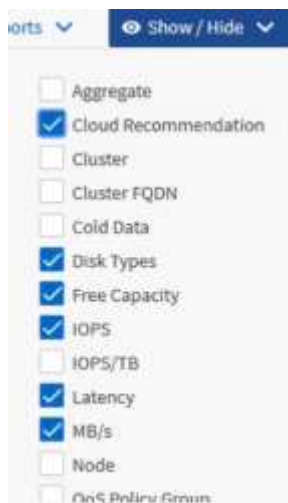
您必须具有应用程序管理员或存储管理员角色才能管理报告。

### 自定义列

使用\*显示/隐藏\*来选择您想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

- 单击“显示/隐藏”以添加或删除列。



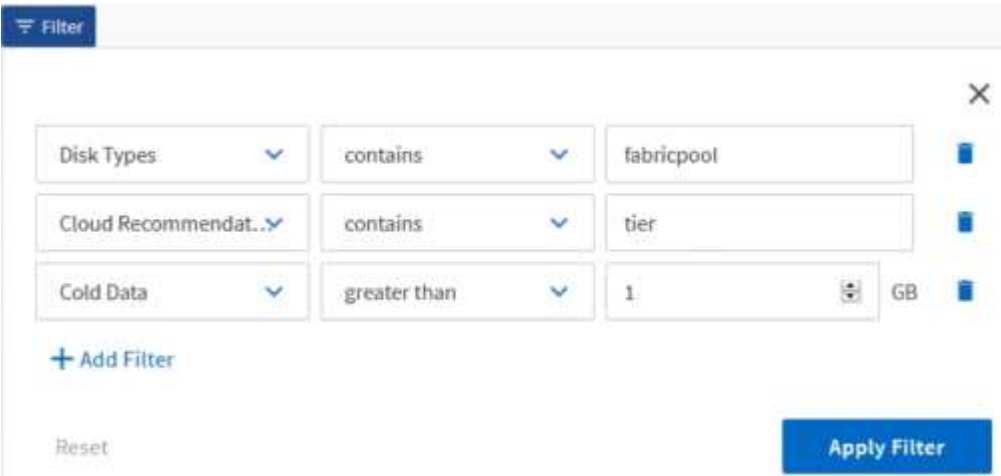
- 在库存页面上，拖动列以按照报告中所需的顺序重新排列它们。
- 命名未保存的视图以保存您的更改。

### 过滤数据

过滤数据以确保结果符合您的报告要求。通过过滤，您可以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聚焦您想要查看的结果，然后单击\*应用过滤器\*。



2. 命名未保存的视图以保存您的更改。

对数据进行排序

要对结果进行排序，请单击某一列并指示升序或降序。对数据进行排序可以确定报告所需信息的优先顺序。

步骤

1. 单击列的顶部对结果进行排序，以便最重要的信息显示在视图的顶部。
2. 命名未保存的视图以保存您的更改。

使用搜索来优化您的视图

获得所需的视图后，您可以使用搜索字段进一步优化结果，以关注要包含在报告中的结果。

步骤

1. 打开您想要用作报告基础的自定义或默认视图。
2. 在搜索字段中输入内容以优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，如果您想搜索名称中包含“US\_East”的节点，您可以优化完整的节点列表。

搜索结果将保存在自定义视图中并用于生成的计划报告中。

3. 命名未保存的视图以保存您的更改。

使用 **Excel** 自定义报告

保存视图后，您可以以 Excel 工作簿格式 (.xlsx) 下载它。打开 Excel 文件时，您可以使用高级 Excel 功能来自定义报告。

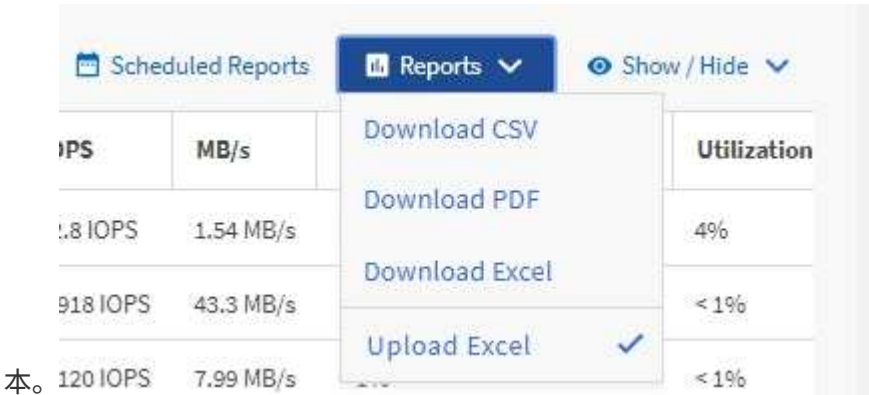
开始之前

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，而不是您保存的名称。
  - 格式为 <View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx.
  - 例如，名为 `Volumes-not online` 文件名为 `health-volumes-05-May-2020-19-18-00.xlsx` 如果在那天和那个时间保存。
- 您可以向 Excel 文件添加工作表，但不要更改现有工作表。
  - 不要更改现有的表格、数据和信息。相反，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“数据”页面上创建公式。使用数据页公式在新页面上创建图表。
  - 不要命名新表数据或信息。
- 如果存在自定义的 Excel 文件，则 报告 > 上传 **Excel** 菜单项旁边会有一个复选标记。下载 Excel 文件时，将使用具有自定义的版



步骤

1. 打开您想要用作报告基础的默认、自定义或已保存的视图。
2. 选择\*报告\* > 下载 **Excel**。
3. 保存文件。该文件已保存到您的下载文件夹。
4. 在 Excel 中打开保存的文件。请勿将文件移动到新位置，或者如果您在其他位置进行工作，请在上传文件之前使用原始文件名将文件保存回原始位置。
5. 使用 Excel 功能（例如复杂排序、分层过滤器、数据透视表或图表）自定义文件。有关更多信息，请参阅 Microsoft® Excel 文档。
6. 选择\*报告\* > \*上传 Excel\*并选择您修改的文件。最近下载的文件是从同一文件位置上传的。
7. 使用\*计划报告\*功能向自己发送测试报告。



## 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（例如 Microsoft Excel）打开 CSV 和 XLSX 文件，使用阅读器（例如 Adobe Acrobat）打开 PDF 文件。

### 步骤

1. 单击“报告”按钮可以下载以下报告之一：

| 选择       | 目的                                |
|----------|-----------------------------------|
| 下载 CSV   | 将报告保存为逗号分隔值 (CSV) 文件。             |
| 下载 PDF   | 将报告保存为 .pdf 文件。                   |
| 下载 Excel | 将报告保存为 Microsoft Excel (XLSX) 文件。 |

## 计划报告

在您拥有想要重复使用并作为报告共享的视图后，您可以使用Active IQ Unified Manager 来安排它。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 中安排大多数视图或库存页面。例外情况是事件，它们是您可以作为 CSV 文件下载的报告，但您无法安排事件进行重新生成和共享。您也无法下载或安排仪表盘、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、分层过滤器、数据透视表和图表。当对生成的 Excel 报告满意时，您可以上传 Excel 文件以供每次安排和共享报告时使用。

您可以安排内置视图或自定义视图。您可以选择要发送的文件类型，CSV、PDF 或 XSLX。当您第一次安排报告时，您可以下载该报告并将自己指定为唯一查看该报告的收件人，因为您的收件人将会看到它。

## 安排报告

在您拥有想要安排定期生成和分发的视图或 Excel 文件后，您可以安排报告。

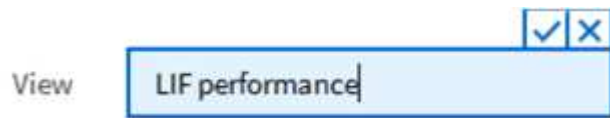
### 开始之前

- 您必须具有应用程序管理员或存储管理员角色。
- 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发送到 Unified Manager 服务器的收件人列表。
- 必须配置电子邮件服务器以允许附件与生成的电子邮件一起发送。

使用以下步骤测试并安排为视图生成的报告。选择或自定义您想要使用的视图。以下步骤使用网络视图来显示网络接口的性能，但您可以使用任何您想要的视图。

### 步骤

1. 開啟你的視野。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 的高级功能来自定义您的报告。有关详细信息，请参阅[使用 Excel 自定义报告](#)。
5. 要在安排或共享之前查看输出：

| 选项                         | 描述                                               |
|----------------------------|--------------------------------------------------|
| 如果您使用 <b>Excel</b> 自定义报告   | 查看现有的已下载的 Excel 文件。                              |
| 如果您没有使用 <b>Excel</b> 自定义报告 | 将报告下载为 <b>CSV</b> 、 <b>PDF</b> 或 <b>XLSX</b> 文件。 |

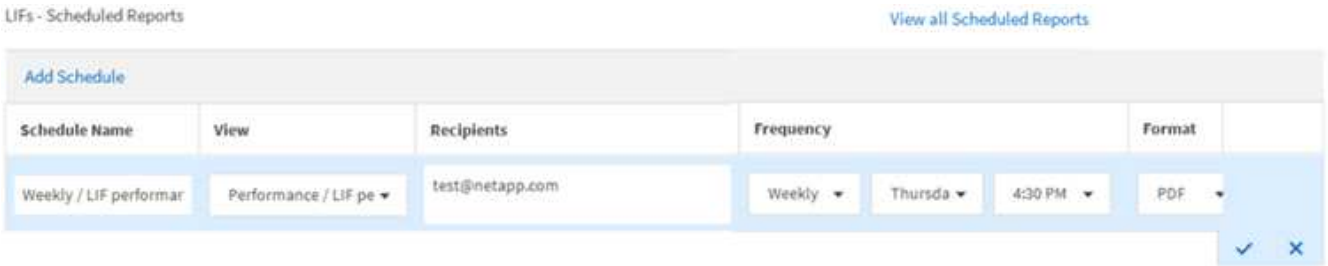
使用已安装的应用程序打开文件，例如 Microsoft Excel (CSV/XSLX) 或 Adobe Acrobat (PDF)。

6. 如果您对报告满意，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，即视图名称和频率的组合，或者自定义\*计划名称\*。
9. 要首次测试预定报告，只需将您自己添加为\*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，**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 (✓) 保存报表计划。



此时将立即发送一个测试报告。此后，将生成报告并按照预定频率通过电子邮件发送给列出的收件人。

### 安排导入 .rptdesign 报告

您可以安排在早期版本的 Unified Manager 中创建和导入的现有报告。

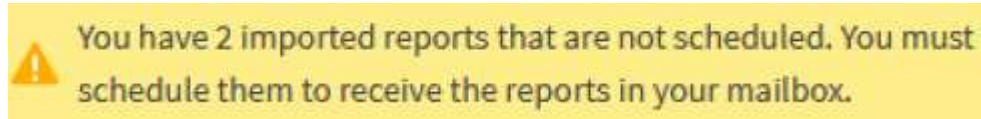
安排导入报告需要以下内容：

- 在早期的 Unified Manager 版本中导入 BIRT 设计的 .rptdesign 文件报告
- 适用于升级到 Unified Manager 9.6 GA 或更高版本

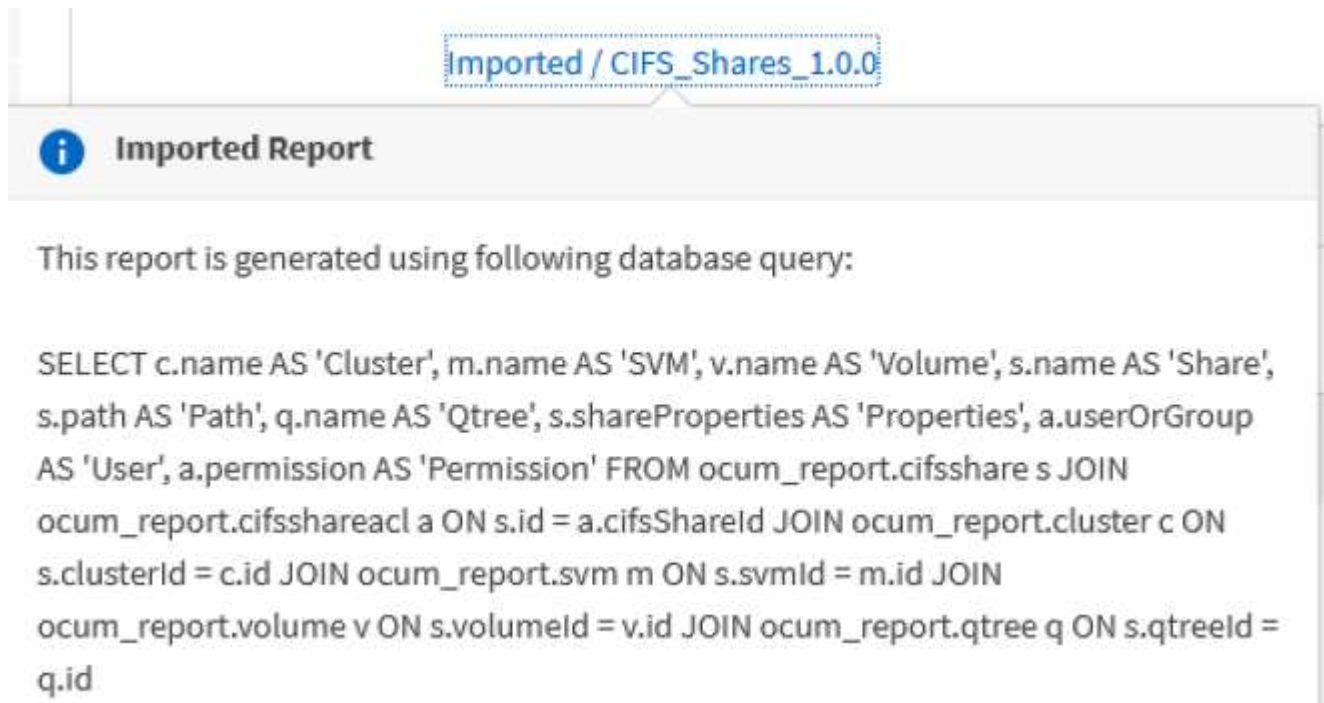
升级到 Unified Manager 9.6 GA 或更高版本后，“报告计划”页面会列出导入的报告。您可以编辑这些报告的时间表以指定收件人的电子邮件地址、频率和格式（PDF 或 CSV）。否则，这些报告无法在 Unified Manager UI 中编辑或查看。

#### 步骤

1. 打开报告计划页面。如果您已导入报告，则会出现一条消息。



2. 单击“查看”名称以显示用于生成报告的 SQL 查询。



3. 点击更多图标 ，点击\*编辑\*，定义报告计划详细信息，并保存报告。



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

您可以从“报告计划”页面管理您的报告计划。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。您只能从对象库存页面添加计划报告。

- 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                                                                                                                                                                                                                      |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 查看现有时间表 | 使用滚动条和页面控件滚动浏览现有报告列表。                                                                                                                                                                                                   |
| 编辑现有时间表 | <ol style="list-style-type: none"><li>a. 点击更多图标  您想要使用的时间表。</li><li>b. 单击“编辑”。</li><li>c. 做出必要的改变。</li><li>d. 单击复选标记以保存更改。</li></ol> |
| 删除现有计划  | <ol style="list-style-type: none"><li>a. 点击更多图标  您想要使用的时间表。</li><li>b. 单击“删除”。</li><li>c. 确认你的决定。</li></ol>                          |

编辑计划报告

报告安排完成后，您可以在“报告安排”页面上编辑它们。

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”。

Scheduled Reports 

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

 Search Scheduled Reports

| Schedule Name            | View                                          | Recipients      | Frequency                 | Format |                                                                                       |
|--------------------------|-----------------------------------------------|-----------------|---------------------------|--------|---------------------------------------------------------------------------------------|
| Weekly /Node performance | <a href="#">Performance / Tom_test</a>        | test@netapp.com | Weekly - Monday 5:30 PM   | PDF    |  |
| Weekly / my view         | <a href="#">Health / my view</a>              | test@netapp.com | Weekly - Friday 5:30 PM   | PDF    |  |
| Weekly / LIF performance | <a href="#">Performance / LIF performance</a> | test@netapp.com | Weekly - Thursday 4:30 PM | PDF    |  |



如果您拥有适当的权限，您可以更改系统中的任何报告及其时间表。

- 2.

点击更多图标  您想要更改的时间表。

- 3. 单击“编辑”。
- 4. 您可以更改报告计划的\*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更改。

删除计划报告

安排报告后，您可以从“报告安排”页面中删除它们。

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”。

Scheduled Reports 

View and modify existing report scheduling information. To add a new report and create a schedule for the report, click 'Schedule Report' from any Storage / Network inventory page.

 Search Scheduled Reports

| Schedule Name            | View                                          | Recipients      | Frequency                 | Format |                                                                                       |
|--------------------------|-----------------------------------------------|-----------------|---------------------------|--------|---------------------------------------------------------------------------------------|
| Weekly /Node performance | <a href="#">Performance / Tom_test</a>        | test@netapp.com | Weekly - Monday 5:30 PM   | PDF    |    |
| Weekly / my view         | <a href="#">Health / my view</a>              | test@netapp.com | Weekly - Friday 5:30 PM   | PDF    |  |
| Weekly / LIF performance | <a href="#">Performance / LIF performance</a> | test@netapp.com | Weekly - Thursday 4:30 PM | PDF    |  |



如果您拥有适当的权限，您可以删除系统中的任何报告及其时间表。

- 2. 点击更多图标  您想要删除的时间表。
- 3. 单击“删除”。
- 4. 确认你的决定。

预定的报告将从列表中删除，并且将不再按照设定的时间表生成和分发。



如果您从库存页面删除自定义视图，则使用该视图的任何自定义 Excel 文件或计划报告也将被删除。

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对潜在问题做出响应。

本节中的报告列表并不详尽，并且会随着时间的推移而增加。您可以通过提供文档反馈来建议将自定义报告添加到此部分。



您必须具有应用程序管理员或存储管理员角色才能管理报告。

## 自定义集群存储报告

本节中的示例集群存储报告仅仅是帮助您了解如何创建有关集群容量的报告以帮助您监控存储系统资源的示例。

### 创建报告以按集群模型查看容量

您可以创建报告来根据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。

使用以下步骤创建一个按集群模型显示容量的自定义视图，然后安排为该视图生成报告。

#### 步骤

1. 在左侧导航窗格中，单击“存储”>“集群”。
2. 在“查看”菜单中，选择“容量”>“所有集群”。
3. 选择“显示/隐藏”以删除您不想在报告中显示的任何列，例如“集群 FQDN”和“操作系统版本”。
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“模型/系列”列的顶部，按集群类型对结果进行排序。
6. 使用反映视图所显示内容的特定名称保存视图，例如“按集群模型划分的容量”。
7. 单击库存页面上的“计划报告”按钮。
8. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
9. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可能希望为某些集群添加更多容量，或者升级较旧的集群模型。

### 创建报告以识别未分配 LUN 容量最多的集群

您可以创建报告来查找未分配 LUN 容量最多（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。

使用以下步骤创建一个自定义视图，显示具有最多未分配 LUN 容量的集群，然后安排为该视图生成报告。

#### 步骤

1. 在左侧导航窗格中，单击“存储”>“集群”。

2. 在“查看”菜单中，选择“容量”>“所有集群”。
3. 选择“显示/隐藏”以删除报告中不需要的任何列。
4. 将“未分配的 LUN 容量”列拖到“HA 对”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，按未分配的 LUN 容量最大数量对结果进行排序。
7. 使用反映视图显示内容的特定名称保存视图，例如“Most unallocated LUN capacity”，然后单击复选标记 (✓)。
8. 单击库存页面上的“计划报告”按钮。
9. 单击“添加计划”以向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
10. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可能希望使用集群未分配的 LUN 容量。

创建报告以查看具有最多可用容量的 **HA 对**

您可以创建报告来查找具有最大容量的高可用性 (HA) 对，以配置新的卷和 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，该视图显示按最多可用容量排序的 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“查看”菜单中，选择“容量”>“所有集群”。
3. 选择“显示/隐藏”以删除报告中不需要的任何列。
4. 将“聚合未使用容量”列拖到“HA 对”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\*：
  - 未使用容量总计大于 0.5 TB
6. 单击“未使用总容量”列的顶部，按未使用总容量的最大数量对结果进行排序。
7. 使用反映视图显示内容的特定名称保存视图，例如“最少使用的聚合容量”，然后单击复选标记 (✓)。
8. 单击库存页面上的“计划报告”按钮。
9. 单击“添加计划”以向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
10. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可能希望根据总容量来平衡 HA 对。

创建报告以查看运行旧版本**ONTAP**的节点

您可以创建一个报告来显示所有集群节点上安装的ONTAP软件版本，以便您可以看到应该升级哪些节点。

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显示运行旧版本ONTAP的节点的自定义视图，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”>“节点”。
2. 选择“显示/隐藏”以删除报告中不需要的任何列。
3. 将“OS Version”列拖到“Node”列附近。
4. 单击“OS Version”列顶部，按ONTAP的最旧版本对结果进行排序。
5. 使用反映视图所显示内容的特定名称保存视图，例如“按ONTAP版本划分的节点”。
6. 单击库存页面上的“计划报告”按钮。
7. 单击“添加计划”以向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
8. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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旧版本ONTAP的节点。

## 自定义聚合容量报告

这些示例自定义报告用于帮助您识别和应对与聚合存储容量相关的潜在问题。

本节中的报告只是示例，旨在帮助您了解如何创建有关聚合容量的报告，以帮助您监控存储系统资源。

创建报告以查看达到满负荷的聚合

您可以创建报告来查找达到满容量的聚合，以便可以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。

使用以下步骤创建一个显示达到满容量的聚合的自定义视图，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“聚合”。
2. 在“查看”菜单中，选择“容量”>“所有聚合”。



3. 选择“显示/隐藏”以删除报告中不需要的任何列。
4. 单击过滤器图标，添加以下过滤器，然后单击\*应用过滤器\*：
  - 完成学业所需时间少于 45 天
5. 单击“达到满负荷天数”列的顶部，按达到满负荷所需的最少天数对结果进行排序。
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. 单击库存页面上的“计划报告”按钮。
8. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
9. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可能希望增加达到满容量的聚合存储。此外，您可能希望将“达到满容量所需的天数”阈值增加到默认的 7 天以上，以便接收有更多时间对空间聚合不足做出反应的事件。

创建报告以查看已满 **80%** 或以上的聚合

您可以创建报告来突出显示已满 **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，显示已满 80% 或以上的聚合，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“聚合”。
2. 在“查看”菜单中，选择“容量”>“所有聚合”。
3. 选择“显示/隐藏”以删除报告中不需要的任何列。
4. 将“可用数据 %”和“已使用数据 %”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\*：
  - 使用的数据百分比大于 80%
6. 单击“已用数据百分比”列的顶部，按容量百分比对结果进行排序。
7. 使用反映视图所显示内容的特定名称保存视图，例如“Aggregates nearing full”，然后单击复选标记 (✓)。
8. 单击库存页面上的“计划报告”按钮。
9. 单击“添加计划”以向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
10. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可能希望从某些聚合中移动一些数据。

创建报告以查看过度承诺的聚合

您可以创建报告来分析存储容量和聚合的使用情况，并查看过度使用的聚合。

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，显示超过过量提交阈值的聚合，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“聚合”。
2. 在“查看”菜单中，选择“容量”>“所有聚合”。
3. 选择“显示/隐藏”以删除报告中不需要的任何列。
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\*：
  - 超额承诺容量百分比大于 100%
6. 单击“超额承诺容量百分比”列的顶部，按容量百分比对结果进行排序。
7. 使用反映视图所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. 单击库存页面上的“计划报告”按钮。
9. 单击“添加计划”以向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
10. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可能希望向聚合添加更多容量，或者从某些聚合中移动一些数据。

## 自定义卷容量报告

这些示例自定义报告用于帮助您识别和响应与卷容量和性能相关的潜在问题。

创建报告以识别已关闭快照自动删除功能的接近满容量的卷

您可以创建一个报告，其中包含在禁用快照自动删除功能的情况下接近满容量的卷列表。结果可以帮助您识别可能想要配置快照自动删除的卷。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

按照以下步骤创建一个以正确顺序显示所需列的自定义视图，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“查看”菜单中，选择“容量”>“所有卷”。

3. 选择“显示/隐藏”以删除报告中不需要的任何列。
4. 将“快照自动删除”和“剩余天数”列拖放到“可用数据容量”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\*：
  - 满期天数少于 30 天
  - 快照自动删除已禁用
6. 单击“剩余天数”列的顶部，以便剩余天数最少的卷出现在列表顶部。
7. 使用反映视图所显示内容的特定名称保存视图，例如“Vols near capacity”。
8. 单击库存页面上的“计划报告”按钮。
9. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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快照自动删除或找到增加可用空间的方法。

创建报告以确定禁用精简配置的卷所使用的空间

当卷未进行精简配置时，它将占用创建卷时定义的磁盘上的全部空间。识别已禁用精简配置的卷有助于您决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。

按照以下步骤创建一个以正确顺序显示所需列的自定义视图，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“查看”菜单中，选择“容量”>“所有卷”。
3. 选择“显示/隐藏”以删除报告中不需要的任何列。
4. 将“已用数据百分比”和“精简配置”列拖放到“可用数据容量”列附近。
5. 单击过滤器图标，添加以下过滤器，**Thin provisioned** 为 **No**，然后单击 **Apply Filter**。
6. 单击“已使用数据百分比”列的顶部对结果进行排序，以便百分比最高的卷出现在列表顶部。
7. 使用名称保存视图以反映视图所显示的内容，例如“Vols no thin provisioning”。
8. 单击库存页面上的“计划报告”按钮。
9. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
10. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可能希望在某些卷上启用精简配置。

创建报告以识别**FabricPool**聚合上应将数据移动到云层的卷

您可以创建一个报告，其中包含当前驻留在FabricPool聚合上、具有 Tier 云建议且具有大量冷数据的卷列表。此报告可以帮助您决定是否应将某些卷的分层策略更改为“自动”或“全部”，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。

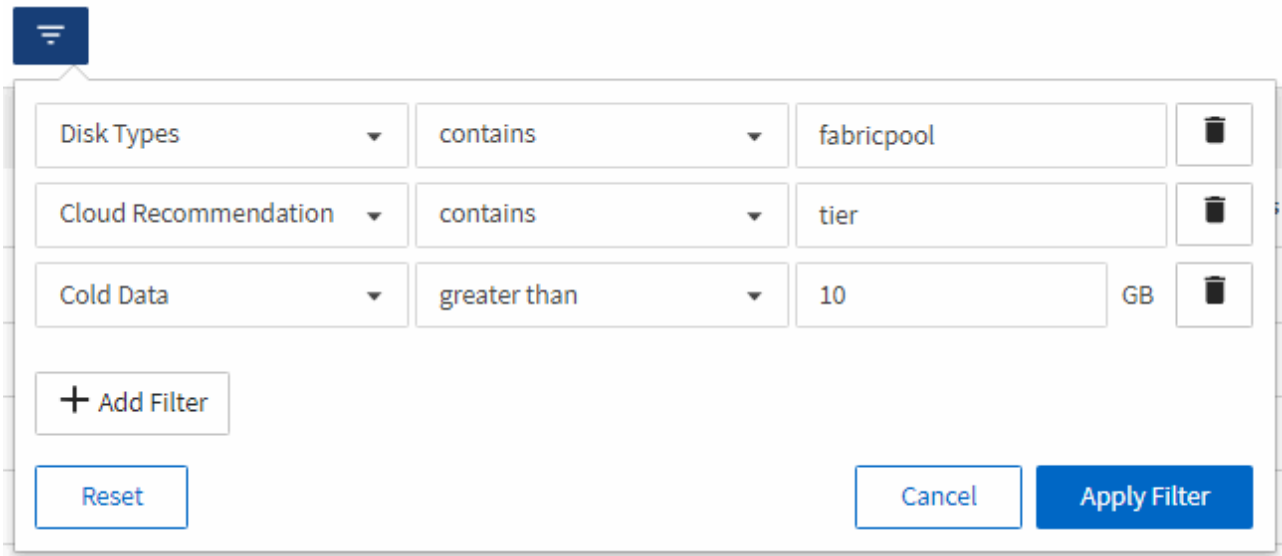
按照以下步骤创建一个以正确顺序显示所需列的自定义视图，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“查看”菜单中，选择“性能”>“所有卷”。
3. 在列选择器中，确保“磁盘类型”列出现在视图中。

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”列拖放到“云推荐”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，以便具有最多冷数据的卷出现在视图的顶部。
7. 使用名称保存视图以反映视图所显示的内容，例如“Vols change tiering policy”。

Latency, IOPS, MBps are based on hourly samples averaged over the previous 72 hours.

View
Vols change tiering policy
Search Volumes
3

| Assign Performance Threshold Policy |                                                                                         | Clear Performance Threshold Policy |                  | Schedule Report      |               |   |
|-------------------------------------|-----------------------------------------------------------------------------------------|------------------------------------|------------------|----------------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Volume                              | Cold Data                                                                               | Tiering Policy                     | Disk Types       | Cloud Recommendation | Free Capacity | Total Capacity                                                                                                                                                          |
| nfs_vol4                            | 38 GB  | Snapshot Only                      | SSD (FabricPool) | Tier                 | 2.62 TB       | 3 TB                                                                                                                                                                    |
| kjagnfsdst                          | 28 GB                                                                                   | Snapshot Only                      | SSD (FabricPool) | Tier                 | 121 GB        | 150 GB                                                                                                                                                                  |

- 单击库存页面上的“计划报告”按钮。
- 单击“添加计划”以向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
- 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可能需要使用系统管理器或ONTAP CLI 将某些卷的分层策略更改为“自动”或“全部”，以将更多冷数据传输到云层。

## 自定义 Qtree 容量报告

这些示例自定义报告用于帮助您识别和响应与 Qtree 容量相关的潜在问题。

创建报告以查看几乎已满的 **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。

使用以下步骤创建一个显示几乎已满的 **qtree** 的自定义视图，然后计划为该视图生成报告。

步骤

- 在左侧导航窗格中，单击“存储”>“Qtree”。
- 选择“显示/隐藏”以删除报告中不需要的任何列。
- 将“磁盘已用百分比”列拖到“Qtrees”列附近。
- 单击过滤器图标，添加以下过滤器，然后单击\*应用过滤器\*：
  - 磁盘使用率百分比大于 75%
- 单击“磁盘使用百分比”列的顶部，按容量百分比对结果进行排序。
- 使用反映视图所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 (✓)。
- 单击库存页面上的“计划报告”按钮。

8. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。

9. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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（如果设置），或在 qtree 之间平衡数据。

## 自定义 NFS 共享报告

您可以自定义 NFS 共享报告来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具有无法访问的安装路径的卷和具有默认导出策略的卷。

创建报告以查看具有无法访问的挂载路径的卷

您可以创建报告来查找具有无法访问的安装路径的卷。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤为具有不可访问的安装路径的卷创建自定义视图，然后安排为该视图生成报告。

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”以删除报告中不需要的任何列。
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“Volumes with an inaccessible mount path”，然后单击复选标记 (✓)。
5. 单击库存页面上的“计划报告”按钮。
6. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
7. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可能需要纠正无法访问的挂载路径。

创建报告以查看使用默认导出策略的卷

您可以创建报告来查找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”以删除报告中不需要的任何列。
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
5. 使用反映视图显示内容的特定名称保存视图，例如“具有默认导出策略的卷”，然后单击复选标记 (✓)。
6. 单击库存页面上的“计划报告”按钮。
7. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
8. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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。

## 自定义存储虚拟机报告

您可以创建存储虚拟机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数的 SVM 并分析已停止的 SVM。

创建报告以查看达到最大卷限制的存储虚拟机

您可以创建报告来查找达到最大容量限制的 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。

使用以下步骤创建一个自定义视图，显示达到最大卷限制的存储虚拟机，然后安排为该视图生成报告。

## 步骤

1. 在左侧导航窗格中，单击“存储”>“存储虚拟机”。
2. 选择“显示/隐藏”以删除报告中不需要的任何列。
3. 将“卷数”和“最大允许卷”列拖到“存储虚拟机”列附近。
4. 单击“允许的最大卷”列的顶部，按卷数最多对结果进行排序。
5. 使用反映视图所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. 单击库存页面上的“计划报告”按钮。
7. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
8. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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虚拟机的卷，或者如果可能，使用ONTAP系统管理器更改



允许的最大卷数。

创建报告以查看已停止的存储虚拟机

您可以创建报告来显示所有已停止的 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虚拟机的自定义视图，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“存储虚拟机”。
2. 在“查看”菜单中，选择“健康”>“所有存储虚拟机”。
3. 选择“显示/隐藏”以删除报告中不需要的任何列。
4. 将“状态”列拖到“存储 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“Stopped SVM”，然后单击复选标记 (✓)。
7. 单击库存页面上的“计划报告”按钮。
8. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。
9. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，以确定是否应该重新启动已停止的 SVM。

## 自定义数量关系报告

通过卷关系库存报告，您可以分析集群中的存储库存详细信息，了解卷所需的保护程度，并根据故障源、模式和计划过滤卷详细信息。

创建报告以按故障源对卷关系进行分组

您可以创建一个报告，根据关系处于不健康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，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“查看”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”列出现在视图中。

添加或删除其他列以创建对您的报告很重要的视图。

4. 将“关系健康”和“不健康原因”列拖到“状态”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\*：
  - 关系健康状况不佳
6. 单击“不健康原因”列的顶部，按故障源对卷关系进行分组。
7. 使用反映视图所显示内容的特定名称保存视图，例如“Vol relationships by failure”。
8. 单击库存页面上的“计划报告”按钮。
9. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可以调查每种故障的来源和影响。

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。

使用以下步骤创建按问题对卷关系进行分组的自定义视图，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“查看”菜单中，选择“关系”>“所有关系”。
3. 选择“显示/隐藏”以删除报告中不需要的任何列。
4. 将“不健康原因”列拖到“状态”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. 使用反映视图所显示内容的特定名称保存视图，例如“Vol relationships by issue”。
7. 单击库存页面上的“计划报告”按钮。
8. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可以调查每种问题的来源和影响。

创建报告以查看特定时间间隔的传输量趋势

您可以创建一个报告来显示特定时间间隔内的传输量趋势。

## 开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤为特定时间间隔的卷创建自定义视图，然后安排为该视图生成报告。

## 步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“查看”菜单中，选择“关系”>“过去 1 个月的转移状态”。
3. 选择“显示/隐藏”以删除报告中不需要的任何列。
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 天内的转移结束时间
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. 使用反映视图所显示内容的特定名称保存视图，例如“按持续时间划分的卷”。
8. 单击库存页面上的“计划报告”按钮。
9. 输入报告计划的名称，将频率设置为\*每周\*，并完成其他报告字段，然后单击复选标记 (✓) 位于行尾。

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。

## 创建报告以查看失败或成功的卷传输

您可以创建一个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来显示哪些传输失败以及哪些传输成功，然后安排为该视图生成报告。

## 步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“查看”菜单中，选择“关系”>“过去 1 个月的转移状态”。
3. 选择“显示/隐藏”以删除报告中不需要的任何列。
4. 将“操作结果”列拖到“状态”列附近。
5. 单击“操作结果”列的顶部，按状态对卷进行排序。
6. 使用反映视图所显示内容的特定名称保存视图，例如“按传输状态划分的卷”。
7. 单击库存页面上的“计划报告”按钮。
8. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可以调查转移状态。

创建报告以根据传输大小查看传输量

您可以创建报告来根据传输大小查看传输量。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤根据传输大小创建卷传输的自定义视图，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“查看”菜单中，选择“关系”>“过去 1 个月的转移率”。
3. 单击“总传输大小”列的顶部，按大小对卷传输进行排序。
4. 使用反映视图所显示内容的特定名称保存视图，例如“按传输大小划分的卷”。
5. 单击库存页面上的“计划报告”按钮。
6. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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。

创建报告以查看按天分组的传输量

您可以创建报告来查看按天分组的传输量。

开始之前

- 您必须具有应用程序管理员或存储管理员角色。

使用以下步骤创建按天分组的批量传输自定义视图，然后安排为该视图生成报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 在“查看”菜单中，选择“关系”>“过去 1 个月的转移率”。
3. 单击“天”列顶部可按天对交易量转移进行排序。
4. 使用反映视图所显示内容的特定名称保存视图，例如“按天传输量”。
5. 单击库存页面上的“计划报告”按钮。
6. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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，您可以按天调查交易量转移。

## 自定义卷性能报告

这些示例自定义报告用于帮助您识别和响应与卷性能相关的潜在问题。

创建报告以查看未启用**FabricPool** 的聚合上具有大量冷数据的卷

您可以创建报告来显示非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“存储”>“卷”。
2. 在“查看”菜单中，选择“性能”>“所有卷”。
3. 选择“显示/隐藏”以确保“磁盘类型”列出现在视图中。

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”列的顶部，按磁盘类型对卷进行排序，以便磁盘类型 SSD（FabricPool）位于底部。
7. 使用反映视图所显示内容的特定名称保存视图，例如“Cold data vols not FabricPool”。
8. 单击库存页面上的“计划报告”按钮。
9. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。

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聚合的卷。

## Microsoft Excel 报告示例

这些 Microsoft Excel 示例报告旨在介绍使用 Excel 高级功能可用的报告选项。

Excel 的高级功能可以根据您的需求创建各种各样的报告。有关如何使用 Excel 的完整信息，请参阅产品文档。



您必须具有应用程序管理员或存储管理员角色才能管理报告。

## 创建报告以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在 Excel 文件中创建报告来分析容量。

### 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 Excel 文件，并安排最终报告。

### 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**。



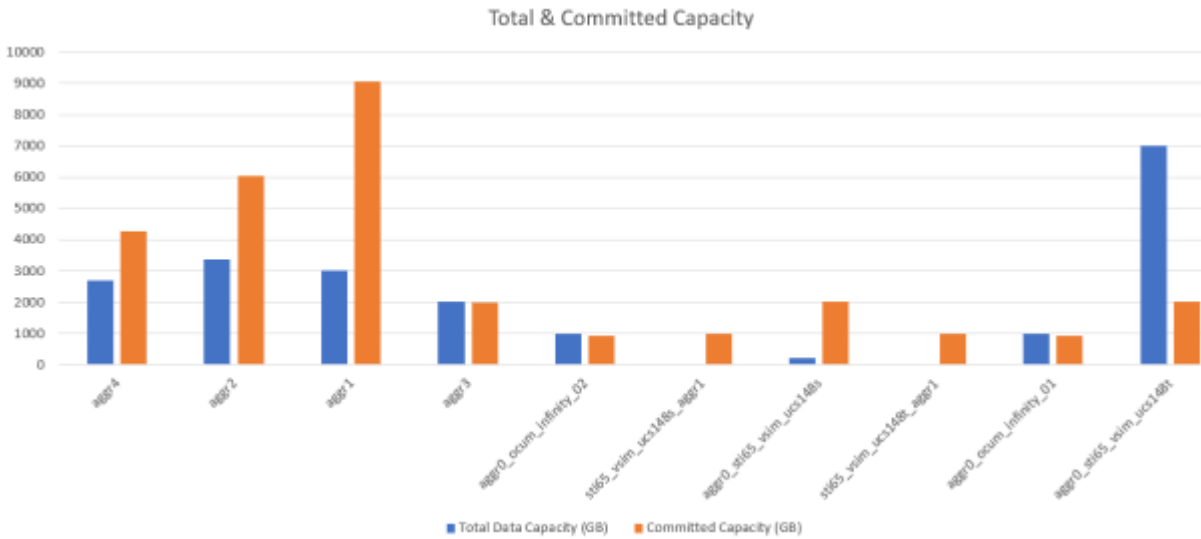
根据您的浏览器，您可能需要单击“确定”来保存文件。

3. 如果需要，请单击“启用编辑”。
4. 在 Excel 中打开下载的文件。
5. 创建新工作表（）之后 `data` 表并将其命名为\*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. 承诺容量（GB）
  - c. 已用数据容量（GB）
  - d. 可用数据容量（GB）
7. 在每一列的第一行中，输入以下公式，确保它引用数据表（数据！），并引用捕获数据的正确列和行说明符（总数据容量从 E 列、第 2 行到第 20 行提取数据）。
  - a. =SUM（数据！ E\$2： 数据！ E\$20）
  - b. =SUM（数据！ F\$2： 数据！ F\$50）
  - c. =SUM（数据！ G\$2： 数据！ G\$50）
  - d. =SUM(数据！ H\$2:数据！ H\$50)

该公式根据当前数据对每一列进行总计。

| Total Data Capacity (GB) | Committed Capacity (GB) | Used Data Capacity (GB) | Available Data Capacity (GB) |
|--------------------------|-------------------------|-------------------------|------------------------------|
| 5380.31                  | 6892.47                 | 11764.27                | 3911.03                      |

- 1. 在数据表上，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` 床单。
- 4. 使用选择图表时可用的“设计”和“格式”菜单，您可以自定义图表的外观。
- 5. 满意后，保存包含更改的文件。请勿更改文件名或位置。



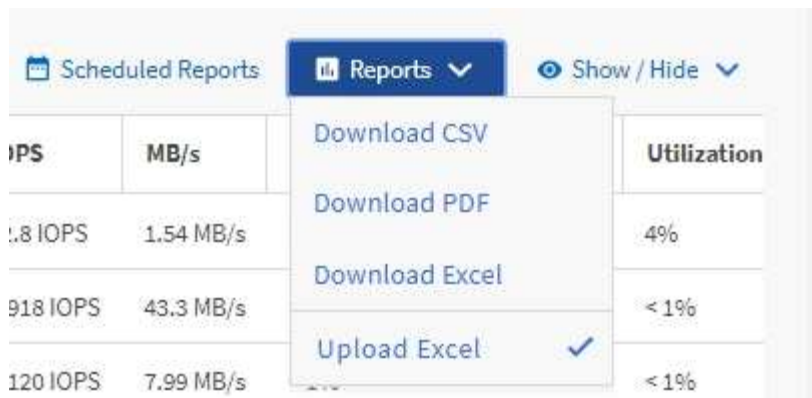
- 6. 在 Unified Manager 中，选择 报告 > 上传 **Excel**。



确保您处于下载 Excel 文件的同一视图中。

- 7. 选择您已修改的 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“计划报告”。
11. 单击“添加计划”以向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。



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，然后单击复选标记 (✓) 位于行尾。

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，您可能需要研究如何最好地利用整个网络的可用容量。

## 创建报告以显示总计与可用容量图表

您可以创建报告，以 Excel 图表格式分析存储总量和已提交容量。

### 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 中下载该视图，创建总容量和承诺容量图表，上传自定义 Excel 文件，并安排最终报告。

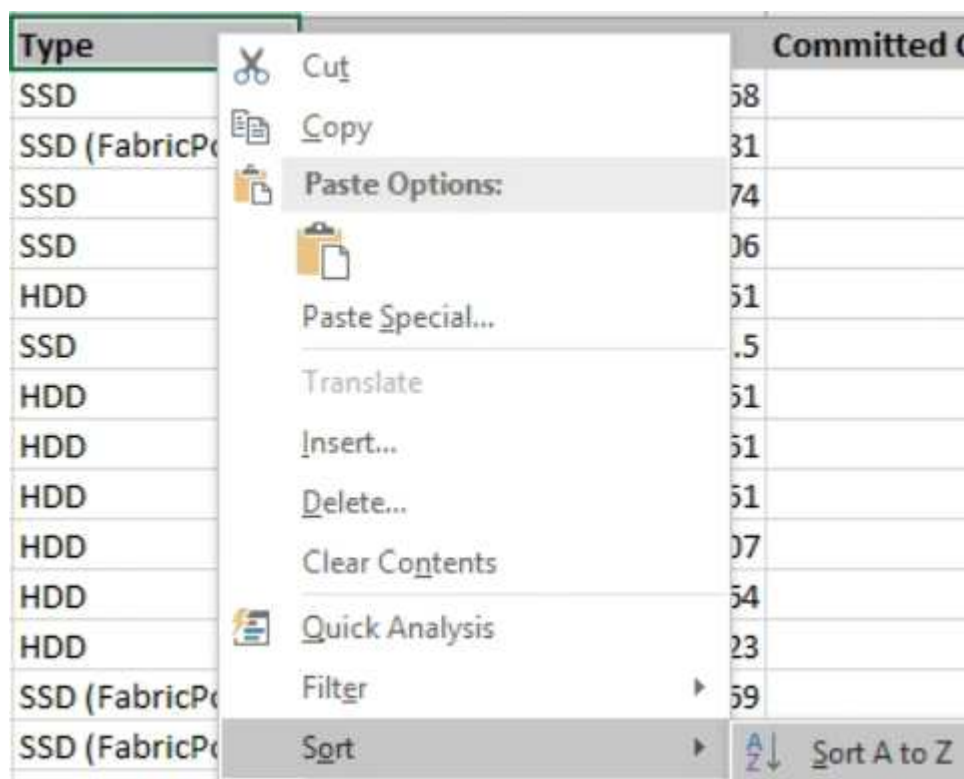
### 步骤

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”来保存文件。

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，右键单击类型列并选择\*排序\* > 按 **A** 到 **Z** 排序。



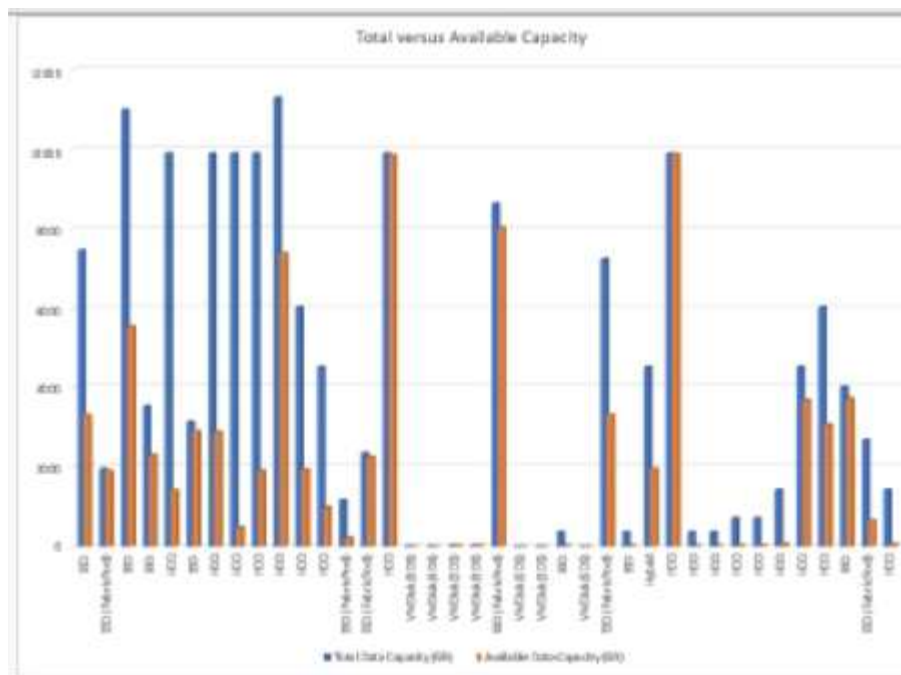
这将按存储类型排列您的数据，例如：

- HDD
- 杂交种
- SSD
- SSD (FabricPool)

6. 选择 `Type, Total Data Capacity,` 和 `Available Data Capacity` 列。







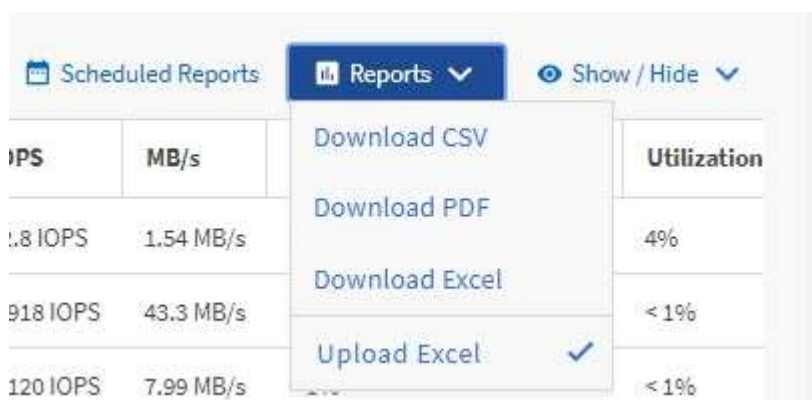
13. 在 Unified Manager 中，选择 报告 > 上传 **Excel**。



确保您处于下载 Excel 文件的同一视图中。

14. 选择您已修改的 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“计划报告”。
18. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。



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，然后单击复选标记 (✓) 位于行尾。

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。

## 创建报告以查看可用卷容量图表

您可以创建报告来分析 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 Excel 文件，并安排最终报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“卷”。
2. 选择\*报告\* > 下载 **Excel**。



根据您的浏览器，您可能需要单击“确定”来保存文件。

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`工作表中，选择要使用的数据 `Volume`和 `Available Data% 列。
6. 在“插入”菜单上，选择 3-D piechart.

该图表显示哪些卷具有最大的可用空间。该图表出现在数据表上。

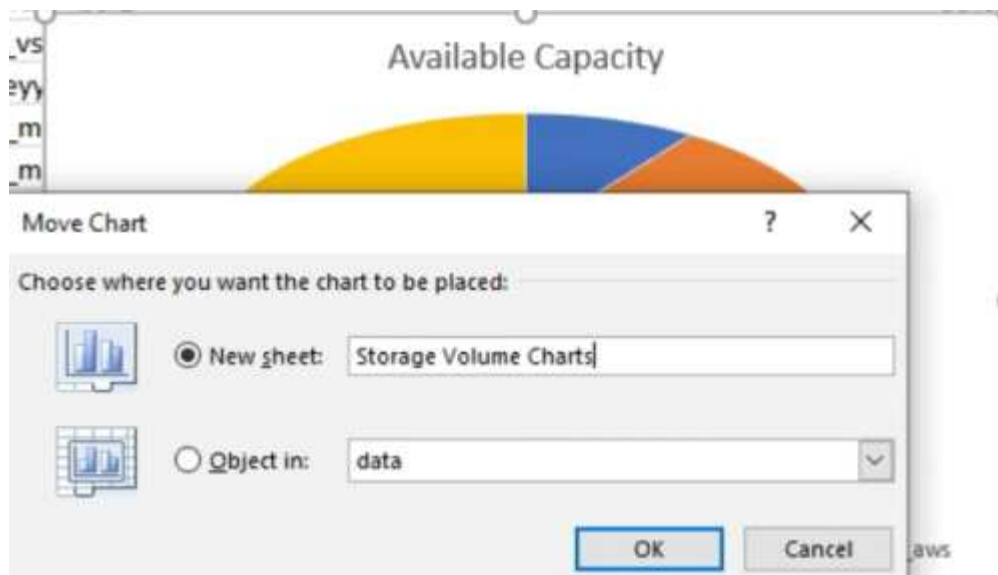


根据您的网络配置，选择整列或太多数据行可能会导致饼图无法读取。此示例使用三维饼图，但您可以使用任何图表类型。使用最能显示您想要捕获的数据的图表。

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”并将工作表命名为“存储量图表”。



确保新表出现在信息和数据表之后。



10. 使用选择图表时可用的“设计”和“格式”菜单，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**。



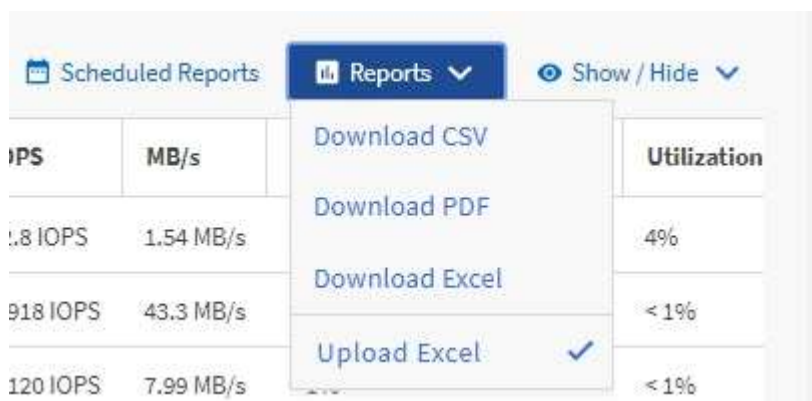
确保您处于下载 Excel 文件的同一视图中。

13. 选择您已修改的 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“计划报告”。

17. 单击“添加计划”向“报告计划”页面添加新行，以便您可以定义新报告的计划特征。

18. 输入报告计划的名称并填写其他报告字段，然后单击复选标记 (✓) 位于行尾。



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，您可能需要平衡卷上的负载。

## 创建报告以查看具有最多可用 IOPS 的聚合

此报告显示哪些聚合具有每种聚合类型最多的可用 IOPS，您可以在其上配置新的工作负载。

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 Excel 文件，并安排最终报告。

步骤

1. 在左侧导航窗格中，单击“存储”>“聚合”。
2. 从“查看”下拉菜单中选择“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. 拖放 `Available IOPS` 和 `Free Capacity` 旁边的列 `Type` 柱子。
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”来保存文件。

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，单击表左上角的小三角形以选择整个表。
10. 在“数据”功能区中，从“排序”中选择 Sort & Filter area.
11. 设置以下排序级别：
  - a. 将\*排序依据\*指定为 Available IOPS (IOPS)，\*排序依据\*为 Cell Values, `并且\*订单\*为 `Largest to Smallest`.

- b. 单击“添加级别”。
- c. 将\*排序依据\*指定为 Type, \*排序依据\*为 Cell Values, `并且\*订单\*为 `Z to A.
- d. 单击“添加级别”。
- e. 将\*排序依据\*指定为 Free Capacity (GB), 排序依据 Cell Values, `并且\*订单\*为 `Largest to Smallest.
- f. 单击“确定”。

12. 保存并关闭 Excel 文件。

13. 在 Unified Manager 中, 选择 报告 > 上传 **Excel**。



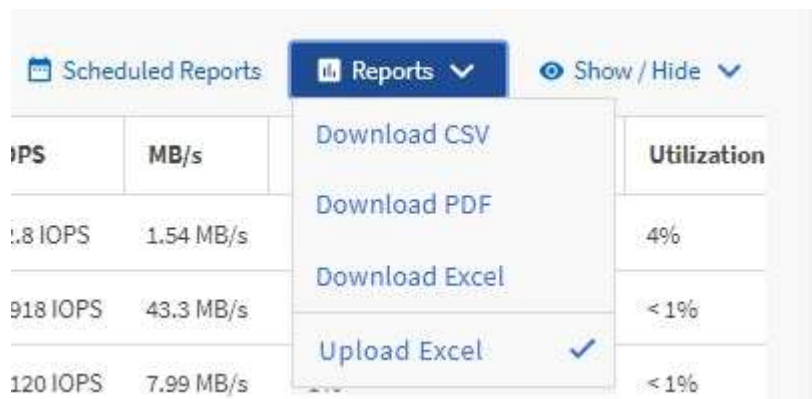
确保您处于下载 Excel 文件的同一视图中。

14. 选择您修改过的 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“计划报告”。

18. 单击“添加计划”以向“报告计划”页面添加新行, 以便您可以定义新报告的计划特征。

19. 输入报告计划的名称并填写其他报告字段, 然后单击复选标记 (✓) 位于行尾。



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, 您可能希望在具有最大可用 IOPS 的聚合上配置新的工作负载。

# 使用 REST API 管理存储

## 开始使用Active IQ Unified Manager REST API

Active IQ Unified Manager提供了一组 API，通过 RESTful Web 服务接口管理受支持存储系统上的存储资源，以实现任何第三方集成。

在这些主题中，您将找到有关 Unified Manager API、解决特定问题的示例工作流程以及一些示例代码的信息。利用这些信息，您可以创建NetApp Manageability 软件解决方案的 RESTful 客户端来管理NetApp系统。API 基于表述性状态转移 (REST) 架构风格。支持所有四种 REST 操作：创建、读取、更新和删除（也称为 CRUD）。

看["Active IQ Unified Manager"](#)有关Active IQ Unified Manager REST API 优势的更多资源和详细信息。

### 此内容的受众

此处的主题适用于创建通过 REST API 与Active IQ Unified Manager软件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来基本了解如何使用 Unified Manager REST API 构建客户端应用程序来管理和监控NetApp存储系统。

如果您想使用存储提供程序、ONTAP集群和管理管理 API 来管理存储，则应该使用此信息。



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。

### Active IQ Unified Manager API 访问和类别

Active IQ Unified Manager API 使您能够管理和配置环境中的存储对象。您还可以访问 Unified Manager Web UI 来执行其中一些功能。

#### 构建 URL 以直接访问 REST API

您可以通过编程语言（例如 Python、C#、C++、JavaScript 等）直接访问 REST API。输入主机名或 IP 地址以及用于访问 REST API 的 URL，格式如下

`https://<主机名>/api`



默认端口为 443。您可以根据环境的需要配置端口。

#### 访问在线 API 文档页面

您可以访问随产品打包的 API 文档\_参考内容页面，展示 API 文档，也可以手动发起 API 调用（例如在接口上，Swagger）。您可以通过单击“菜单栏”>“帮助按钮”>“API 文档”来访问此文档

或者，输入主机名或 IP 地址以及 URL 以访问 REST API 页面，格式如下



<https://<主机名>/docs/api/>

## 类别

API 调用根据区域或类别按功能进行组织。要找到特定的 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 分为以下类别。

- 数据中心

此类别包含帮助您使用工具（例如工作流自动化和 Ansible）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。

- 管理服务器

**management-server** 类别下的 API 包含 ``jobs``、``system`` 和 ``events`` 蜜蜂。作业是计划异步执行的与管理 Unified Manager 上的存储对象或工作负载相关的操作。这 ``events`` API 返回数据中心中的事件，并且 ``system`` API 返回 Unified Manager 实例详细信息。

- 存储提供商

此类别包含管理和配置文件共享、LUN、性能服务级别和存储效率策略所需的所有配置 API。API 还使您能够配置访问端点、Active Directory，以及在存储工作负载上分配性能服务级别和存储效率策略。

- 行政

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 数据源的信任库证书以及将 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 并管理数据中心中的存储对象。

- 安全

此类别包含用于管理 Unified Manager 用户的 API。

## 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。返回的最大记录数 ``GET`` 操作为 1000。



API 使您能够根据支持的属性对记录进行过滤、排序和排列。



- POST 示例：`POST /datacenter/svm/svms` 创建自定义存储虚拟机 (SVM)。
- PATCH 示例：`PATCH /datacenter/svm/svms/{key}` 使用其唯一键修改 SVM 的属性。
- 删除示例：`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 <b>REST</b> 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   | <p>读取所有数据的权限。具有此角色的用户可以运行所有 GET 请求。</p> <p>此外，他们还具有写访问权限（运行 PATCH、POST 和 DELETE 请求）来执行特定活动，例如管理、存储服务对象和存储管理选项。</p> |
| 应用程序管理员 | 对所有数据的读写访问。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 操作的更多信息，请参阅\_在线 API 文档\_。

## Active IQ Unified Manager 中的 API 版本

Active IQ Unified Manager 中的 REST API URI 指定了版本号。例如，`/v2/datacenter/svm/svms` 版本号 `v2` 在 `/v2/datacenter/svm/svms` 表示特定版本中使用的 API 版本。版本号通过发回客户端可以处理的响应来最大限度地减少 API 更改对客户端软件的影响。

此版本号的数字部分随着版本的发布而递增。带有版本号的 URI 提供了一致的接口，以保持未来版本的向后兼容性。例如，您还可以找到没有版本的相同 API `/datacenter/svm/svms` 表示没有版本的基本 API。基础 API 始终是最新版本的 API。



在您的 Swagger 界面右上角，您可以选择要使用的 API 版本。默认选择最高版本。建议您使用 Unified Manager 实例中可用的特定 API 的最高版本（就增量整数而言）。

对于所有请求，您必须明确请求要使用的 API 版本。当指定版本号时，服务不会返回您的应用程序未设计处理的响应元素。在 REST 请求中，您应该包含版本参数。早期版本的 API 在几次发布后最终会被弃用。在此版本中，`v1` 该 API 的版本已被弃用。

## ONTAP 中的存储资源

ONTAP 中的存储资源大致可分为\_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 有效地管理 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

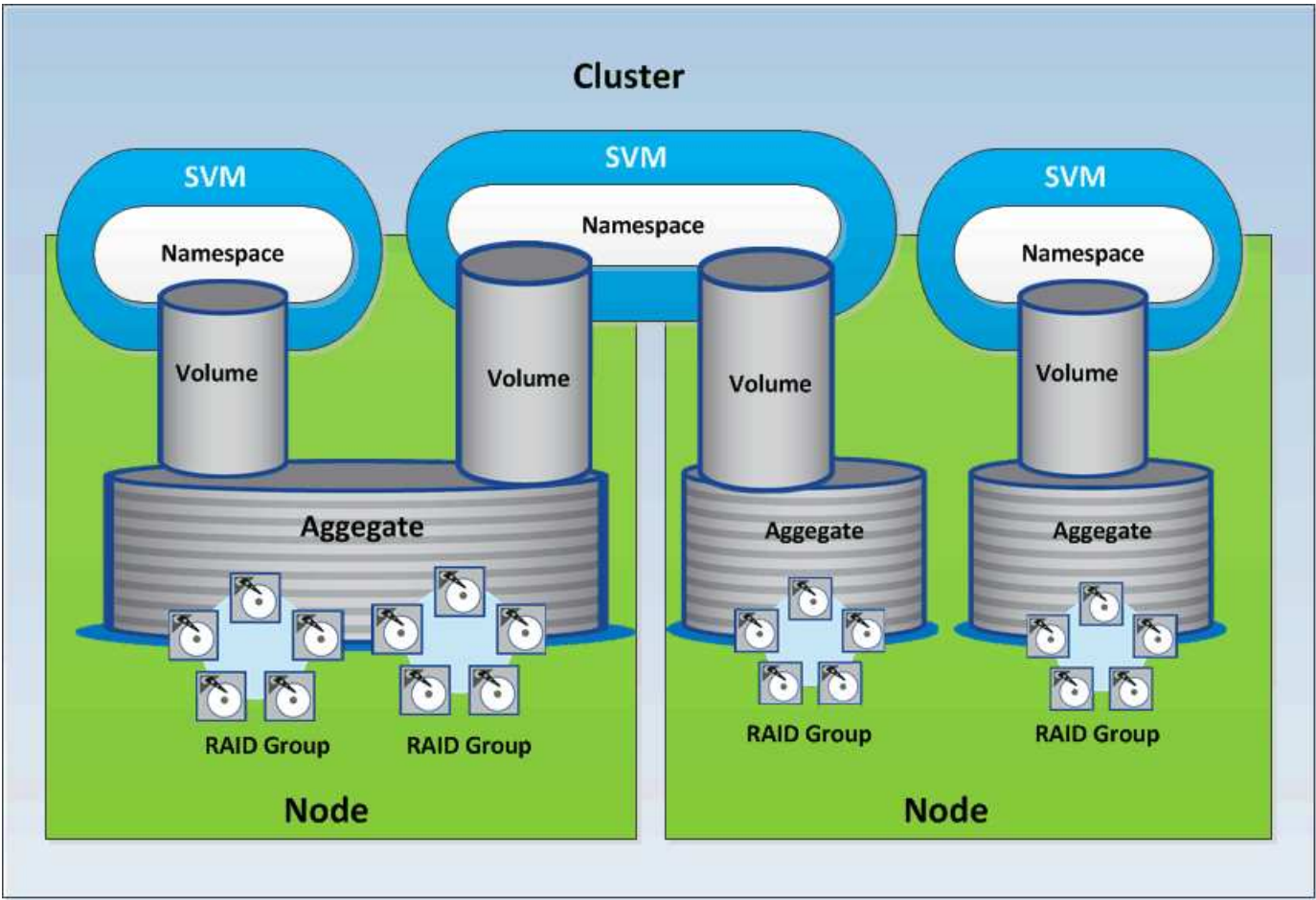
指ONTAP提供的物理存储对象。物理存储资源包括磁盘、集群、存储控制器、节点和聚合。

- 逻辑存储资源

指ONTAP提供的不与物理资源绑定的存储资源。这些资源与存储虚拟机（SVM，以前称为 Vserver）相关联，并且它们独立于任何特定的物理存储资源（例如磁盘、阵列 LUN 或聚合）而存在。

逻辑存储资源包括所有类型和 qtree 的卷，以及可以与这些资源一起使用的功能和配置，例如 Snapshot 副本、重复数据删除、压缩和配额。

下图显示了双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

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 客户端或编程平台访问Active IQ Unified Manager REST API。

示例请求和响应：

- 要求

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

• 回复

```
{
 "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 cURL 和 Perl 等脚本平台访问 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，用于服务器验证。该证书可以用自定义证书（或CA证书）替换。

您必须配置用户对 API 服务器的访问权限才能调用 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（如果您已将 API 服务器配置为通过 LDAP 进行身份验证）。您可以通过登录 Unified Manager 管理控制台用户界面来管理用户访问。

## Active IQ Unified Manager中使用的 HTTP 状态代码

在运行 API 或解决问题时，您应该注意Active IQ Unified Manager API 使用的各种 HTTP 状态代码和错误代码。

下表列出了与认证相关的错误代码：

| HTTP 状态代码 | 状态代码标题  | 描述                                   |
|-----------|---------|--------------------------------------|
| 200       | 确定      | 同步 API 调用成功执行后返回。                    |
| 201       | 已创建     | 通过同步调用创建新资源，例如 Active Directory 的配置。 |
| 202       | 已接受     | 成功执行配置功能（例如创建 LUN 和文件共享）的异步调用后返回。    |
| 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密钥。      |
| 401       | 未经授权的请求 | 您无权查看资源/未经授权。                        |
| 403       | 禁止请求    | 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过多请求时返回。                  |

| HTTP 状态代码 | 状态代码标题  | 描述                                                                                                                                      |
|-----------|---------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 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永久性的，也可能不是。例如，如果你运行 `GET` 或者 `GET ALL` 操作并收到此错误，建议您重复此操作至少五次。如果是永久性错误，则返回的状态代码继续为 500。如果操作成功，返回的状态码为 200。 |

## 使用Active IQ Unified Manager API 的建议

使用Active IQ Unified Manager中的 API 时，您应该遵循某些建议的做法。

- 为了有效执行，所有响应内容类型必须采用以下格式：

```
application/json
```

- API版本号与产品版本号无关。您应该使用适用于 Unified Manager 实例的最新版本的 API。有关 Unified Manager API 版本的更多信息，请参阅“Active IQ Unified Manager中的 REST API 版本控制”部分。
- 使用 Unified Manager API 更新数组值时，必须更新整个值字符串。您不能将值附加到数组。您只能替换现有阵列。
- 您可以对所有查询参数使用过滤运算符，例如竖线 (|) 和通配符 (\*)，但双精度值除外，例如指标 API 中的 IOPS 和性能。
- 避免使用过滤运算符通配符 (\*) 和管道符 (|) 的组合来查询对象。它可能会检索到不正确数量的对象。
- 使用值进行过滤时，确保值不包含任何 `?` 特点。这是为了减轻 SQL 注入的风险。
- 请注意 `GET` 任何 API 的 (all) 请求最多返回 1000 条记录。即使您通过设置 `max\_records` 参数设置为高于 1000 的值，则仅返回 1000 条记录。
- 为了执行管理功能，建议您使用 Unified Manager UI。

## 故障排除日志

系统日志使您能够分析故障原因并解决运行 API 时可能出现的问题。

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 | <p>包含所有API调用详情，例如调用API的用户的用户名、开始时间、执行时间、状态、URL等。</p> <p>您可以使用此日志文件检查常用的 API，或排除任何 GUI 工作流程的故障。您还可以根据执行时间使用它来扩展分析。</p> |

| 日志位置                         | 用途                                                                                                  |
|------------------------------|-----------------------------------------------------------------------------------------------------|
| /var/log/ocum/ocumserver.log | 包含所有 API 执行日志。<br><br>您可以使用此日志文件来排除故障和调试 API 调用。                                                    |
| /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。<br><br>您可以使用此日志文件来查找 Wildfly 服务器启动、停止或部署期间发生的任何问题的根本原因。             |
| /var/log/ocie/au.log         | 包含采集单元相关日志。<br><br>当您在ONTAP中创建、修改或删除任何对象但这些对象不会反映在Active IQ Unified Manager REST API 中时，您可以使用此日志文件。 |

## Job对象异步进程

Active IQ Unified Manager提供 `jobs` API 检索有关在运行其他 API 时执行的作业的信息。您必须知道如何使用作业对象进行异步处理。

某些 API 调用（尤其是用于添加或修改资源的调用）可能比其他调用需要更长的时间才能完成。Unified Manager 异步处理这些长时间运行的请求。

### 使用 Job 对象描述的异步请求

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并接受，但尚未完成。该请求将作为后台任务处理，并在客户端收到初始 HTTP 响应后继续运行。响应中包含锚定该请求的 Job 对象及其唯一标识符。

### 查询与 API 请求关联的 Job 对象

HTTP 响应中返回的 Job 对象包含多个属性。您可以查询 state 属性来确定请求是否已成功完成。Job对象可以处于以下状态之一：

- NORMAL
- WARNING
- PARTIAL\_FAILURES
- ERROR

轮询 Job 对象来检测任务的最终状态（成功或失败）时，可以使用两种技术：

- 标准轮询请求：立即返回当前作业状态。
- 长轮询请求：当作业状态转移到 NORMAL, ERROR, 或者 PARTIAL\_FAILURES.

## 异步请求中的步骤

您可以使用以下高级过程来完成异步 API 调用：

1. 发出异步 API 调用。
2. 收到 HTTP 响应 202，表示成功接受请求。
3. 从响应主体中提取 Job 对象的标识符。
4. 在循环中，等待 Job 对象达到终止状态 NORMAL，ERROR，`或者` PARTIAL\_FAILURES。
5. 验证作业的最终状态并检索作业结果。

## 你好 API 服务器

*Hello API server* 是一个示例程序，演示如何使用简单的 REST 客户端调用 Active IQ Unified Manager 中的 REST API。示例程序以 JSON 格式向您提供有关 API 服务器的基本信息（服务器仅支持 `application/json` 格式）。

使用的 URI 是：`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（默认值：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（例如 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：

- 使用与 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
- 握手期间跳过主机名验证
- 用途 `javax.net.ssl.HttpsURLConnection` 用于 URI 连接
- 使用第三方库(org.apache.commons.codec.binary.Base64) 用于构建 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，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 {
 HttpURLConnection connection =
getAllTrustingHttpsURLConnection();
 if (connection == null) {
 System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
 System.exit(1);
 }
 System.out.println("Invoking API: " + server_url);
 connection.setRequestMethod("GET");
 connection.setRequestProperty("Accept", "application/" +
response_format);
 String authString = getAuthorizationString();
 connection.setRequestProperty("Authorization", "Basic " +
authString);
 if (connection.getResponseCode() != 200) {

```

```

 System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
 + connection.getResponseMessage());
 System.exit(1);
 }
 BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
 String response;
 System.out.println("Response:");
 while ((response = br.readLine()) != null) {
 System.out.println(response);
 }
 connection.disconnect();
} catch (Exception e) {
 e.printStackTrace();
}
}

/* Print the usage of this sample code */ private static void
printUsage() {
 System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
 System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
 System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
 System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
 System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
 System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
}

/* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
 String[] args) {
 server = args[0];
 user = args[1];
 password = args[2];
 if (server.contains(":")) {
 String[] parts = server.split(":");
 server = parts[0];
 port = parts[1];
 }
}
}

```

```

/*
 * * Create a trust manager which accepts all certificates and * use
this trust
 * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
 * SSL Context and skip * server hostname verification during SSL
handshake. * *
 * Note: Trusting all certificates or skipping hostname verification *
is not
 * required for API Services to work. These are done here to * keep
this sample
 * REST Client code as simple as possible.
*/ private static 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

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细节。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找到该调用所需的信息。找到特定的 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。

工作流中的每个 API 调用都包含以下信息，以帮助在文档页面上找到该调用：

- 类别

API 调用在文档页面上按功能相关区域或类别进行组织。要找到特定的 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 动词标识对资源执行的操作。每个 API 调用都通过单个 HTTP 动词执行。

- 路径

路径决定了操作在执行调用时所使用的特定资源。路径字符串会附加到核心 URL 中，以形成标识资源的完整 URL。

### 使用 API 管理数据中心内的存储对象

REST API 下的 `datacenter` 类别使您能够管理数据中心中的存储对象，例如集群、节点、聚合、存储虚拟机、卷、LUN、文件共享和命名空间。这些 API 可用于查询对象的配置，其中一些 API 使您能够执行添加、删除或修改这些对象的操作。

大多数 API 都是 GET 调用，提供跨集群聚合、过滤、排序和分页支持。运行这些 API 时，它们会从数据库返回数据。因此，新创建的对象需要在下一个获取周期中被发现并出现在响应中。

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 来查看其详细信息。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>"
```



您的 Swagger API 界面上提供了 CURL 命令、示例、请求和对 API 的响应。您可以按照 Swagger 上指示的特定参数过滤和排序结果。这些 API 使您能够过滤特定存储对象（例如集群、卷或存储 VM）的结果。

## 数据中心存储对象的 API

| HTTP 动词 | 路径                                                                                                                         | 描述                                                                                                                                 |
|---------|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| GET     | <code>/datacenter/cluster/clusters</code><br><br><code>/datacenter/cluster/clusters/{key}</code>                           | 您可以使用此方法查看整个数据中心的ONTAP集群的详细信息。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），并指示集群是否为全 SAN 阵列。                   |
| GET     | <code>/datacenter/cluster/licensing/licenses</code><br><code>/datacenter/cluster/licensing/licenses/{key}</code>           | 返回数据中心集群上安装的许可证的详细信息。您可以根据所需条件过滤结果。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来检索特定许可证的详细信息。                                             |
| GET     | <code>/datacenter/cluster/nodes</code><br><br><code>/datacenter/cluster/nodes/{key}</code>                                 | 您可以通过此方法查看数据中心内节点的详细信息。您可以查看有关集群、节点健康状况、性能容量和节点的高可用性 (HA) 对的信息。                                                                    |
| GET     | <code>/datacenter/protocols/cifs/shares</code><br><br><code>/datacenter/protocols/cifs/shares/{key}</code>                 | 您可以通过此方式查看数据中心内CIFS共享的详细信息。除了集群、SVM 和卷详细信息之外，还会返回有关访问控制列表 (ACL) 的信息。                                                               |
| GET     | <code>/datacenter/protocols/nfs/export-policies</code><br><br><code>/datacenter/protocols/nfs/export-policies/{key}</code> | 您可以使用此方法查看受支持的 NFS 服务的导出策略的详细信息。<br><br>您可以查询集群或存储虚拟机的导出策略，并重复使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更多信息，请参阅“配置 CIFS 和 NFS 文件共享”。 |

| HTTP 动词 | 路径                                                                             | 描述                                                                                                                                                      |
|---------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET     | /datacenter/storage/aggregates<br><br>/datacenter/storage/aggregates/{key}     | 您可以使用此方法查看数据中心中的聚合集合或特定聚合，以便在其上配置工作负载或进行监控。返回集群和节点详细信息、使用的性能容量、可用和已用空间以及存储效率等信息。                                                                        |
| GET     | /datacenter/storage/luns<br><br>/datacenter/storage/luns/{key}                 | 可以通过此方法查看整个数据中心的LUN集合。您可以查看有关 LUN 的信息，例如集群和 SVM 详细信息、QoS 策略和 igroup。                                                                                    |
| GET     | /datacenter/storage/qos/policies<br><br>/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。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<br><br>/datacenter/storage/qtrees/{key}             | 您可以使用此方法查看数据中心内所有FlexVol卷或FlexGroup卷的qtree 详细信息。返回集群和 SVM 详细信息、 FlexVol volume和导出策略等信息。                                                                 |
| GET     | /datacenter/storage/volumes<br><br>/datacenter/storage/volumes/{key}           | <p>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，以及卷的类型是读写、数据保护还是负载共享。</p> <p>对于FlexVol和FlexClone卷，您可以查看有关相应聚合的信息。对于FlexGroup卷，查询返回组成聚合的列表。</p> |

| HTTP 动词                        | 路径                                                                                       | 描述                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET<br>POST<br>DELETE<br>PATCH | /datacenter/protocols/san/<br>igroups<br><br>/datacenter/protocols/san/<br>igroups/{key} | <p>您可以分配授权访问特定 LUN 目标的启动器组 (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。</p> <p>您可以分别使用这些方法来查询、创建、删除和修改 igroup。</p> <p>注意事项：</p> <ul style="list-style-type: none"> <li>• <b>`POST`:</b> 创建 igroup 时，您可以指定要分配访问权限的存储虚拟机。</li> <li>• <b>`DELETE`:</b> 您需要提供 igroup 键作为输入参数来删除特定的 igroup。如果您已经为 LUN 分配了 igroup，则无法删除该 igroup。</li> <li>• <b>`PATCH`:</b> 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。</li> </ul> |
| GET<br>POST<br>DELETE<br>PATCH | /datacenter/svm/svms<br><br>/datacenter/svm/svms/{key}                                   | <p>您可以使用这些方法来查看、创建、删除和修改存储虚拟机（存储 VM）。</p> <ul style="list-style-type: none"> <li>• <b>`POST`:</b> 您必须输入要创建的存储虚拟机对象作为输入参数。您可以创建自定义存储虚拟机，然后为其分配所需的属性。</li> <li>• <b>`DELETE`:</b> 您需要提供存储虚拟机密钥来删除特定的存储虚拟机。</li> <li>• <b>`PATCH`:</b> 您需要提供存储虚拟机密钥来修改特定的存储虚拟机。您还需要输入要更新的属性及其值。</li> </ul>                                                                                                                                         |



#### 注意事项：

如果您在环境中启用了基于 SLO 的工作负载配置，则在创建存储虚拟机时，请确保它支持配置 LUN 及其文件共享所需的所有协议，例如 CIFS 或 SMB、NFS、FCP 和 iSCSI。如果存储虚拟机不支持所需的服务，则配置工作流程可能会失败。建议在存储虚拟机上也启用相应类型工作负载的服务。

如果您已在环境中启用基于 SLO 的工作负载配置，则无法删除已配置存储工作负载的存储虚拟机。当您删除已配置 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 服务器名称仍会保留在 Active Directory 配置中，您必须将其从 Active Directory 服务

器中手动删除。

数据中心网络元素的 **API**

数据中心类别中的以下 API 检索有关您环境中的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 动词 | 路径                                                                                                           | 描述                                                                                             |
|---------|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| GET     | <code>/datacenter/network/ethernet/ports</code><br><br><code>/datacenter/network/ethernet/ports/{key}</code> | 检索有关数据中心环境中所有以太网端口的信息。使用端口键作为输入参数，您可以查看该特定端口的信息。检索信息，例如集群详细信息、广播域、端口详细信息（例如状态、速度和类型）以及端口是否启用。  |
| GET     | <code>/datacenter/network/fc/interfaces</code><br><br><code>/datacenter/network/fc/interfaces/{key}</code>   | 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。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     | <code>/datacenter/network/fc/ports</code><br><br><code>/datacenter/network/fc/ports/{key}</code>             | 检索有关数据中心环境中节点中使用的所有 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。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     | <code>/datacenter/network/ip/interfaces</code><br><br><code>/datacenter/network/ip/interfaces/{key}</code>   | 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。使用接口键作为输入参数，您可以查看该特定接口的信息。检索集群详细信息、IP 空间详细信息、主节点详细信息、是否启用故障转移等信息。 |

通过代理访问访问**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 仅支持在 Unified Manager 数据源（即ONTAP集群）上执行一组选定的操作。您可以通过ONTAP API 使用其他功能。网关 API 允许 Unified Manager 成为一个直通过接口，用于传输在其管理的ONTAP集群上执行的所有 API 请求，而无需单独登录到每个数据中心集群。它作为单一管理点，在由 Unified Manager 实例管理的ONTAP集群中运行 API。API 网关功能允许 Unified Manager 成为单一控制平面，您可以从中管理多个ONTAP集群，而无需单独登录它们。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集群。





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，通过维护与 ONTAP API 相同的格式的标头和正文请求来传输 API 请求。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，而无需传递单独的集群凭据。它继续管理集群身份验证和集群管理，但将 API 请求重定向到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 动词                                                                         | 路径 (URL)                                                                                                                                                                                                                                                                                     | 描述                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET                                                                             | /gateways                                                                                                                                                                                                                                                                                    | <p>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根据集群 UUID 或通用唯一标识符 (UUID) 运行其他方法。</p> <div>  <p>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。</p> </div>                                                                        |
| GET<br>POST<br>DELETE<br>PATCH<br>OPTIONS (Swagger 上不可用)<br>HEAD (Swagger 上不可用) | <p>/gateways/{uuid}/{path}</p> <div>  <p>{uuid} 的值必须替换为要执行 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，并通过 HTTPS 添加到 Unified Manager。{path} 必须替换为 ONTAP REST URL。您必须删除 '/api/' 来自 URL。</p> </div> | <p>这是一个单点代理 API，支持所有 ONTAP REST API 的 POST、DELETE、PATCH 操作和 GET。只要受 ONTAP 支持，任何 API 均不受任何限制。隧道或代理功能无法被禁用。</p> <p>这 '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，运行 'OPTIONS' 使用此网关 API 返回的方法 'GET' 作为回应。Swagger 上不支持此方法，但其他 API 工具上可以执行。</p> <p>这 'OPTIONS' 方法确定资源是否可用。此操作可用于查看 HTTP 响应头中有关资源的元数据。Swagger 上不支持此方法，但其他 API 工具上可以执行。</p> |

## 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 将标头和响应主体中的 URL 和超媒体转换为应用程序状态引擎 (HATEOAS) 链接以及 API 网关基本 URL。网关 API 充当代理基本 URL，您可以将 ONTAP REST URL 附加到该 URL 并执行所需的 ONTAP REST 端点。



为了使ONTAP API 能够通过 API 网关成功运行，该 API 必须得到其所运行的ONTAP集群版本的支持。运行ONTAP集群上不支持的 API 不会返回任何结果。

在此示例中，网关 API（代理基本 URL）为： `/gateways/{uuid}/`

采用的ONTAP API 是： `/storage/volumes`。您需要添加ONTAP API REST URL 作为路径参数的值。



添加路径时，请确保已删除“/” symbol at the beginning of the URL. For the API `/storage/volumes`, 添加 `storage/volumes`.

附加的 URL 是： `/gateways/{uuid}/storage/volumes`

在运行 GET 操作，生成的URL如下：

`GET https://<hostname>/api/gateways/<cluster_UUID>/storage/volumes`

这 `/api` 附加 URL 中的ONTAP REST URL 标签被删除，而网关 API 的标签被保留。

示例 **cURL** 命令

```
curl -X GET "https://<hostname>/api/gateways/lcd8a442-86d1-11e0-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。响应格式与您从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 都在集群范围内设置了上下文。基于存储虚拟机操作的API也是以集群为范围的，即API操作是在被管理的集群内的特定存储虚拟机上执行的。当你运行 `/gateways/{uuid}/{path}` API，请确保输入运行该操作的集群的集群 UUID（Unified Manager 数据源 UUID）。要将上下文设置为该集群内的特定存储虚拟机，请输入存储虚拟机密钥作为 `X-Dot-SVM-UUID` 参数或输入存储虚拟机名称作为 `X-Dot-SVM-Name` 参数。该参数作为过滤器添加到字符串标头中，并且操作在该集群内的该存储虚拟机范围内运行。

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 的更多信息，请参阅<https://docs.netapp.com/us-en/ontap-automation/index.html>["ONTAP REST API 自动化"]

使用 **API** 执行管理任务

您可以使用 `administration` 类别来修改备份设置、验证备份文件信息和集群证书，以及将ONTAP集群作为Active IQ Unified Manager数据源进行管理。



您必须具有应用程序管理员角色才能运行这些操作。您还可以使用 Unified Manager Web UI 来配置这些设置。

| HTTP 动词          | 路径                             | 描述                                                                                                                                                                                                                                                                                                  |
|------------------|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GET<br><br>PATCH | <br><br>/admin/backup-settings | <p>您可以使用 `GET` 方法查看 Unified Manager 中默认配置的备份计划的设置。您可以验证以下内容：</p> <ul style="list-style-type: none"><li>• 计划是否启用或禁用</li><li>• 计划备份的频率（每日或每周）</li><li>• 备份时间</li><li>• 应用程序中应保留的最大备份文件数量</li></ul> <p>备份时间为服务器时区。</p> <p>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` 方法来修改默认设置。</p> |
| GET              | /admin/backup-file-info        | 每次修改 Unified Manager 的备份计划时都会生成备份转储文件。您可以使用此方法来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相符。                                                                                                                                                                                                            |
| GET              | /admin/datasource-certificate  | 您可以使用此方法从信任库中查看数据源（集群）证书。在将ONTAP集群添加为 Unified Manager 数据源之前，需要验证证书。                                                                                                                                                                                                                                 |

| HTTP 动词 | 路径                                | 描述                                                        |
|---------|-----------------------------------|-----------------------------------------------------------|
| GET     | /admin/datasources/clusters       | 您可以使用 `GET` 方法来检索由 Unified Manager 管理的数据源（ONTAP集群）的详细信息。  |
| POST    |                                   |                                                           |
| PATCH   | /admin/datasources/clusters/{key} | 您还可以将新集群添加到 Unified Manager 作为数据源。要添加集群，您必须知道其主机名、用户名和密码。 |
| DELETE  |                                   | 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 管理用户

您可以使用 `security` 类别来控制用户对 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。根据您的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。



您必须具有应用程序管理员角色才能运行这些操作。您还可以使用 Unified Manager Web UI 来配置这些设置。

下的 API `security` 类别使用用户参数（即用户名），而不是键参数作为用户实体的唯一标识符。

| HTTP 动词 | 路径                     | 描述                                                                                                         |
|---------|------------------------|------------------------------------------------------------------------------------------------------------|
| GET     | /security/users        | <p>您可以使用这些方法获取用户的详细信息或向 Unified Manager 添加新用户。</p> <p>您可以根据用户类型为用户添加特定角色。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。</p> |
| POST    | /security/users        |                                                                                                            |
| GET     | /security/users/{name} | <p>GET 方法使您能够检索用户的所有详细信息，例如姓名、电子邮件地址、角色、授权类型。PATCH 方法使您能够更新详细信息。DELETE 方法使您能够删除用户。</p>                     |
| PATCH   |                        |                                                                                                            |
| DELETE  |                        |                                                                                                            |

## 使用 API 查看性能指标

Active IQ Unified Manager 为您提供了一组 API `/datacenter` 类别，使您能够查看数据中心中的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，例如集群、节

点、LUN、卷、聚合、存储虚拟机、FC 接口、FC 端口、以太网端口和 IP 接口。

这 `/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中以下存储对象的不同级别的详细信息：

- 集群
- 节点
- 存储虚拟机
- 聚合
- 卷
- LUN
- FC 接口
- FC 端口
- 以太网端口
- IP 接口

下表对 `/metrics` 和 `/analytics` 与检索到的性能数据细节有关的 API。

| 指标                                                                                                       | 分析                                                                                                     |
|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| 单个对象的性能详细信息。例如，<br><code>/datacenter/cluster/clusters/{key}/metrics</code> API 要求输入集群键作为路径参数来检索该特定集群的指标。 | 数据中心内同一类型的多个对象的性能详细信息。例如，<br><code>/datacenter/cluster/clusters/analytics</code> API 检索数据中心中所有集群的集体指标。 |
| 根据检索的时间间隔参数对存储对象的性能指标进行采样。                                                                               | 某一类型存储对象在一定时期内（72 小时以上）的性能高级聚合值。                                                                       |
| 检索对象的基本详细信息，例如节点或集群的详细信息。                                                                                | 未检索到具体细节。                                                                                              |
| 检索单个对象的累积计数器，例如最小值、最大值、第 95 个百分位数和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。                                          | 对于同一类型的所有对象，将显示单个聚合值。                                                                                  |

| 指标                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 分析                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| <p>时间范围和样本数据基于以下时间表：数据的时间范围。例如 1h、12h、1d、2d、3d、15d、1w、1m、2m、3m、6m。如果范围超过 3 天（72 小时），您将获得 1 小时样本，否则您将获得 5 分钟样本。每个时间段的周期如下：</p> <ul style="list-style-type: none"><li>• 1 小时：最近 5 分钟内采样的一小时内的指标。</li><li>• 12h：最近 12 小时内每 5 分钟采样一次的指标。</li><li>• 1d：最近一天 5 分钟内采样的指标。</li><li>• 2d：最近 2 天的 5 分钟采样指标。</li><li>• 3d：最近 3 天的 5 分钟采样指标。</li><li>• 15d：最近 15 天的 1 小时内采样的指标。</li><li>• 1w：最近一周内 1 小时内采样的指标。</li><li>• 1m：最近一个月内 1 小时内采样的指标。</li><li>• 2m：最近 2 个月内 1 小时内采样的指标。</li><li>• 3m：最近 3 个月内 1 小时内采样的指标。</li><li>• 6m：最近 6 个月内 1 小时内采样的指标。</li></ul> <p>可用值：1h、12h、1d、2d、3d、15d、1w、1m、2m、3m、6m</p> <p>默认值：1h</p> | <p>超过72小时。计算此样本的持续时间以 ISO-8601 标准格式表示。</p> |

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）：



摘要值中的 95 分位数表示该期间收集的 95% 样本的计数器值小于指定的 95 分位数。

```
{
 "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（以及其他值）：



```
{
 "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

下表描述了 `/metrics` 和 `/analytics` 详细的 API。



这些 API 返回的 IOPS 和性能指标都是 double 值，例如 100.53。不支持使用管道符 (|) 和通配符 (\*) 过滤这些浮点值。

| HTTP 动词 | 路径                                                                                      | 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）。返回集群键和 UUID、时间范围、IOPS、吞吐量、样本数等信息。                                     |
| GET     | /datacenter/cluster/clusters/analytics                                                  | 检索数据中心内所有集群的高级性能指标。您可以根据所需条件过滤结果。返回聚合 IOPS、吞吐量和收集周期（以小时为单位）等值。                                     |
| GET     | /datacenter/cluster/nodes/{key}/metrics                                                 | 检索节点键的输入参数指定的节点的性能数据（样本和摘要）。返回节点 UUID、时间范围、IOPS 摘要、吞吐量、延迟和性能、收集的样本数和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过滤结果。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                                            | 检索聚合键的输入参数指定的聚合的性能数据（样本和摘要）。返回的信息包括时间范围、IOPS 摘要、延迟、吞吐量和性能容量、每个计数器收集的样本数以及利用率百分比。                   |
| GET     | /datacenter/storage/aggregates/analytics                                                | 检索数据中心内所有聚合的高级性能指标。您可以根据所需条件过滤结果。返回诸如聚合和集群键之类的信息以及诸如聚合 IOPS、吞吐量和收集周期（以小时为单位）之类的值。                  |
| GET     | /datacenter/storage/luns/{key}/metrics<br><br>/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）。返回读取、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每个计数器收集的样本数等信息。 |

| HTTP 动词 | 路径                                                                              | 描述                                                                                                              |
|---------|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| GET     | /datacenter/storage/luns/analytics<br><br>/datacenter/storage/volumes/analytics | 检索数据中心内所有 LUN 或卷的高级性能指标。您可以根据所需条件过滤结果。返回存储 VM 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/svm/svms/{key}/metrics                                              | 检索由存储 VM 键的输入参数指定的存储 VM 的性能数据（样本和摘要）。根据每个支持的协议汇总 IOPS，例如 nvmf, fcp, iscsi, 和 nfs、吞吐量、延迟和收集的样本数量。                |
| GET     | /datacenter/svm/svms/analytics                                                  | 检索数据中心内所有存储虚拟机的高级性能指标。您可以根据所需条件过滤结果。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。当提供支持范围的间隔（时间范围）时，API 将返回累积的计数器，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。返回集群和节点密钥和 UUID、吞吐量、收集周期和端口的利用率百分比等信息。您可以根据可用参数（例如端口键、利用率百分比、集群和节点名称以及 UUID 等）过滤结果。     |
| 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。当提供支持范围的间隔（时间范围）时，API 将返回累积的计数器，例如该时间段内的最小值、最大值和平均性能值。                            |
| GET     | /datacenter/network/fc/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。返回集群和 FC 接口密钥和 UUID、吞吐量、IOPS、延迟和存储 VM 等信息。您可以根据可用参数过滤结果，例如集群和 FC 接口名称和 UUID、存储 VM、吞吐量等。 |

| HTTP 动词 | 路径                                              | 描述                                                                                                             |
|---------|-------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| 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。当提供支持范围的间隔（时间范围）时，API 将返回累积的计数器，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。返回集群和节点密钥和 UUID、吞吐量、收集周期和端口的利用率百分比等信息。您可以根据可用参数（例如端口键、利用率百分比、集群和节点名称以及 UUID 等）过滤结果。   |
| GET     | /datacenter/network/ip/interfaces/{key}/metrics | 检索接口键的输入参数指定的网络 IP 接口的性能指标。当从支持的范围中提供一个间隔（时间范围）时，API 将返回信息，例如样本数、累积计数器、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。返回集群和 IP 接口密钥和 UUID、吞吐量、IOPS 和延迟等信息。您可以根据可用参数过滤结果，例如集群和 IP 接口名称和 UUID、IOPS、延迟、吞吐量等。 |

## 查看作业和系统详细信息

您可以使用 `jobs` API 下的 `management-server` 类别查看异步操作的执行详情。这 `system` API 下的 `management-server` 类别使您能够查看 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由同步和异步 API 调用执行。为异步执行而安排的调用可以通过为该调用创建的 Job 对象进行跟踪。每个 Job 对象都有一个唯一的键用于识别。每个 Job 对象都会返回 Job 对象 URI，以便您访问和跟踪作业的进度。您可以使用此 API 来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。查询所有作业，默认返回通过 Web UI 和 API 接口触发的最近 20 个作业的详细信息。使用内置过滤器查看特定的作业。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 动词 | 路径                                                             | 描述                                          |
|-------|---------|----------------------------------------------------------------|---------------------------------------------|
| 管理服务器 | GET     | /management-server/jobs                                        | 返回所有作业的作业详细信息。没有任何排序顺序，最后提交的 Job 对象将返回在最上面。 |
| 管理服务器 | GET     | /management-server/jobs/{key}<br><br>输入Job对象的job键来查看该job的具体详情。 | 返回特定 Job 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 环境的特定于实例的详细信息。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 动词 | 路径                        | 描述                                                |
|-------|---------|---------------------------|---------------------------------------------------|
| 管理服务器 | GET     | /management-server/system | 运行此 API 不需要输入参数。默认返回当前 Unified Manager 实例的系统详细信息。 |

## 使用 API 管理事件和警报

这 `events`，`alerts`，和 ``scripts`` API 下的 ``management-server`` 类别使您能够管理 Active IQ Unified Manager 环境中的事件、警报以及与警报相关的脚本。

### 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，您可以查看为您的集群生成的事件，并解决和更新它们。

通过运行 ``GET`` 方法 `/management-server/events`` API，可以查询您数据中心内的事件，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，您可以启用事件的解决工作流。您可以将事件分配给自己或其他用户并确认收到该事件。在资源上执行步骤以解决触发事件的问题时，您可以使用此 API 将事件标记为已解决。

有关事件的更多信息，请参阅["管理活动"](#)。

| 类别    | HTTP 动词 | 路径                                                           | 描述                                                                                                 |
|-------|---------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| 管理服务器 | GET     | /management-server/events<br>/management-server/events/{key} | 当您运行 Get ALL 方法时，响应主体包含数据中心中所有事件的事件详细信息。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。响应主体包含该事件的详细信息。 |
| 管理服务器 | 修补      | management-server/events/{key}                               | 运行此 API 来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事件分配给您自己或其他用户。这是一个同步操作。                                      |

## 管理警报

事件是自动且连续生成的。仅当事件满足特定过滤条件时，Unified Manager 才会生成警报。您可以选择应生成警报的事件。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某些严重程度类型的事件时自动发送通知。

有关警报的更多信息，请参阅["管理警报"](#)。

| 类别    | HTTP 动词 | 路径                                                           | 描述                                                                                                                     |
|-------|---------|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 管理服务器 | GET     | /management-server/alerts<br>/management-server/alerts/{key} | 使用警报键查询环境中所有现有警报或特定警报。您可以查看有关您的环境中生成的警报的信息，例如警报描述、操作、发送通知的电子邮件 ID、事件和严重性。                                              |
| 管理服务器 | POST    | /management-server/alerts                                    | 此方法使您能够为特定事件添加警报。您必须添加警报名称、警报适用的物理或逻辑资源或事件、警报是否启用以及是否发出 SNMP 陷阱。您可以添加要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）等等。 |

| 类别    | HTTP 动词 | 路径                             | 描述                                                                  |
|-------|---------|--------------------------------|---------------------------------------------------------------------|
| 管理服务器 | 修补并删除   | 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，您可以删除该警报。 |



在选择用于添加警报的资源时，请注意，选择集群作为资源并不会自动选择该集群内的存储对象。例如，如果您为所有集群的所有关键事件创建警报，那么您将只收到集群关键事件的警报。您将不会收到有关节点、聚合等的关键事件的警报。

## 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关联起来。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。当事件触发警报时，脚本就会执行。您可以上传自定义脚本并在生成警报时测试其执行情况。您可以将警报与脚本关联，以便在 Unified Manager 中针对某个事件发出警报时执行该脚本。

有关脚本的更多信息，请参阅["管理脚本"](#)。

| 类别    | HTTP 动词 | 路径                         | 描述                                         |
|-------|---------|----------------------------|--------------------------------------------|
| 管理服务器 | GET     | /management-server/scripts | 使用此 API 查询您环境中所有现有的脚本。使用标准过滤和排序操作来仅查看特定脚本。 |
| 管理服务器 | POST    | /management-server/scripts | 使用此 API 为脚本添加描述并上传与警报相关的脚本文件。              |

## 使用 API 管理工作负载

这里描述的 API 涵盖了存储管理的各种功能，例如查看存储工作负载、创建 LUN 和文件共享、管理性能服务级别和存储效率策略以及在存储工作负载上分配策略。

### 使用 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内所有 ONTAP 集群的存储工作负载的综合列表。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您数据中心内所有集群的所有存储工作负载。有关根据特定列过滤响应的信息，请参阅 Unified Manager 实例中提供的 API 参考文档。

| 类别    | HTTP 动词 | 路径                          |
|-------|---------|-----------------------------|
| 存储提供商 | GET     | /storage-provider/workloads |

#### 查看存储工作负载摘要

您可以使用以下方法来评估每个性能服务级别所管理的已用容量、可用容量、已用 IOPS、可用 IOPS 和存储工作负载数量。显示的存储工作负载可以是任何 LUN、NFS 文件共享或 CIFS 共享。API 提供了存储工作负载概览、Unified Manager 配置的存储工作负载概览、数据中心概览、以及数据中心的总空间、已用空间和可用空间以及 IOPS 概览（根据分配的性能服务级别）。响应此 API 所收到的信息用于填充 Unified Manager UI 中的仪表板。

| 类别    | HTTP 动词 | 路径                                  |
|-------|---------|-------------------------------------|
| 存储提供商 | GET     | /storage-provider/workloads-summary |

#### 使用 API 管理访问端点

您需要创建访问端点或逻辑接口 (LIF)，这是配置存储虚拟机 (SVM)、LUN 和文件共享所必需的。您可以查看、创建、修改和删除 Active IQ Unified Manager 环境中的 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，您需要输入 SVM、LUN 或文件共享的唯一标识符。您还可以输入唯一的访问端点密钥来检索特定访问端点的详细信息。

| 类别    | HTTP 动词 | 路径                                                                                 |
|-------|---------|------------------------------------------------------------------------------------|
| 存储提供商 | GET     | /storage-provider/access-endpoints<br><br>/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、系统管理器或 ONTAP CLI 在每个节点上创建访问端点。支持使用 IPv4 和 IPv6 地址创建访问端点。



您必须为每个节点的 SVM 配置最少数量的访问端点，才能成功配置 LUN 和文件共享。您应该为每个节点配置至少两个 SVM 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 动词 | 路径                                 |
|-------|---------|------------------------------------|
| 存储提供商 | POST    | /storage-provider/access-endpoints |

#### 删除访问端点

您可以使用以下方法删除特定的访问端点。您需要提供访问端点密钥作为输入参数来删除特定的访问端点。

| 类别    | HTTP 动词 | 路径                                       |
|-------|---------|------------------------------------------|
| 存储提供商 | 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来修改特定的访问端点。您还需要输入要更新的属性及其值。

| 类别    | HTTP 动词 | 路径                                       |
|-------|---------|------------------------------------------|
| 存储提供商 | 修补      | /storage-provider/access-endpoints/{key} |

#### 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，这些映射是在 SVM 上配置 CIFS 共享所需的。需要配置 Active Directory 映射才能将 SVM 与 ONTAP 映射。

#### 查看 Active Directory 映射

您可以使用以下方法查看 SVM 的 Active Directory 映射的配置详细信息。要查看 SVM 上的 Active Directory 映射，您需要输入 SVM 密钥。要查询特定映射的详细信息，您必须输入映射键。

| 类别    | HTTP 动词 | 路径                                                                                                       |
|-------|---------|----------------------------------------------------------------------------------------------------------|
| 存储提供商 | GET     | /storage-provider/active-directories-mappings<br><br>/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 动词 | 路径                                            |
|-------|---------|-----------------------------------------------|
| 存储提供商 | POST    | /storage-provider/active-directories-mappings |

## 使用 API 管理文件共享

您可以使用 `/storage-provider/file-shares` 用于查看、添加、修改和删除数据中心环境中的 CIFS 和 NFS 文件共享卷的 API。

在配置文件共享卷之前，请确保已创建 SVM 并使用支持的协议进行配置。如果您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会自动添加到您的 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 动词 | 路径                                                                       |
|-------|---------|--------------------------------------------------------------------------|
| 存储提供商 | GET     | /storage-provider/file-shares<br><br>/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。您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 来添加 FlexGroup 卷。

| 类别    | HTTP 动词 | 路径                            |
|-------|---------|-------------------------------|
| 存储提供商 | 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，创建 CIFS 共享或 NFS 文件共享。如果您不提供 ACL 参数的值，则不会创建 CIFS 共享，并且默认创建 NFS 共享，以提供所有人的访问权限。

创建数据保护卷：当您向 SVM 添加文件共享时，默认情况下挂载的卷类型是 `rw`（读写）。要创建数据保护 (DP) 卷，请指定 `dp` 作为 `type` 范围。

### 删除文件共享

您可以使用以下方法删除特定的文件共享。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 动词 | 路径                                  |
|-------|---------|-------------------------------------|
| 存储提供商 | DELETE  | /storage-provider/file-shares/{key} |

#### 修改文件共享

您可以使用以下方法修改文件共享并更新其属性。

您需要提供文件共享密钥来修改特定的文件共享。此外，您还需要输入要更新的属性及其值。



请注意，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 动词 | 路径                                  |
|-------|---------|-------------------------------------|
| 存储提供商 | 修补      | /storage-provider/file-shares/{key} |

#### 使用 API 管理 LUN

您可以使用 `/storage-provider/luns` API 用于查看、添加、修改和删除数据中心环境中的 LUN。

在配置 LUN 之前，请确保已创建 SVM 并使用支持的协议进行配置。如果您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会自动添加到您的 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 键运行此 API 来查看特定 LUN 的详细信息。

| 类别    | HTTP 动词 | 路径                                                         |
|-------|---------|------------------------------------------------------------|
| 存储提供商 | GET     | /storage-provider/luns<br><br>/storage-provider/luns/{key} |

#### 添加 LUN

您可以使用以下方法将 LUN 添加到您的 SVM。

| 类别    | HTTP 动词 | 路径                     |
|-------|---------|------------------------|
| 存储提供商 | POST    | /storage-provider/luns |



在您的 cURL 请求中，如果您在输入中为可选参数 `volume_name_tag` 提供了一个值，那么在创建 LUN 期间命名卷时将使用该值。此标签可以轻松搜索卷。如果您在请求中提供音量键，则会跳过标记。

## 删除 LUN

您可以使用以下方法删除特定的 LUN。您需要提供 LUN 密钥来删除特定的 LUN。



如果您在 ONTAP 中创建了一个卷，然后通过 Unified Manager 在该卷上配置了 LUN，则当您使用此 API 删除所有 LUN 时，该卷也会从 ONTAP 集群中删除。

| 类别    | HTTP 动词 | 路径                           |
|-------|---------|------------------------------|
| 存储提供商 | DELETE  | /storage-provider/luns/{key} |

## 修改 LUN

您可以使用以下方法修改 LUN 并更新其属性。您需要提供 LUN 密钥来修改特定的 LUN。您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，您应该查看“使用 API 的建议”中的建议。



每次调用此 API 时只能更新一个属性。对于多次更新，您需要多次运行此 API。

| 类别    | HTTP 动词 | 路径                           |
|-------|---------|------------------------------|
| 存储提供商 | 修补      | /storage-provider/luns/{key} |

## 使用 API 管理性能服务级别

您可以使用 Active IQ Unified Manager 上的存储提供程序 API 查看、创建、修改和删除性能服务级别。

### 查看性能服务级别

您可以使用以下方法查看性能服务级别，并将其分配给存储工作负载。API 列出了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，则需要输入该性能服务级别的唯一 ID 来检索其详细信息。

| 类别    | HTTP 动词 | 路径                                                                                                     |
|-------|---------|--------------------------------------------------------------------------------------------------------|
| 存储提供商 | GET     | /storage-provider/performance-service-levels<br><br>/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不满足存储工作负载所需的服务级别目标 (SLO)，您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。输入您想要创建的性能服务级别的详细信息。对于 IOPS 属性，请确保输入有效范围的值。

| 类别    | HTTP 动词 | 路径                                           |
|-------|---------|----------------------------------------------|
| 存储提供商 | 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性能服务级别。如果性能服务级别已分配给工作负载，或者它是唯一可用的性能服务级别，则您无法删除该性能服务级别。您需要提供性能服务级别的唯一 ID 作为输入参数来删除特定的性能服务级别。

| 类别    | HTTP 动词 | 路径                                                 |
|-------|---------|----------------------------------------------------|
| 存储提供商 | DELETE  | /storage-provider/performance-service-levels/{key} |

修改性能服务级别

您可以使用以下方法修改性能服务级别并更新其属性。您无法修改系统定义或分配给工作负载的性能服务级别。您需要提供唯一的 ID 来修改特定的性能服务级别。您还必须输入要更新的 IOPS 属性以及有效值。

| 类别    | HTTP 动词 | 路径                                                 |
|-------|---------|----------------------------------------------------|
| 存储提供商 | 修补      | /storage-provider/performance-service-levels/{key} |

根据性能服务级别查看聚合功能

您可以使用以下方法查询基于性能服务级别的聚合能力。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。在卷上配置工作负载时，您可以查看聚合支持特定性能服务级别的能力，并根据该能力配置工作负载。仅当您使用 API 调配工作负载时，才可以指定聚合。此功能在 Unified Manager Web UI 上不可用。

| 类别    | HTTP 动词 | 路径                                                                                             |
|-------|---------|------------------------------------------------------------------------------------------------|
| 存储提供商 | GET     | /storage-provider/aggregate-capabilities<br><br>/storage-provider/aggregate-capabilities/{key} |

## 使用 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，分配存储效率策略不是强制性的。
- 在为工作负载分配策略后，您无法取消分配该策略。
- 如果工作负载在ONTAP卷上指定了某些存储设置（例如重复数据删除和压缩），则这些设置可能会被您在 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覆盖。

### 查看存储效率策略

您可以使用以下方法在将存储效率策略分配给存储工作负载之前查看存储效率策略。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。如果您想查询特定的存储效率策略，您需要输入该策略的唯一 ID 来检索其详细信息。

| 类别    | HTTP 动词 | 路径                                                                                                       |
|-------|---------|----------------------------------------------------------------------------------------------------------|
| 存储提供商 | GET     | /storage-provider/storage-efficiency-policies<br><br>/storage-provider/storage-efficiency-policies/{key} |

### 添加存储效率策略

如果系统定义的策略不满足您的存储工作负载的配置要求，您可以使用以下方法创建自定义存储效率策略，并将其分配给您的存储工作负载。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 动词 | 路径                                            |
|-------|---------|-----------------------------------------------|
| 存储提供商 | 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，则您无法删除该策略。您需要提供存储效率策略的唯一 ID 作为输入参数来删除特定的存储效率策略。

| 类别    | HTTP 动词 | 路径                                                  |
|-------|---------|-----------------------------------------------------|
| 存储提供商 | DELETE  | /storage-provider/storage-efficiency-policies/{key} |

### 修改存储效率策略

您可以使用以下方法修改存储效率策略并更新其属性。您无法修改系统定义或分配给工作负载的存储效率策略。您需要提供存储效率策略的唯一 ID 来修改特定的存储效率策略。此外，您还需要提供想要更新的属性及其值。

| 类别    | HTTP 动词 | 路径                                                  |
|-------|---------|-----------------------------------------------------|
| 存储提供商 | 修补      | /storage-provider/storage-efficiency-policies/{key} |

## 存储管理的常见 API 工作流程

常见的工作流程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 来执行常见存储管理功能的示例。本节包含一些示例工作流程。

工作流程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 调用组成的工作流程来描述。

### 了解工作流中使用的 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细节。本文档中的工作流示例中使用的每个 API 调用仅包含在文档页面上找到该调用所需的信息。找到特定的 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。

工作流中的每个 API 调用都包含以下信息，以帮助在文档页面上找到该调用：

- 类别：API 调用在文档页面上按功能相关区域或类别组织。要查找特定的 API 调用，请滚动到页面底部，然后点击相应的 API 类别。
- HTTP 动词（调用）：HTTP 动词标识对资源执行的操作。每个 API 调用都通过单个 HTTP 动词执行。
- 路径：路径决定了执行调用时操作所应用的特定资源。路径字符串会附加到核心 URL 中，以形成标识资源的完整 URL。

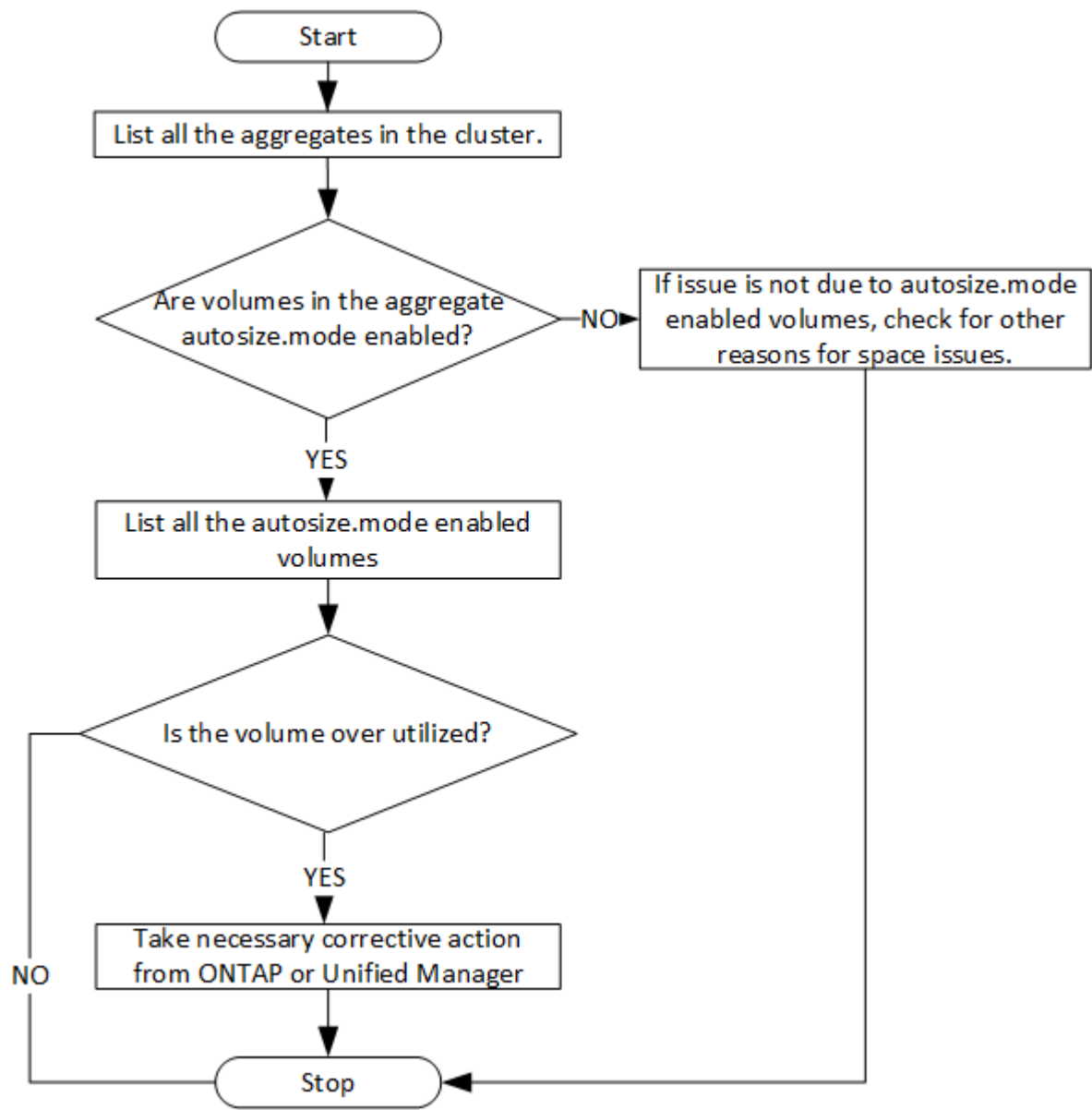
### 使用 API 确定聚合中的空间问题

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利用或利用不足的存储资源。

聚合的数据中心 API 检索有关可用空间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过滤检索到的信息。

确定聚合中是否缺少空间的一种方法是验证您的环境中是否存在启用了自动调整大小模式的卷。然后，您应该确定哪些卷被过度利用并执行任何纠正措施。

以下流程图说明了检索启用自动调整大小模式的卷信息的过程：



此流程假定集群已在ONTAP中创建并添加到 Unified Manager。

- 1. 获取集群密钥，除非您知道其值：

| 类别   | HTTP 动词 | 路径                           |
|------|---------|------------------------------|
| 数据中心 | GET     | /datacenter/cluster/clusters |



2. 使用集群键作为过滤参数，查询该集群上的聚合。

| 类别   | HTTP 动词 | 路径                             |
|------|---------|--------------------------------|
| 数据中心 | GET     | /datacenter/storage/aggregates |

3. 根据响应，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，从相同的 JSON 输出中获取聚合键。
4. 使用每个聚合键，过滤所有具有 autosize.mode 参数值的卷 grow。

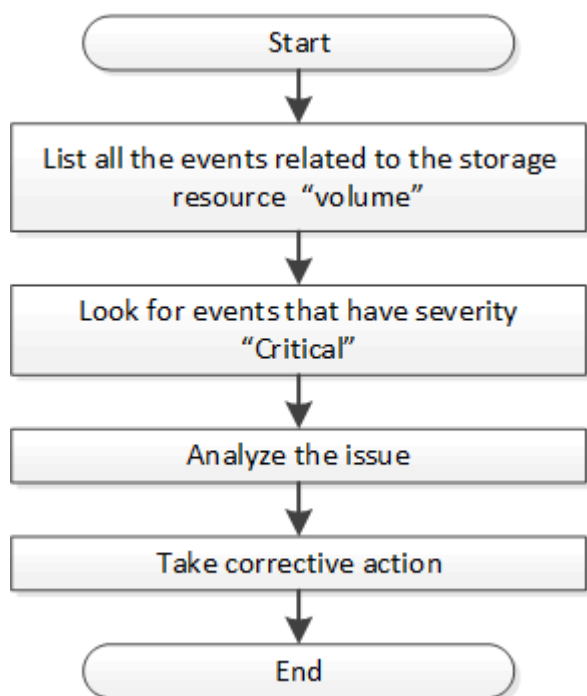
| 类别   | HTTP 动词 | 路径                          |
|------|---------|-----------------------------|
| 数据中心 | GET     | /datacenter/storage/volumes |

5. 分析哪些卷被过度利用。
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。

## 使用事件 API 确定存储对象中的问题

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，您可以分析问题并采取纠正措施，方法是使用 `events` 蜜蜂。

此工作流程以卷作为资源对象的示例。您可以使用 `events` API 用于检索与卷相关的事件列表，分析该卷的关键问题，然后采取纠正措施来纠正问题。



在采取补救措施之前，请按照以下步骤确定卷中的问题。

步骤

- 1. 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 动词 | 路径        |
|-------|---------|-----------|
| 管理服务器 | GET     | /管理服务器/事件 |

- 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 执行必要的操作来解决问题。

使用网关 API 对ONTAP卷进行故障排除

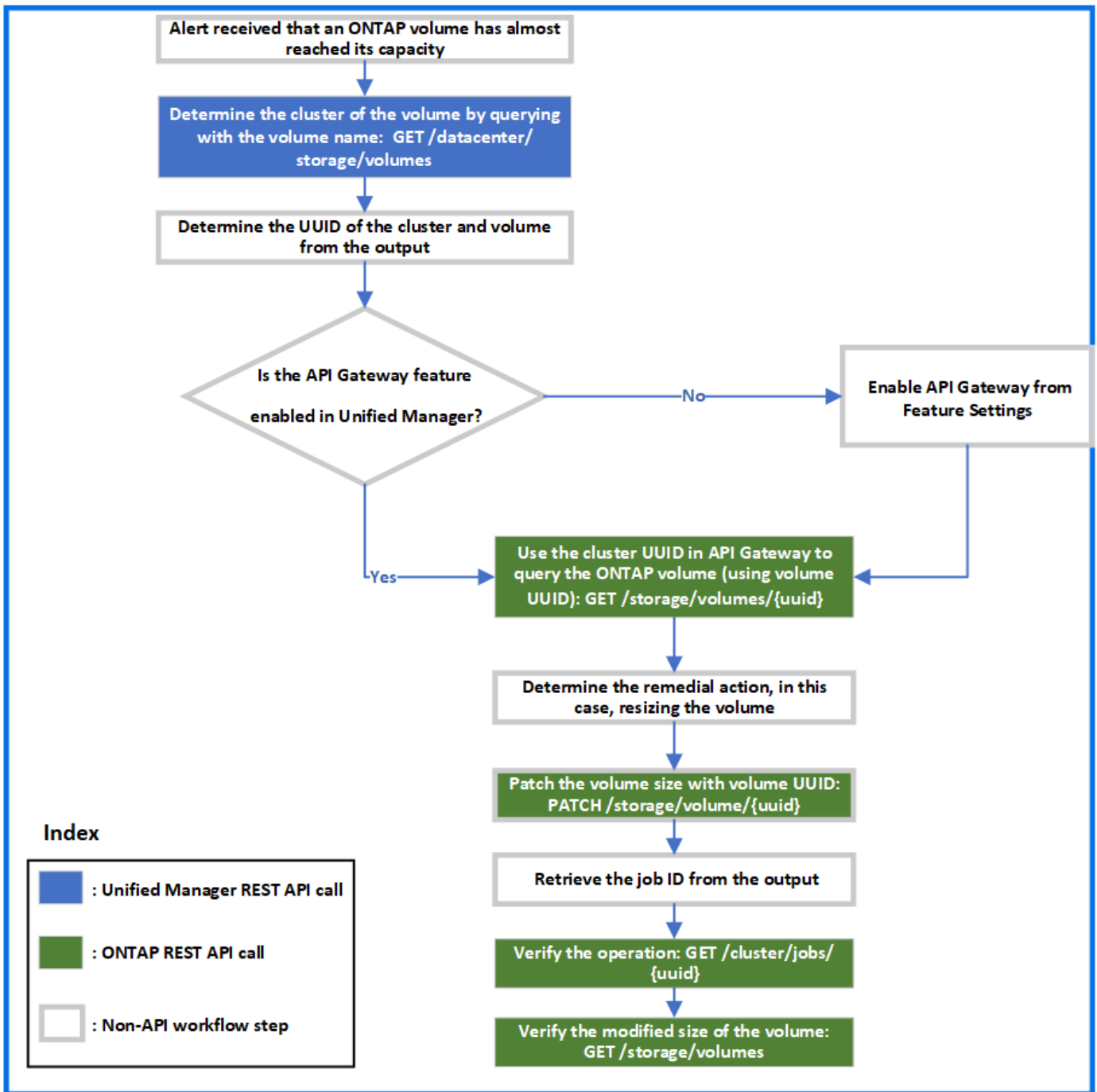
网关 API 充当网关，调用ONTAP API 来查询有关ONTAP存储对象的信息并采取补救措施来解决报告的问题。

此工作流程采用一个示例用例，其中当ONTAP卷几乎达到其容量时会引发一个事件。该工作流程还演示了如何通过调用Active IQ Unified Manager和ONTAP REST API 的组合来解决此问题。



- 在运行 workflow 步骤之前，请确保以下事项：
- 您了解网关 API 及其使用方法。有关信息，请参阅["通过代理访问ONTAP API"](#)。
  - 您了解ONTAP REST API 的用法。有关使用ONTAP REST API 的信息，请参阅<https://docs.netapp.com/us-en/ontap-automation/index.html>["ONTAP自动化文档"]。
  - 您是应用程序管理员。
  - 您要在其上运行 REST API 操作的集群受ONTAP 9.5 或更高版本支持，并且该集群通过 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中的每个步骤。



该工作流程涵盖 Unified Manager 和 ONTAP REST API 的调用点。

- 记下通知卷容量利用率的事件中的卷名称。
- 通过使用卷名称作为名称参数中的值，通过运行以下 Unified Manager API 来查询卷。

| 类别   | HTTP 动词 | 路径                          |
|------|---------|-----------------------------|
| 数据中心 | GET     | /datacenter/storage/volumes |

- 从输出中检索集群 UUID 和卷 UUID。

- 在 Unified Manager Web UI 上，导航到 常规 > 功能设置 > **API 网关** 以验证 API 网关功能是否已启用。除非启用，否则网关类别下的 API 不可供您调用。如果该功能被禁用，请启用它。
- 使用集群 UUID 运行ONTAP API`storage/volumes/{uuid}`通过 API 网关。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，并且您不需要为单个集群访问运行额外的身份验证步骤。

| 类别       | HTTP 动词 | 路径                                    |
|----------|---------|---------------------------------------|
| 统一管理器：网关 | GET     | 网关 API：<br>/gateways/{uuid}/{path}    |
| ONTAP：存储 |         | ONTAP API：<br>/storage/volumes/{uuid} |



在 /gateways/{uuid}/{path} 中，{uuid} 的值必须替换为要执行 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/lcd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

- 根据输出，确定大小、用途和要采取的补救措施。在此工作流程中，采取的补救措施是调整卷大小。
- 使用集群 UUID 并通过 API 网关运行以下ONTAP API 来调整卷大小。有关网关和ONTAP API 的输入参数的信息，请参阅步骤 5。

| 类别       | HTTP 动词 | 路径                                    |
|----------|---------|---------------------------------------|
| 统一管理器：网关 | 修补      | 网关 API：<br>/gateways/{uuid}/{path}    |
| ONTAP：存储 |         | ONTAP API：<br>/storage/volumes/{uuid} |



除了集群 UUID 和卷 UUID 之外，您还必须输入用于调整卷大小的参数值。确保以字节为单位输入值。例如，如果要将卷的大小从 100 GB 增加到 120 GB，请在查询末尾输入参数大小的值：`-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。

- 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，请参阅步骤 5。

| 类别       | HTTP 动词 | 路径                                 |
|----------|---------|------------------------------------|
| 统一管理器：网关 | GET     | 网关 API：<br>/gateways/{uuid}/{path} |
| ONTAP：集群 |         | ONTAP API：<br>/cluster/jobs/{uuid} |

返回的 HTTP 代码与 ONTAP REST API HTTP 状态代码相同。

- 运行以下 ONTAP API 来查询已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 动词 | 路径                                    |
|----------|---------|---------------------------------------|
| 统一管理器：网关 | GET     | 网关 API：<br>/gateways/{uuid}/{path}    |
| ONTAP：存储 |         | ONTAP API：<br>/storage/volumes/{uuid} |

输出显示卷大小增加到了 120 GB。

## 用于工作负载管理的 API workflow

使用 Active IQ Unified Manager，您可以配置和修改存储工作负载（LUN、NFS 文件共享和 CIFS 共享）。配置包括多个步骤，从创建存储虚拟机 (SVM) 到在存储工作负载上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和启用附加功能的步骤。

描述了以下工作流程：

- 在 Unified Manager 上配置存储虚拟机 (SVM) 的工作流程。



在 Unified Manager 上配置 LUN 或文件共享之前，需要执行此工作流程。

- 配置文件共享。
- 配置 LUN。
- 修改 LUN 和文件共享（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 升级到 AQoS



对于每个配置工作流程（LUN 和文件共享），请确保您必须已完成验证集群上的 SVM 的工作流程。

在工作流中使用每个 API 之前，您还必须阅读建议和限制。API 的相关详细信息可在相关概念和参考中列出的各个部分中找到。

使用 **API** 验证集群上的 **SVM**

在配置文件共享或 LUN 之前，您必须验证集群上是否创建了存储虚拟机 (SVM)。



该工作流程假定ONTAP集群已添加到 Unified Manager，并且已获取集群密钥。集群应具有配置 LUN 和文件共享所需的许可证。

1. 验证集群是否已创建 SVM。

| 类别   | HTTP 动词 | 路径                                                     |
|------|---------|--------------------------------------------------------|
| 数据中心 | GET     | /datacenter/svm/svms<br>/datacenter/svm/svms/{key<br>} |

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，您需要在其上配置 SVM 的集群密钥。您还需要指定 SVM 名称。请按照以下步骤操作。

| 类别   | HTTP 动词 | 路径                                                                 |
|------|---------|--------------------------------------------------------------------|
| 数据中心 | GET     | /datacenter/cluster/clusters<br>/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. 从输出中获取集群键，然后将其用作创建 SVM 的输入。



创建 SVM 时，确保它支持配置 LUN 及其上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，则配置工作流程可能会失败。建议在 SVM 上也启用相应类型工作负载的服务。

| 类别   | HTTP 动词 | 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\"] },
\"fcg\": { \"enabled\": true }, \"ip_interface\": [{ \"enabled\": true,
\"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" } },
\"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\":
\"dataLif1\" }], \"ipspace\": { \"name\": \"exchange\" },
\"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\",
\"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\",
\"bind_dn\": \"string\", \"enabled\": true, \"servers\": [\"string\"]
},
\"name\": \"svm1\", \"nfs\": { \"enabled\": true },
\"nis\": { \"domain\": \"string\", \"enabled\": true,
\"servers\": [\"string\"] }, \"nvme\": { \"enabled\": true },
\"routes\": [{ \"destination\": { \"address\": \"10.10.10.7\",
\"netmask\": \"24\" } }, \"gateway\": \"string\" }],
\"snapshot_policy\": { \"name\": \"default\" },
\"state\": \"running\", \"subtype\": \"default\"}"
```

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 SVM。

4. 使用作业对象键进行查询来验证 SVM 创建。如果 SVM 创建成功，则在响应中返回 SVM 密钥。

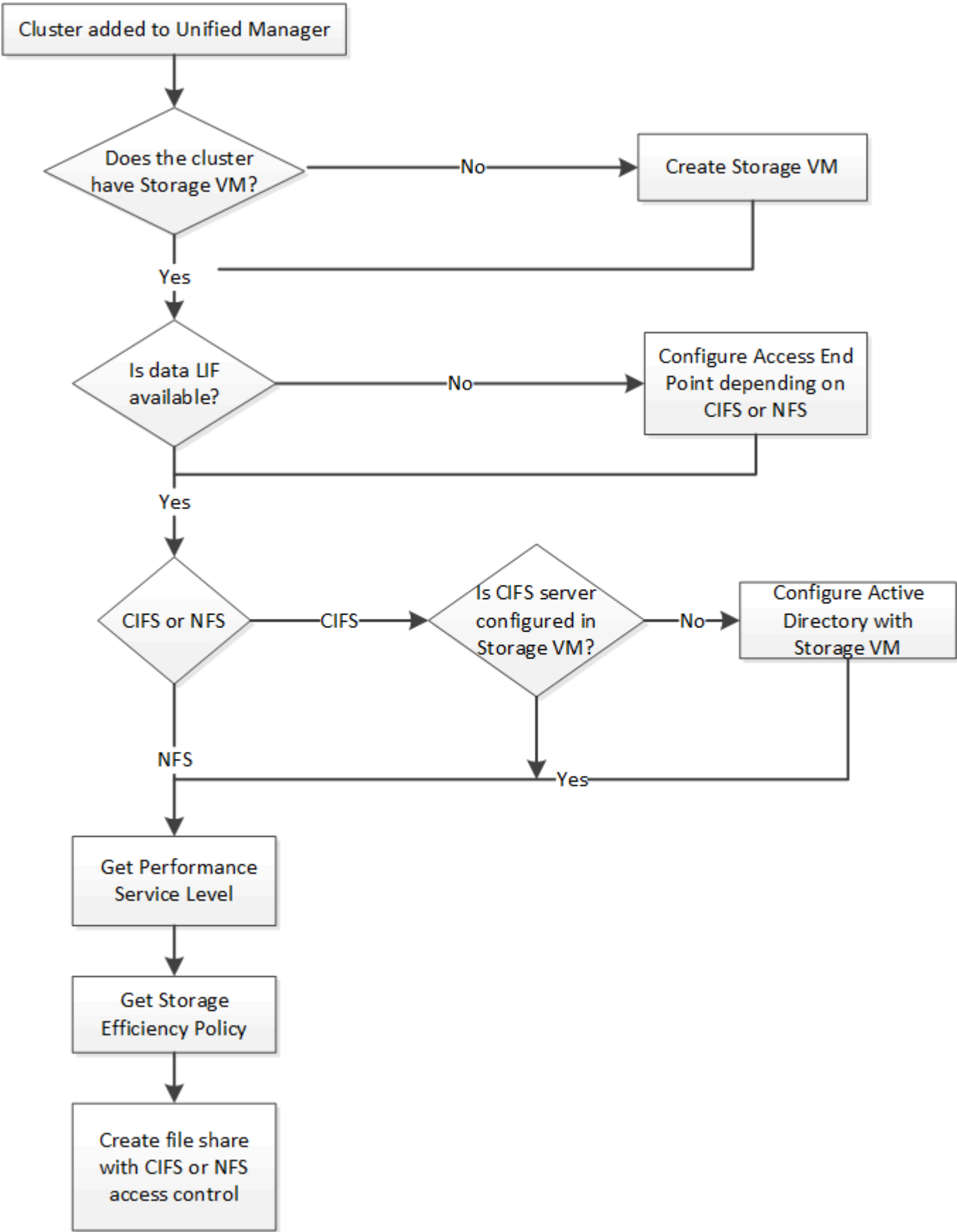
| 类别    | HTTP 动词 | 路径                            |
|-------|---------|-------------------------------|
| 管理服务器 | GET     | /management-server/jobs/{key} |

## 使用 API 预配 CIFS 和 NFS 文件共享

您可以使用Active IQ Unified Manager提供的配置 API 在存储虚拟机 (SVM) 上配置 CIFS 共享和 NFS 文件共享。此配置工作流程详细说明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配置工作流程中的每个步骤。它包括配置 CIFS 共享和 NFS 文件共享。



确保以下事项：



- ONTAP集群已添加到 Unified Manager，并且已获取集群密钥。
- 已在集群上创建 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 端口已在线，可供端口配置。

1. 确定要创建 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 动词 | 路径                                                                             |
|-------|---------|--------------------------------------------------------------------------------|
| 存储提供商 | GET     | /storage-provider/access-endpoints<br>/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，则获取访问端点密钥，否则创建访问端点。



确保创建已启用 CIFS 协议的访问端点。除非您创建了启用了 CIFS 协议的访问端点，否则配置 CIFS 共享将失败。

| 类别    | HTTP 动词 | 路径                                 |
|-------|---------|------------------------------------|
| 存储提供商 | POST    | /storage-provider/access-endpoints |

#### 示例 cURL

您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，您可以使用它来验证您创建的访问端点。

### 3. 验证访问端点：

| 类别    | HTTP 动词 | 路径                            |
|-------|---------|-------------------------------|
| 管理服务器 | GET     | /management-server/jobs/{key} |

### 4. 确定是否必须创建 CIFS 共享或 NFS 文件共享。要创建 CIFS 共享，请按照以下子步骤操作：

- a. 确定您的 SVM 上是否配置了 CIFS 服务器，即确定 SVM 上是否创建了 Active Directory 映射。

| 类别    | HTTP 动词 | 路径                                            |
|-------|---------|-----------------------------------------------|
| 存储提供商 | GET     | /storage-provider/active-directories-mappings |

- b. 如果创建了 Active Directory 映射，则获取密钥，否则在 SVM 上创建 Active Directory 映射。

| 类别    | HTTP 动词 | 路径                                            |
|-------|---------|-----------------------------------------------|
| 存储提供商 | POST    | /storage-provider/active-directories-mappings |

示例 **cURL**

您必须输入创建 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，则会显示错误消息，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\_验证集群上的 SVM\_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来获取性能服务级别的密钥。

| 类别    | HTTP 动词 | 路径                                           |
|-------|---------|----------------------------------------------|
| 存储提供商 | GET     | /storage-provider/performance-service-levels |



您可以通过设置 `system_defined`输入参数`true`。从输出中获取要在文件共享上应用的性能服务级别的密钥。

7. 或者，通过运行以下 API 并从响应中检索密钥，获取要在文件共享上应用的存储效率策略的存储效率策略密钥。

| 类别    | HTTP 动词 | 路径                                            |
|-------|---------|-----------------------------------------------|
| 存储提供商 | 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。如果您想要创建文件共享以仅支持卷上的一种协议，则以下子步骤将提供信息。您还可以在创建 NFS 共享后更新 NFS 文件共享以包含访问控制列表。有关信息，请参阅“修改存储工作负载”主题。
  - a. 要仅创建 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，在配置 CIFS/SMB 共享时都会创建一个 ACL。根据您为 ACL 和 Active Directory 映射输入的值，在创建 CIFS 共享时确定其访问控制和映射。

## 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，收集有关导出策略的信息。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，导出策略在创建时会附加到 NFS 文件共享。



在配置 NFS 共享时，您可以通过提供所有必需的值来创建导出策略，或者提供导出策略密钥并重用现有的导出策略。如果要重新使用存储虚拟机的导出策略，则需要添加导出策略密钥。除非您知道密钥，否则您可以使用 `/datacenter/protocols/nfs/export-policies` API。要创建新策略，您必须输入如以下示例所示的规则。对于输入的规则，API 尝试通过匹配主机、存储虚拟机和规则来搜索现有的导出策略。如果存在现有的导出策略，则使用该策略。否则，将创建新的出口政策。

## 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：



存储效率策略是创建文件共享的可选参数。

| 类别    | HTTP 动词 | 路径                            |
|-------|---------|-------------------------------|
| 存储提供商 | 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。。使用查询作业中返回的作业对象键来验证文件共享的创建：

| 类别    | HTTP 动词 | 路径                            |
|-------|---------|-------------------------------|
| 管理服务器 | GET     | /management-server/jobs/{key} |

在响应的末尾，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 动词 | 路径                                  |
|-------|---------|-------------------------------------|
| 存储提供商 | GET     | /storage-provider/file-shares/{key} |

JSON 输出示例

您可以看到 `storage-provider/file-shares` 内部调用每个函数所需的所有 API 并创建对象。例如，它调用 `storage-provider/performance-service-levels/` 用于分配文件共享上的性能服务级别的 API。

```

{
 "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_vsl",
 "_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",

```



```

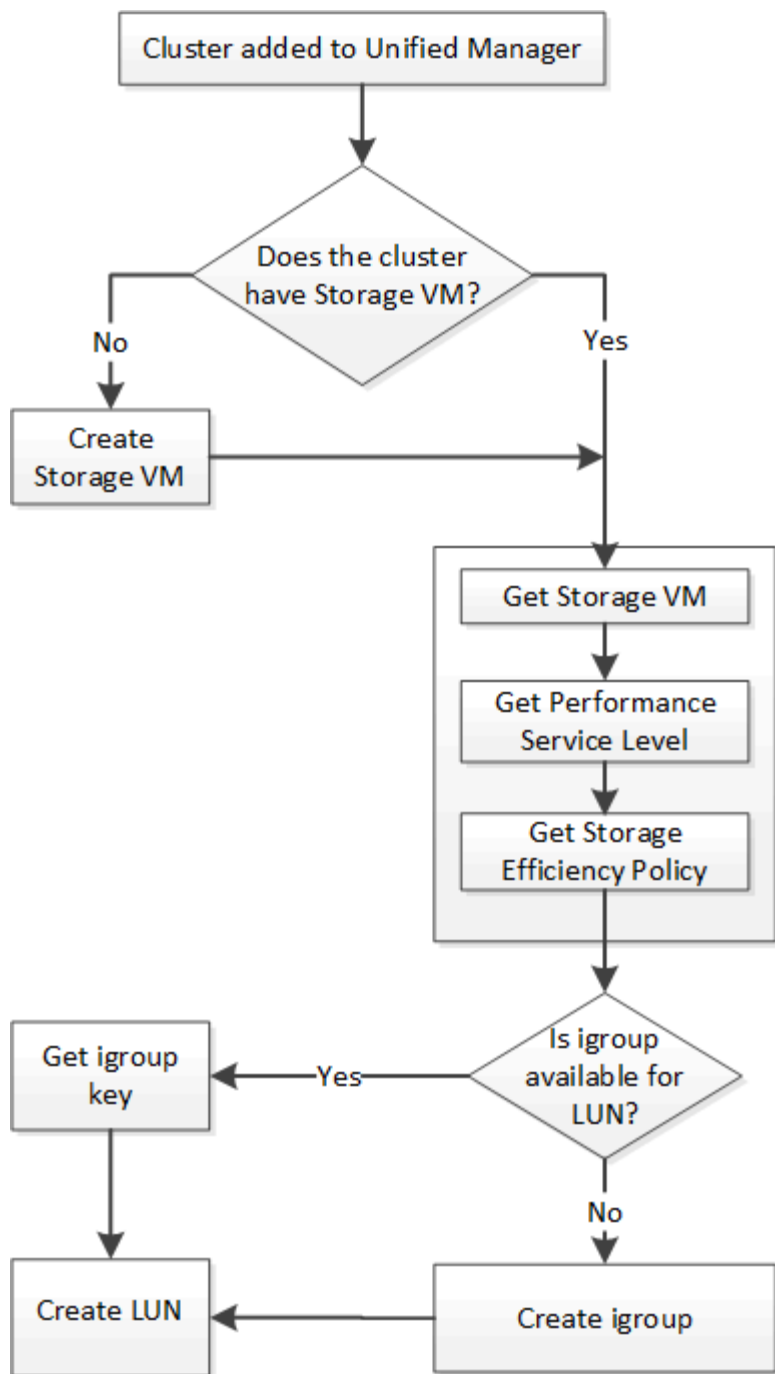
 "clients": [
 {
 "match": "0.0.0.0/0"
 }
],
 "index": 2,
 "protocols": [
 "cifs"
],
 "ro_rule": [
 "ntlm"
],
 "rw_rule": [
 "ntlm"
],
 "superuser": [
 "none"
]
 }
],
"_links": {
 "self": {
 "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
 }
}
},
"_links": {
 "self": {
 "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
 }
}
}
}

```

## 使用 API 预配 LUN

您可以使用Active IQ Unified Manager提供的配置 API 在存储虚拟机 (SVM) 上配置 LUN。此配置工作流程详细说明了在创建 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 配置工作流程中的步骤。



此工作流程假定ONTAP集群已添加到 Unified Manager，并且已获取集群密钥。该工作流还假设已在集群上创建了 SVM。

1. 获取要在其上创建 LUN 的 SVM 的 SVM 密钥，如\_验证集群上的 SVM\_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来获取性能服务级别的密钥。

| 类别    | HTTP 动词 | 路径                                           |
|-------|---------|----------------------------------------------|
| 存储提供商 | GET     | /storage-provider/performance-service-levels |



您可以通过设置 `system_defined`输入参数`true`。从输出中获取要在 LUN 上应用的性能服务级别的密钥。

- 或者，通过运行以下 API 并从响应中检索密钥，获取要在 LUN 上应用的存储效率策略的存储效率策略密钥。

| 类别    | HTTP 动词 | 路径                                            |
|-------|---------|-----------------------------------------------|
| 存储提供商 | GET     | /storage-provider/storage-efficiency-policies |

- 确定是否已创建启动程序组 (igroup) 来授予对要创建的 LUN 目标的访问权限。

| 类别   | HTTP 动词 | 路径                                                                           |
|------|---------|------------------------------------------------------------------------------|
| 数据中心 | GET     | /datacenter/protocols/san/igroups<br>/datacenter/protocols/san/igroups/{key} |

您必须输入参数值来指示 igroup 有权访问的 SVM。此外，如果您想查询特定的 igroup，请输入 igroup 名称（键）作为输入参数。

- 在输出中，如果您可以找到要授予访问权限的 igroup，请获取密钥。否则创建 igroup。

| 类别   | HTTP 动词 | 路径                                |
|------|---------|-----------------------------------|
| 数据中心 | POST    | /datacenter/protocols/san/igroups |

您必须输入要创建的 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 igroup 的创建。如果出现错误，则会显示一条消息，以便您排除故障并重新运行 API。

- 创建 LUN。

| 类别    | HTTP 动词 | 路径                     |
|-------|---------|------------------------|
| 存储提供商 | POST    | /storage-provider/luns |

要创建 LUN，请确保已将检索到的值添加为强制输入参数。



存储效率策略是创建 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 输出显示一个作业对象键，您可以使用它来验证您创建的 LUN。

7. 使用查询作业中返回的作业对象键来验证 LUN 的创建：

| 类别    | HTTP 动词 | 路径                            |
|-------|---------|-------------------------------|
| 管理服务器 | GET     | /management-server/jobs/{key} |

在响应的末尾，您会看到创建的 LUN 的密钥。

8. 通过使用返回的密钥运行以下 API 来验证 LUN 的创建：

| 类别    | HTTP 动词 | 路径                           |
|-------|---------|------------------------------|
| 存储提供商 | GET     | /storage-provider/luns/{key} |

JSON 输出示例

您可以看到 `/storage-provider/luns` 内部调用每个函数所需的所有 API 并创建对象。例如，它调用 `/storage-provider/performance-service-levels/` 用于在 LUN 上分配性能服务级别的 API。

== LUN 创建或映射失败的故障排除步骤

完成此工作流程后，您可能仍会看到 LUN 创建失败。即使成功创建了 LUN，由于创建 LUN 的节点上 SAN LIF 或访问端点不可用，LUN 与 igroup 的映射也可能会失败。如果发生故障，您将看到以下消息：

```
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.
```

请按照以下故障排除步骤来解决此故障。

1. 在您尝试创建 LUN 的 SVM 上创建支持 iSCSI/FCP 协议的访问端点。

| 类别    | HTTP 动词 | 路径                                 |
|-------|---------|------------------------------------|
| 存储提供商 | POST    | /storage-provider/access-endpoints |

示例 cURL

您必须输入要创建的访问端点的详细信息作为输入参数。



确保在输入参数中已添加指示 LUN 主节点的地址和指示主节点的伙伴节点的 `ha_address`。当您运行此操作时，它会在主节点和伙伴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，以验证它是否已成功运行以在 SVM 上添加访问端点，以及是否已在 SVM 上启用 iSCSI/FCP 服务。

| 类别    | HTTP 动词 | 路径                            |
|-------|---------|-------------------------------|
| 管理服务器 | GET     | /management-server/jobs/{key} |

#### JSON 输出示例

在输出的最后，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”值表示在主节点的伙伴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。有关工作流程修改的更多信息，请参阅“修改存储工作负载”。

| 类别    | HTTP 动词 | 路径                          |
|-------|---------|-----------------------------|
| 存储提供商 | 修补      | /storage-provider/lun/{key} |

在输入中，指定要用来更新 LUN 映射的 igroup 键以及 LUN 键。

#### 示例 cURL

JSON 输出显示一个 Job 对象键，您可以使用它来验证映射是否成功。

4. 通过查询 LUN 键来验证 LUN 映射。

| 类别    | HTTP 动词 | 路径                           |
|-------|---------|------------------------------|
| 存储提供商 | GET     | /storage-provider/luns/{key} |

#### JSON 输出示例

在输出中，您可以看到 LUN 已成功映射到最初配置的 igroup（键 d19ec2fa-fec7-11e8-b23d-00a098e32c28）。

### 使用 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，或者更改现有参数。

此工作流程以更新 LUN 和文件共享的性能服务级别为例。



工作流程假定 LUN 或文件共享已配置性能服务级别。

修改文件共享时，您可以更新以下参数：

- 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恢复文件共享上的默认（空）导出策略规则。

 在单个 API 运行期间，您只能更新一个参数。

此过程描述了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 动词 | 路径                            |
|-------|---------|-------------------------------|
| 存储提供商 | GET     | /storage-provider/file-shares |

2. 使用您获取的文件共享密钥运行以下 API 来查看文件共享的详细信息。

| 类别    | HTTP 动词 | 路径                                  |
|-------|---------|-------------------------------------|
| 存储提供商 | 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. 获取您想要在此文件共享上分配的性能服务级别的密钥。目前尚未为其分配任何策略。

| 类别     | HTTP 动词 | 路径                                           |
|--------|---------|----------------------------------------------|
| 性能服务级别 | GET     | /storage-provider/performance-service-levels |



您可以通过设置 `system_defined`` 输入参数 ``true`。从输出中获取要应用于文件共享的性能服务级别的密钥。

#### 4. 在文件共享上应用性能服务级别。

| 类别    | HTTP 动词 | 路径                                  |
|-------|---------|-------------------------------------|
| 存储提供商 | 修补      | /storage-provider/file-shares/{key} |

在输入中，您必须仅指定要更新的参数以及文件共享密钥。在这种情况下，它是性能服务水平的关键。

#### 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 Job 对象，您可以使用它来验证主节点和合作伙伴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性能服务级别是否已添加到文件共享。

| 类别    | HTTP 动词 | 路径                            |
|-------|---------|-------------------------------|
| 管理服务器 | GET     | /management-server/jobs/{key} |

如果通过作业对象的 ID 进行查询，您可以看到文件共享是否已成功更新。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 动词 | 路径                                  |
|-------|---------|-------------------------------------|
| 存储提供商 | 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，您可以修改以下参数：

- 容量或尺寸
- 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。

此过程描述了向 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 返回数据中心内所有 LUNS 的详细信息。如果您已经知道 LUN 密钥，请跳过此步骤。

| 类别    | HTTP 动词 | 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 来查看 LUN 的详细信息。

| 类别    | HTTP 动词 | 路径                           |
|-------|---------|------------------------------|
| 存储提供商 | GET     | /storage-provider/luns/{key} |

在输出中查看 LUN 的详细信息。您可以看到没有为该 LUN 分配性能服务级别。

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 的性能服务级别的密钥。

| 类别     | HTTP 动词 | 路径                                           |
|--------|---------|----------------------------------------------|
| 性能服务级别 | GET     | /storage-provider/performance-service-levels |



您可以通过设置 `system_defined`` 输入参数 ``true`。从输出中获取要在 LUN 上应用的性能服务级别的密钥。

### 4. 在 LUN 上应用性能服务级别。

| 类别    | HTTP 动词 | 路径                          |
|-------|---------|-----------------------------|
| 存储提供商 | 修补      | /storage-provider/lun/{key} |

在输入中，您必须仅指定要更新的参数以及 LUN 键。在这种情况下，它是性能服务水平的关键。

#### 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 输出显示一个作业对象键，您可以使用它来验证已更新的 LUN。

### 5. 使用您获取的 LUN 密钥运行以下 API 来查看 LUN 的详细信息。

| 类别    | HTTP 动词 | 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 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。在创建文件共享期间，可以为同一个文件共享指定访问控制列表 (ACL) 参数和导出策略规则。但是，如果您想在创建 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来创建 NFS 文件共享。有关信息，请参阅 [\\_管理文件共享\\_](#) 和 [\\_修改存储工作负载\\_](#)。
2. 您必须拥有文件共享密钥才能运行此操作。有关查看文件共享详细信息和使用作业 ID 检索文件共享密钥的信息，请参阅 [\\_配置 CIFS 和 NFS 文件共享\\_](#)。

这适用于您通过仅添加导出策略规则而不是 ACL 参数创建的 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，执行 `PATCH` 使用允许 CIFS 访问的 ACL 详细信息进行操作。

| 类别    | HTTP 动词 | 路径                            |
|-------|---------|-------------------------------|
| 存储提供商 | 修补      | /storage-provider/file-shares |

#### 示例 cURL

根据您分配给用户组的访问权限（如以下示例所示），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. 通过查询同一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 动词 | 路径                                  |
|-------|---------|-------------------------------------|
| 存储提供商 | 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、专利等的访问。

## 版权

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## 商标

NETAPP、NETAPP 徽标和NetApp商标页面上列出的标志是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/"](https://www.netapp.com/company/legal/trademarks/)

## 专利

NetApp拥有的专利的最新列表可以在以下位置找到：

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## 隐私政策

["https://www.netapp.com/company/legal/privacy-policy/"](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 9.16 通知"](#)

## 版权信息

版权所有 © 2025 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。