Active IQ Unified Manager Dokumentation

Active IQ Unified Manager

NetApp
November 13, 2026

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

Inhalt

Active IQ Unified Manager Dokumentation . . . 1
Versionshinweise für Active IQ Unified Manager . . . 2
Los geht’s . . . 3
Erste Schritte mit Active IQ Unified Manager auf VMware vSphere . . . 3
Systemvoraussetzungen . . . 3
Active IQ Unified Manager installieren . . . 3
Erste Schritte mit Active IQ Unified Manager unter Linux . . . 4
Systemvoraussetzungen . . . 4
Active IQ Unified Manager installieren . . . 4
Erste Schritte mit Active IQ Unified Manager unter Windows . . . 5
Systemvoraussetzungen . . . 5
Active IQ Unified Manager installieren . . . 6
Installation von Unified Manager auf VMware vSphere Systemen . . . 7
Informationen zu Active IQ Unified Manager . . . 7
Informationen zu Active IQ Unified Manager . . . 7
Informationen zu den Funktionen des Active IQ Unified Manager Servers . . . 7
Informationen zur Installationsreihenfolge von Active IQ Unified Manager . . . 7
Voraussetzungen für die Installation von Unified Manager . . . 8
Es muss sichergestellt werden, dass der Server die Installationsanforderungen für Active IQ Unified Manager erfüllt. . . . 8
Informationen zur virtuellen Infrastruktur und zu den Hardwareanforderungen für Active IQ Unified Manager . . . 8
Informationen zur VMware Software und zu den Installationsvoraussetzungen für Active IQ Unified Manager . . . 10
Unterstützte Browser in Active IQ Unified Manager . . . 10
Informationen zu Protokoll- und Portanforderungen für Active IQ Unified Manager . . . 11
Das Arbeitsblatt in Active IQ Unified Manager wird vervollständigt . . . 14
Installation, Upgrade und Entfernung von Unified Manager auf VMware vSphere . . . 16
Informationen zum Active IQ Unified Manager Bereitstellungsprozess . . . 16
Workflow für die Bereitstellung der virtuellen Unified Manager Appliance . . . 17
Upgrade Workflow für die virtuelle Unified Manager Appliance . . . 20
Starten Sie die virtuelle Maschine Active IQ Unified Manager neu. . . . 23
Active IQ Unified Manager entfernen . . . 24
Installation von Unified Manager auf Linux-Systemen . . . 25
Einführung in Active IQ Unified Manager . . . 25
Informationen zu Active IQ Unified Manager . . . 25
Was der Active IQ Unified Manager Server bewirkt . . . 25
Installationssequenz für Active IQ Unified Manager anzeigen . . . 25
Voraussetzungen für die Installation von Unified Manager . . . 26
Die Anforderungen für die Installation von Active IQ Unified Manager verstehen . . . 26
Informationen zu virtueller Infrastruktur und Hardwareanforderungen für Active IQ Unified Manager . . . 26
Informationen zu Linux-Software und Installationsvoraussetzungen in Active IQ Unified Manager . . . 28
Unterstützte Browser für Active IQ Unified Manager verwenden . . . 31

Informationen zu Protokoll- und Portanforderungen in Active IQ Unified Manager . . . 31
Das Arbeitsblatt in Active IQ Unified Manager wird vervollständigt . . . 34
Unified Manager Software installieren, aktualisieren und entfernen . . . 35
Installation, Aktualisierung und Deinstallation der Active IQ Unified Manager Software . . . 36
Die Installationsreihenfolge für Active IQ Unified Manager auf Red Hat Enterprise Linux . . . 36
Einrichtung der erforderlichen Software . . . 36
SELinux für NFS- und CIFS-Freigaben in Active IQ Unified Manager konfigurieren . . . 39
Installation von Unified Manager auf Linux-Systemen . . . 42
Upgrade von Unified Manager auf Red Hat Enterprise Linux . . . 49
Aktualisierung von Drittanbieterprodukten nach der Installation von Unified Manager . . . 54
Active IQ Unified Manager neu starten . . . 55
Active IQ Unified Manager entfernen . . . 56
Der benutzerdefinierte Benutzer „umadmin“ und die Wartungsgruppe für Active IQ Unified Manager werden entfernt . . . 57
Unified Manager auf Windows-Systemen installieren . . . 58
Einführung in Active IQ Unified Manager . . . 58
Informationen zu Active IQ Unified Manager . . . 58
Informationen zu den Funktionen des Active IQ Unified Manager Servers . . . 58
Informationen zur Installationsreihenfolge für Active IQ Unified Manager . . . 58
Voraussetzungen für die Installation von Unified Manager . . . 59
Es muss sichergestellt werden, dass der Server die Installationsanforderungen für Active IQ Unified Manager erfüllt. . . . 59
Informationen zu virtueller Infrastruktur und Hardwareanforderungen für Active IQ Unified Manager . . . 59
Informationen zu den Windows-Software- und Installationsanforderungen für Active IQ Unified Manager . . . 61
Unterstützte Browser in Active IQ Unified Manager . . . 62
Protokoll- und Portanforderungen für Active IQ Unified Manager verstehen . . . 63
Das Arbeitsblatt in Active IQ Unified Manager wird vervollständigt . . . 66
Unified Manager Software installieren, aktualisieren und entfernen . . . 67
Informationen zum Installationsprozess für Active IQ Unified Manager unter Windows . . . 67
Unified Manager unter Windows installieren . . . 68
Änderung des JBoss Passworts unter Windows in Active IQ Unified Manager . . . 71
Der unterstützte Upgrade-Pfad für Versionen von Active IQ Unified Manager ist zu verwenden . . . 72
Aktualisierung von Active IQ Unified Manager unter Windows . . . 73
Aktualisierung von Drittanbieterprodukten . . . 74
Deinstallation von Drittanbieterprodukten in Active IQ Unified Manager . . . 75
Neustart von Active IQ Unified Manager unter Windows . . . 76
Deinstallation von Active IQ Unified Manager . . . 76
Konfigurations- und Verwaltungsaufgaben durchführen . . . 78
Konfigurieren von Active IQ Unified Manager . . . 78
Informationen zur Konfiguration von Active IQ Unified Manager . . . 78
Informationen zur Konfigurationsreihenfolge in Active IQ Unified Manager . . . 78
Zugriff auf die Web-Benutzeroberfläche in Active IQ Unified Manager . . . 78
Die Ersteinrichtung der Active IQ Unified Manager Weboberfläche wird durchgeführt. . . . 79
Cluster zu Active IQ Unified Manager hinzufügen . . . 81

Benachrichtigungen konfigurieren . . . 83
Das lokale Benutzerkennwort in Active IQ Unified Manager kann geändert werden. . . . 92
Die Zeitüberschreitung bei Sitzungsinaktivität in Active IQ Unified Manager festlegen . . . 93
Die Zeitüberschreitung der Sitzung kann über die CLI in Active IQ Unified Manager festgelegt werden. . . 93
Der Hostname von Unified Manager kann geändert werden . . . 94
Aktivieren und Deaktivieren der richtlinienbasierten Speicherverwaltung in Active IQ Unified Manager . . . 98
Active IQ Unified Manager Sicherung konfigurieren . . . 99
Funktionseinstellungen managen . . . 99
Informationen zu Funktionseinstellungen in Active IQ Unified Manager . . . 99
Die richtlinienbasierte Speicherverwaltung in Active IQ Unified Manager kann aktiviert werden . . . 100
Informationen zur API Gateway Funktion in Active IQ Unified Manager . . . 100
Angeben der Zeitüberschreitung bei Inaktivität in Active IQ Unified Manager . . . 101
Aktivierung von Active IQ Portalereignissen in Active IQ Unified Manager . . . 101
Aktivieren und Deaktivieren von Sicherheitseinstellungen für die Compliance in Active IQ Unified Manager . . . 102
Aktivieren und Deaktivieren des Skript-Uploads in Active IQ Unified Manager . . . 103
Hinzufügen eines Anmeldebanners in Active IQ Unified Manager . . . 103
Verwendung der Managementplattform . . . 103
Informationen zur Wartungskonsole in Active IQ Unified Manager . . . 103
Informationen zum Wartungsbenutzer in Active IQ Unified Manager . . . 104
Diagnosefunktionen für Benutzer in Active IQ Unified Manager . . . 104
Zugriff auf die Wartungskonsole in Active IQ Unified Manager . . . 104
Zugriff auf die Wartungskonsole über die vSphere VM-Konsole in Active IQ Unified Manager . . . 105
Menüs der Managementplattform für die Wartung . . . 106
Das Kennwort des Wartungsbenutzers unter Windows in Active IQ Unified Manager ändern . . . 111
Ändern des Active IQ Unified Manager umadmin Passworts auf Linux Systemen . . . 111
Die von Active IQ Unified Manager für die HTTP- und HTTPS-Protokolle verwendeten Ports können geändert werden. . . . 112
Netzwerkschnittstellen zu Active IQ Unified Manager hinzufügen . . . 113
Das Clientzertifikat in Active IQ Unified Manager neu generieren . . . 113
Festplattenspeicher hinzufügen . . . 114
Benutzerzugriff verwalten . . . 117
Benutzer hinzufügen . . . 118
Benutzereinstellungen in Active IQ Unified Manager bearbeiten . . . 119
Benutzer in Active IQ Unified Manager anzeigen . . . 119
Löschen von Benutzern oder Gruppen in Active IQ Unified Manager . . . 120
Informationen zur rollenbasierten Zugriffssteuerung in Active IQ Unified Manager . . . 120
Informationen zu Benutzertypen in Active IQ Unified Manager . . . 121
Informationen zu Benutzerrollen in Active IQ Unified Manager . . . 121
Informationen zu Benutzerrollen und Berechtigungen in Active IQ Unified Manager . . . 122
Verwalten der SAML-Authentifizierungseinstellungen . . . 124
SAML Authentifizierung in Active IQ Unified Manager ist aktiviert . . . 124
Verwendung eines Identitätsanbieters in Active IQ Unified Manager . . . 124
SAML Authentifizierung in Active IQ Unified Manager ist aktiviert . . . 126
Änderung des SAML Authentifizierungs-Identitätsanbieters in Active IQ Unified Manager . . . 127

Aktualisierung der SAML-Authentifizierungseinstellungen nach einer Änderung des Active IQ Unified Manager Sicherheitszertifikats . . . 128
SAML Authentifizierung in Active IQ Unified Manager deaktivieren . . . 129
Die SAML Authentifizierung wird über die Active IQ Unified Manager Wartungskonsole deaktiviert. . . . 130
Die SAML Authentifizierungsseite in Active IQ Unified Manager kann verwendet werden . . . 130
Authentifizierung verwalten . . . 131
Bearbeiten von Authentifizierungsservern in Active IQ Unified Manager . . . 131
Authentifizierungsserver in Active IQ Unified Manager löschen . . . 132
Authentifizierung mit Active Directory oder OpenLDAP in Active IQ Unified Manager . . . 132
Audit-Logging . . . 133
Die Seite „Remote-Authentifizierung“ in Active IQ Unified Manager . . . 135
Sicherheitszertifikate verwalten . . . 139
Das HTTPS-Sicherheitszertifikat in Active IQ Unified Manager anzeigen . . . 139
Herunterladen einer HTTPS-Zertifikatsignierungsanforderung in Active IQ Unified Manager . . . 139
Installation eines von einer Zertifizierungsstelle signierten HTTPS-Zertifikats in Active IQ Unified Manager . . . 140
Informationen zu HTTPS-Zertifikaten, die mit externen Tools in Active IQ Unified Manager Unified Manager generiert wurden . . . 141
Seitenbeschreibungen für die Zertifikatsverwaltung . . . 143
Storage überwachen und managen . . . 146
Einführung in Active IQ Unified Manager . . . 146
Informationen zu Active IQ Unified Manager . . . 146
Informationen zur Zustandsüberwachung in Active IQ Unified Manager . . . 146
Informationen zur Leistungsüberwachung in Active IQ Unified Manager . . . 147
Active IQ Unified Manager REST APIs verwenden . . . 148
Was der Unified Manager Server leistet . . . 148
Die Benutzeroberfläche verstehen . . . 149
Informationen zur Active IQ Unified Manager Benutzeroberfläche . . . 149
Typische Fensterlayouts in Active IQ Unified Manager . . . 149
Anpassen des Fensterlayouts in Active IQ Unified Manager . . . 150
Verwendung der Active IQ Unified Manager Hilfe . . . 151
Lesezeichen für bevorzugte Hilfethemen in Active IQ Unified Manager . . . 152
Suche nach Speicherobjekten in Active IQ Unified Manager . . . 152
Speicherdaten können in Active IQ Unified Manager als Berichte exportiert werden . . . 153
Inhalte der Inventarseite in Active IQ Unified Manager filtern . . . 155
Aktive Ereignisse können über die Benachrichtigungsglocke in Active IQ Unified Manager angezeigt werden . . . 156
Überwachung und Management von Clustern über das Dashboard . . . 156
Cluster lassen sich über das Dashboard in Active IQ Unified Manager überwachen und verwalten . . . 156
Informationen zur Dashboard-Seite von Active IQ Unified Manager . . . 157
ONTAP Probleme direkt aus Unified Manager beheben oder managen . . . 160
Cluster verwalten . . . 167
Informationen zur Funktionsweise des Cluster-Erkennungsprozesses in Active IQ Unified Manager . . . 167
Liste der von Active IQ Unified Manager überwachten Cluster . . . 168
Cluster zu Active IQ Unified Manager hinzufügen . . . 169

Bearbeiten der Clustereinstellungen in Active IQ Unified Manager . . . 171
Entfernung von Clustern aus Active IQ Unified Manager . . . 172
Cluster in Active IQ Unified Manager erneut erkennen . . . 173
Überwachung der VMware virtuellen Infrastruktur . . . 173
Informationen dazu, wie Active IQ Unified Manager die virtuelle Infrastruktur von VMware überwacht . . . 173
vCenter Server in Active IQ Unified Manager anzeigen und hinzufügen . . . 177
Entfernung eines vCenter Server aus Active IQ Unified Manager . . . 179
Informationen dazu, wie Active IQ Unified Manager virtuelle Maschinen überwacht . . . 179
Sichtbarkeit der virtuellen Infrastruktur in einer Disaster Recovery Einrichtung mit Active IQ Unified Manager . . . 181
Provisionierung und managen von Workloads . . . 183
Bereitstellen und Verwalten von Workloads in Active IQ Unified Manager . . . 183
Übersicht über Workloads . . . 184
Verwalten von Performance Service Levels . . . 191
Verwaltung von Richtlinien zur Storage-Effizienz . . . 198
Management und Überwachung von MetroCluster Konfigurationen . . . 200
Informationen zum Volume Verhalten bei Umschaltung und Rückschaltung in Active IQ Unified Manager . . . 200
Grundlegendes zur Cluster-Konnektivität in einer MetroCluster FC Konfiguration in Active IQ Unified Manager . . . 202
Informationen zu MetroCluster über FC-Datenspiegelung in Active IQ Unified Manager . . . 203
Überwachung von MetroCluster Konfigurationen in Active IQ Unified Manager . . . 204
Überwachung der MetroCluster Replikation in Active IQ Unified Manager . . . 207
Quoten managen . . . 208
Informationen zu Kontingentgrenzen in Active IQ Unified Manager . . . 208
Benutzer- und Benutzergruppenkontingente in Active IQ Unified Manager anzeigen . . . 208
Regeln zum Generieren von E-Mail-Adressen in Active IQ Unified Manager . . . 208
Ein E-Mail-Benachrichtigungsformat für Benutzer- und Gruppenkontingente in Active IQ Unified Manager erstellen . . . 209
Bearbeiten von E-Mail-Adressen für Benutzer- und Gruppenkontingente in Active IQ Unified Manager 210
Weitere Informationen zu Quoten . . . 211
Beschreibung der Dialogfelder für Kontingente . . . 211
Fehlerbehebung . . . 215
Hinzufügen von Speicherplatz zum Unified Manager Datenbankverzeichnis . . . 215
Das Erfassungsintervall für Leistungsstatistiken in Active IQ Unified Manager ändern . . . 218
Ändern der Zeitspanne, für die Active IQ Unified Manager Ereignis- und Leistungsdaten speichert . . . 219
Behebung eines unbekannten Authentifizierungsfehlers in Active IQ Unified Manager . . . 220
Behebung eines Fehlers „Benutzer nicht gefunden“ in Active IQ Unified Manager . . . 221
Behebung des Problems, das durch das Hinzufügen von LDAP über den Authentifizierungsdienst „Other authentication service“ in Active IQ Unified Manager verursacht wird . . . 221
Behebung eines Problems mit der Protokollrotation des NetApp Manageability SDK in Active IQ Unified Manager . . . 222
Verwalten von Ereignissen und Warnmeldungen . . . 223
Ereignisse managen . . . 223
Informationen zu Active IQ Plattformereignissen in Active IQ Unified Manager . . . 223

Was Event Management System Ereignisse sind . . . 223
Hier wird erläutert, wie Active IQ Unified Manager ein empfangenes Ereignis verarbeitet . . . 228
Ereignisdetails in Active IQ Unified Manager . . . 229
Nicht zugewiesene Ereignisse in Active IQ Unified Manager . . . 230
Bestätigen und Beheben von Ereignissen in Active IQ Unified Manager . . . 230
Zuweisung von Ereignissen an bestimmte Benutzer in Active IQ Unified Manager . . . 231
Unerwünschte Ereignisse in Active IQ Unified Manager deaktivieren . . . 232
Probleme lassen sich mithilfe der automatischen Fehlerbehebung in Active IQ Unified Manager beheben . . . 233
Aktivieren und Deaktivieren der Active IQ Ereignisberichterstattung in Active IQ Unified Manager . . . 234
Hochladen einer neuen Active IQ Regeldatei in Active IQ Unified Manager . . . 235
Wie Active IQ Unified Manager Active IQ-Plattformereignisse generiert . . . 236
Active IQ Plattformereignisse in Active IQ Unified Manager beheben . . . 236
Konfiguration der Einstellungen zur Ereignisaufbewahrung in Active IQ Unified Manager . . . 237
Was ein Wartungsfenster für Unified Manager ist . . . 237
Verwalten von Hostsystemressourcenereignissen in Active IQ Unified Manager . . . 240
Mehr über Ereignisse . . . 240
Liste der Ereignisse und Schweregrade . . . 246
Beschreibung von Ereignisfenstern und Dialogfeldern . . . 298
Benachrichtigungen verwalten . . . 311
Informationen zu Warnmeldungen in Active IQ Unified Manager . . . 311
Informationen in einer Active IQ Unified Manager Benachrichtigungs-E-Mail . . . 311
Benachrichtigungen hinzufügen . . . 312
Hinzufügen von Warnmeldungen für Leistungsereignisse in Active IQ Unified Manager . . . 315
Warnungen in Active IQ Unified Manager testen . . . 316
Benachrichtigungen für gelöste und veraltete Ereignisse in Active IQ Unified Manager deaktivieren . . . 317
Ausschluss von Ziel-Volumes für die Notfallwiederherstellung von der Generierung von Warnmeldungen in Active IQ Unified Manager . . . 317
Anzeigen von Warnmeldungen in Active IQ Unified Manager . . . 318
Benachrichtigungen in Active IQ Unified Manager bearbeiten . . . 318
Warnmeldungen in Active IQ Unified Manager löschen . . . 319
Beschreibung von Warnfenstern und Dialogfeldern . . . 319
Skripte managen . . . 325
Skripte in Active IQ Unified Manager verwalten . . . 325
Wie Skripte mit Warnmeldungen in Active IQ Unified Manager funktionieren . . . 326
Skripte in Active IQ Unified Manager hinzufügen . . . 327
Skripte in Active IQ Unified Manager löschen . . . 328
Ausführung des Testskripts in Active IQ Unified Manager . . . 328
Informationen zu den unterstützten Active IQ Unified Manager CLI Befehlen . . . 329
Beschreibung der Skriptfenster und Dialogfelder . . . 334
Cluster Performance überwachen und managen . . . 336
Einführung in die Performance-Überwachung mit Active IQ Unified Manager . . . 336
Informationen zur Leistungsüberwachung in Active IQ Unified Manager . . . 336
Die Leistungsüberwachungsfunktionen von Active IQ Unified Manager können erkundet werden. . . . 336
Mit Active IQ Unified Manager Schnittstellen lässt sich die Leistung des Speichersystems verwalten. . . 337

Clusterkonfiguration und Leistungsdaten in Active IQ Unified Manager anzeigen . . . 337
Informationen zu Datenerfassungszyklen für die Datenkontinuität in Active IQ Unified Manager . . . 339
Informationen zu Zeitstempeln in erfassten Daten und Ereignissen in Active IQ Unified Manager . . . 340
Navigation in Performance Workflows in der Unified Manager GUI . . . 340
Navigation durch Performance-Workflows in der Active IQ Unified Manager GUI . . . 340
Anmeldung bei der Active IQ Unified Manager UI . . . 341
Grafische Benutzeroberfläche und Navigationspfade . . . 341
Suche nach Speicherobjekten in Active IQ Unified Manager . . . 347
Inhalte der Inventarseite in Active IQ Unified Manager filtern . . . 348
Überwachung der Cluster-Performance über das Dashboard . . . 350
Die Clusterleistung lässt sich über das Dashboard in Active IQ Unified Manager überwachen . . . 350
Auf dem Active IQ Unified Manager Dashboard stehen Leistungsübersichten zur Verfügung . . . 350
Performance-Bannermeldungen in Active IQ Unified Manager interpretieren . . . 351
Das Erfassungsintervall für Leistungsstatistiken in Active IQ Unified Manager ändern . . . 352
Fehlerbehebung bei Workloads mit dem Workload Analyzer . . . 352
Fehlerbehebung bei Workloads mit dem Workload Analyzer in Active IQ Unified Manager . . . 353
Workload Analyzer Daten in Active IQ Unified Manager verstehen . . . 353
Informationen zur Verwendung des Workload Analyzer in Active IQ Unified Manager . . . 355
Verwendung des Workload Analyzer in Active IQ Unified Manager . . . 355
Sie können die Cluster-Performance auf der Performance Cluster Landing page überwachen. . . . 356
Die Clusterleistung kann auf der Seite „Performance Cluster Landing“ in Active IQ Unified Manager überwacht werden. . . . 356
Die Landingpage des Performance Clusters in Active IQ Unified Manager verstehen . . . 356
Landingpage des Performance Cluster . . . 357
Überwachung der Performance mithilfe der Seiten zur Performance-Inventur . . . 361
Die Objektleistung kann mithilfe der Performance Inventory Seiten in Active IQ Unified Manager überwacht werden. . . . 361
Leistungsinventarseiten für alle Speicherobjekte in Active IQ Unified Manager . . . 362
Inhalte der Performance-Inventarseite überarbeiten . . . 368
Die Empfehlungen von Active IQ Unified Manager für das Tiering von Daten in die Cloud können in Active IQ Unified Manager überprüft werden. . . . 371
Überwachung der Performance mithilfe der Performance Explorer Seiten . . . 372
Die Überwachung der Leistung erfolgt mithilfe der Performance Explorer Seiten in Active IQ Unified Manager . . . 372
Stammobjekte werden für die Leistungsüberwachung in Active IQ Unified Manager verwendet . . . 372
Korrelierte Objekte im Active IQ Unified Manager Raster filtern . . . 373
Zeitbereich für korrelierte Objekte festlegen . . . 373
Korrelierte Objekte für die grafische Darstellung von Vergleichen im Active IQ Unified Manager definieren . . . 375
Zählerdiagramme in Active IQ Unified Manager verstehen . . . 376
Informationen zu den verschiedenen Typen von Leistungsindikator-Diagrammen in Active IQ Unified Manager . . . 377
Auswahl der Leistungsdiagramme zur Anzeige in Active IQ Unified Manager . . . 379
Der Bereich „Zählerdiagramme“ in Active IQ Unified Manager kann erweitert werden . . . 380
Der Fokus der Zählerdiagramme in Active IQ Unified Manager wird auf einen kürzeren Zeitraum

geändert . . . 380
Ereignisdetails in der Ereigniszeitleiste von Active IQ Unified Manager anzeigen . . . 381
Zoomansicht von Zählerdiagrammen . . . 382
Volumenlatenz nach Clusterkomponente in Active IQ Unified Manager anzeigen . . . 384
Anzeige des SVM IOPS Datenverkehrs nach Protokoll in Active IQ Unified Manager . . . 385
Anzeigen von Latenzdiagrammen für Volumes und LUNs zur Überprüfung der Leistungsgarantie in Active IQ Unified Manager . . . 386
Anzeigen der Leistung für All SAN Array Cluster in Active IQ Unified Manager . . . 386
Anzeige der Knoten-IOPS basierend auf lokalen Workloads in Active IQ Unified Manager . . . 387
Komponenten der Landingpages des Objekts . . . 388
Performance mithilfe von QoS-Richtliniengruppeninformationen managen . . . 393
Verwaltung der Performance mithilfe von QoS-Richtliniengruppeninformationen in Active IQ Unified Manager . . . 393
Steuerung des Workload-Durchsatzes mit Storage QoS in Active IQ Unified Manager . . . 394
In Active IQ Unified Manager verfügbare QoS-Richtliniengruppen auf allen Clustern anzeigen . . . 395
Anzeige von Volumes oder LUNs innerhalb derselben QoS-Richtliniengruppe in Active IQ Unified Manager . . . 395
QoS-Richtliniengruppeneinstellungen für Volumes oder LUNs in Active IQ Unified Manager anzeigen . . . 396
Vergleich von Volumes oder LUNs innerhalb derselben QoS-Richtliniengruppe in Active IQ Unified Manager . . . 397
QoS-Richtlinien in Durchsatzdiagrammen mit Active IQ Unified Manager anzeigen . . . 397
Anzeige der minimalen und maximalen QoS-Einstellungen für Workloads in Active IQ Unified Manager . . . 399
Managen der Performance mithilfe von Informationen zur Performance Kapazität und zu verfügbaren IOPS . . . 400
Verwaltung der Leistungskapazität und der verfügbaren IOPS in Active IQ Unified Manager . . . 400
Die verwendete Leistungs kapazität in Active IQ Unified Manager verstehen . . . 401
Verwendung des Werts für die genutzte Performance-Kapazität in Active IQ Unified Manager . . . 402
Verfügbare IOPS in Active IQ Unified Manager . . . 403
Verwendete Werte der Leistungsfähigkeit von Nodes und Aggregaten in Active IQ Unified Manager anzeigen . . . 404
Verfügbare IOPS-Werte für Knoten und Aggregate in Active IQ Unified Manager . . . 405
Anzeigen von Leistungskapazitätszählerdiagrammen in Active IQ Unified Manager . . . 405
Die Schwellenwerte für die genutzte Leistungskapazität in Active IQ Unified Manager konfigurieren . . . 407
Verwenden des Zählers für genutzte Leistungskapazität in Active IQ Unified Manager . . . 408
Die Seite „Node Failover Planning“ verstehen und verwenden . . . 409
Die Seite „Knotenausfallplanung“ in Active IQ Unified Manager kann verwendet werden . . . 409
Die Korrekturmaßnahmen werden auf der Seite „Leistung/Knoten-Failover-Planung“ in Active IQ Unified Manager ermittelt. . . . 409
Eine Übersicht über die Komponenten der Seite „Leistung/Knoten-Failover-Planung“ in Active IQ Unified Manager . . . 409
Schwellenwertrichtlinien für die Node Failover Planung in Active IQ Unified Manager erstellen . . . 411
Das Diagramm „Aufschlüsselung der genutzten Performance-Kapazität“ wird für die Failover-Planung in Active IQ Unified Manager verwendet . . . 412
Daten erfassen und die Workload-Performance überwachen . . . 413

Datenerfassung und Überwachung der Workload-Performance in Active IQ Unified Manager 413
Die Überwachung von Workload-Typen mit Active IQ Unified Manager 414
Grundlegendes zu Kennzahlen für die Messung der Workload-Leistung in Active IQ Unified Manager . 415
Informationen dazu, wie Active IQ Unified Manager den erwarteten Leistungsbereich berechnet 417
Die Latenzprognose kann für die Leistungsanalyse in Active IQ Unified Manager verwendet werden . . 418
Verwenden der Workload-Latenz zur Identifizierung von Leistungsproblemen in Active IQ Unified Manager 419
Bewertung, wie sich Clusteroperationen auf die Workload-Latenz in Active IQ Unified Manager auswirken können 420
Überwachung der MetroCluster Leistung mit Active IQ Unified Manager 421
Performance-Ereignisse und Warnmeldungen verstehen 422
Leistungsereignisse und Warnmeldungen in Active IQ Unified Manager verstehen 422
Quellen von Leistungsereignissen in Active IQ Unified Manager identifizieren 422
Leistungsereignisse nach Schweregrad in Active IQ Unified Manager priorisieren 423
Überwachen von Konfigurationsänderungen, die von Active IQ Unified Manager erkannt wurden 424
Informationen zu systemdefinierten Leistungsschwellenwertrichtlinien in Active IQ Unified Manager . . 425
Analyse von Leistungsereignissen und Benachrichtigungen in Active IQ Unified Manager 428
Es wird erläutert, wie Active IQ Unified Manager die Leistungsauswirkungen eines Ereignisses ermittelt. 429
Clusterkomponenten und Ressourcenkonflikte in Active IQ Unified Manager verstehen 430
Arbeitslastrollen in Leistungsereignissen in Active IQ Unified Manager 432
Performance-Schwellenwerte managen 433
Verwalten von Leistungsschwellenwerten in Active IQ Unified Manager 433
Verwendung benutzerdefinierter Leistungsschwellenwertrichtlinien in Active IQ Unified Manager 434
Reaktion auf Verstöße gegen Leistungsschwellenwertrichtlinien in Active IQ Unified Manager 436
Leistungsindikatoren verstehen, die mithilfe von Schwellenwerten in Active IQ Unified Manager verfolgt werden 436
Kombinationsschwellenwertrichtlinienobjekte und Zähler in Active IQ Unified Manager verstehen 438
In Active IQ Unified Manager können benutzerdefinierte Leistungsschwellenwertrichtlinien erstellt werden 439
Zuweisung von Performance-Schwellenwertrichtlinien zu Speicherobjekten in Active IQ Unified Manager 440
Leistungsschwellenwertrichtlinien in Active IQ Unified Manager anzeigen 441
Das Bearbeiten benutzerdefinierter Leistungsschwellenwertrichtlinien in Active IQ Unified Manager . . 442
Entfernen von Leistungsschwellenwertrichtlinien von Speicherobjekten in Active IQ Unified Manager . 442
Änderungen an Leistungsschwellenwertrichtlinien in Active IQ Unified Manager verstehen 443
Verwalten von Schwellenwertrichtlinien beim Verschieben von Objekten in Active IQ Unified Manager 444
Analyse von Performance Ereignissen 445
Analyse von Leistungsereignissen in Active IQ Unified Manager 445
Informationen zu Leistungsereignissen in Active IQ Unified Manager anzeigen 445
Analyse von Ereignissen anhand benutzerdefinierter Performance-Schwellenwerte 446
Analyse von Ereignissen anhand systemdefinierter Performance-Schwellenwerte 447
Analyse von Ereignissen anhand dynamischer Performance-Schwellenwerte 453
Performance-Ereignisse beheben 461
Leistungsereignisse in Active IQ Unified Manager beheben 461

Bestätigen Sie, dass die Latenz im Active IQ Unified Manager innerhalb des erwarteten Bereichs liegt 461
Bewertung, wie sich Konfigurationsänderungen auf die Workload-Performance in Active IQ Unified Manager auswirken . . . 461
Die Workload-Performance kann durch Anpassen der Client-seitig Einstellungen in Active IQ Unified Manager verbessert werden . . . 462
Wie sich Client- oder Netzwerkprobleme auf die Leistung in Active IQ Unified Manager auswirken . . . 462
Analyse von Volumes mit hoher Aktivität innerhalb einer QoS-Richtliniengruppe in Active IQ Unified Manager . . . 463
Verschieben von LIFs zur Verbesserung der Leistung in Active IQ Unified Manager . . . 463
Ausführung von Storage Effizienzvorgängen zu weniger ausgelasteten Zeiten . . . 464
Informationen dazu, wie sich das Hinzufügen von Festplatten auf die Datenneuverteilung in Active IQ Unified Manager auswirkt . . . 465
Die Workload-Performance lässt sich durch das Aktivieren von Flash Cache auf einem Knoten in Active IQ Unified Manager verbessern . . . 465
Die Workload-Performance kann durch die Aktivierung von Flash Pool auf einem Speicheraggregat in Active IQ Unified Manager verbessert werden. . . . 466
Prüfen des Zustands der MetroCluster Konfiguration in Active IQ Unified Manager . . . 466
Überprüfung der MetroCluster Konfigurationen in Active IQ Unified Manager . . . 466
Workloads in Active IQ Unified Manager in ein anderes Aggregat verschieben . . . 467
Workloads in Active IQ Unified Manager auf einen anderen Node verschieben . . . 468
Verschieben von Workloads auf ein Aggregat auf einem anderen Node in Active IQ Unified Manager . 470
Verschieben von Workloads auf einen Knoten in einem anderen HA-Paar in Active IQ Unified Manager . . . 472
Verschieben von Workloads auf einen anderen Knoten in einem anderen HA-Paar in Active IQ Unified Manager . . . 474
QoS Richtlinieneinstellungen können zur Priorisierung von Node Workloads in Active IQ Unified Manager verwendet werden. . . . 475
Entfernen inaktiver Volumes und LUNs in Active IQ Unified Manager . . . 476
Grundlegende Informationen dazu, wie sich das Hinzufügen von Datenträgern auf das Aggregatlayout in Active IQ Unified Manager auswirkt . . . 477
Einrichten einer Verbindung zwischen einem Unified Manager Server und einem externen Datenanbieter 477
Einrichten einer Verbindung zwischen Active IQ Unified Manager und einem externen Datenanbieter . 477
Übertragung von Active IQ Unified Manager Leistungsdaten an einen externen Server . . . 477
Graphite so konfigurieren, dass Leistungsdaten von Active IQ Unified Manager empfangen werden . . 478
Eine Verbindung zwischen Active IQ Unified Manager und einem externen Datenanbieter wird konfiguriert. . . . 479
Überwachen und Managen des Cluster-Systemstatus . . . 482
Einführung in die Systemstatusüberwachung von Active IQ Unified Manager . . . 482
Informationen zur Zustandsüberwachung von Active IQ Unified Manager . . . 482
Die Funktionen zur Zustandsüberwachung von Active IQ Unified Manager verstehen . . . 483
Active IQ Unified Manager Schnittstellen dienen zur Verwaltung des Zustands des Speichersystems. . 484
Management und Überwachung von Clustern und des Systemstatus von Clusterobjekten . . . 485
Clusterüberwachung verstehen . . . 485
Die Clusterliste und Details sind im Active IQ Unified Manager verfügbar . . . 487
Der Zustand der Cluster in einer MetroCluster Konfiguration in Active IQ Unified Manager kann

überprüft werden . . . 487
Der Gesundheits- und Kapazitätsstatus aller All SAN Array Cluster in Active IQ Unified Manager kann angezeigt werden . . . 489
Die Knotenliste und Details in Active IQ Unified Manager . . . 490
Generieren eines Hardwareinventarberichts für die Vertragsverlängerung in Active IQ Unified Manager . . . 491
Die Liste und Details der Storage-VMs in Active IQ Unified Manager anzeigen . . . 491
Die Aggregatliste und Details sind in Active IQ Unified Manager verfügbar . . . 492
Kapazitätsinformationen zu FabricPool in Active IQ Unified Manager anzeigen . . . 493
Speicherpooldetails in Active IQ Unified Manager anzeigen . . . 494
Die Volumenliste und Details in Active IQ Unified Manager anzeigen . . . 494
Details zu NFS-Freigaben in Active IQ Unified Manager . . . 495
Details zu SMB/CIFS Freigaben in Active IQ Unified Manager . . . 496
Die Liste der Snapshot-Kopien in Active IQ Unified Manager . . . 497
Löschen von Snapshot Kopien in Active IQ Unified Manager . . . 497
Berechnung des zurückforderbaren Speicherplatzes für Snapshot Kopien in Active IQ Unified Manager . . . 498
Informationen zu Clusterobjektfenstern und Dialogfeldern in Active IQ Unified Manager . . . 499
Allgemeine Systemstatus-Workflows und -Aufgaben in Unified Manager . . . 499
Verständnis gängiger Active IQ Unified Manager Arbeitsabläufe und Aufgaben im Zusammenhang mit dem Zustand . . . 499
Überwachen und Beheben von Problemen mit der Datenverfügbarkeit . . . 500
Kapazitätsprobleme lösen . . . 507
Systemstatusschwellenwerte verwalten . . . 509
Cluster-Sicherheitsziele managen . . . 515
Verwaltung von Backup- und Wiederherstellungsvorgängen . . . 527
Skripte managen . . . 544
Gruppen verwalten und überwachen . . . 547
Speicherobjektereignisse mithilfe von Annotationen priorisieren . . . 556
Versand eines Support-Bundles über die Web-Benutzeroberfläche und die Managementplattform . . . 565
Aufgaben und Informationen im Zusammenhang mit verschiedenen Arbeitsabläufen . . . 572
Daten schützen und wiederherstellen . . . 632
Schutzbeziehungen erstellen und Fehler beheben . . . 632
Arten des SnapMirror Schutzes in Active IQ Unified Manager . . . 632
Einrichten von Schutzbeziehungen in Unified Manager . . . 634
Durchführen eines Failovers und Failbacks für eine Schutzbeziehung . . . 636
Fehler in einem Schutzauftrag beheben . . . 640
Behebung von Verzögerungsproblemen in Active IQ Unified Manager . . . 644
Schutzbeziehungen verwalten und überwachen . . . 645
Informationen zur Verwaltung und Überwachung von Schutzbeziehungen in Active IQ Unified Manager . . . 646
Anzeigen des Volume Schutzstatus in Active IQ Unified Manager . . . 646
Anzeigen von Volumenschutzbeziehungen in Active IQ Unified Manager . . . 648
Überwachen von Consistency Group LUN Beziehungen in Active IQ Unified Manager . . . 649
Erstellung einer SnapVault Beziehung in der Ansicht „Gesundheit: Alle Volumes“ in Active IQ Unified

Manager . . . 650
Erstellung einer SnapVault Schutzbeziehung auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager . . . 651
Erstellung einer SnapMirror Beziehung in der Ansicht „Integrität: Alle Volumes“ in Active IQ Unified Manager . . . 652
Erstellung einer SnapMirror Beziehung auf der Detailseite „Volume Health“ in Active IQ Unified Manager . . . 653
Erstellung einer SnapMirror Beziehung mit versionsflexibler Replikation in Active IQ Unified Manager . . . 654
Erstellung von SnapMirror Beziehungen mit versionsflexibler Replikation und Rückwärtsoptionsfunktion in Active IQ Unified Manager . . . 656
Konfiguration der Zieleffizienzeinstellungen in Active IQ Unified Manager . . . 657
Erstellung von SnapMirror und SnapVault Zeitplänen in Active IQ Unified Manager . . . 657
Die Erweiterung des Schutzes mithilfe von Kaskaden- oder Fanout-Beziehungen in Active IQ Unified Manager . . . 658
Auf der Seite „Volume-Beziehungen“ in Active IQ Unified Manager können Schutzbeziehungen bearbeitet werden . . . 659
Auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager können Schutzbeziehungen bearbeitet werden . . . 659
Eine SnapMirror Richtlinie zur Maximierung der Übertragungseffizienz in Active IQ Unified Manager erstellen . . . 660
Erstellung einer SnapVault Richtlinie zur Maximierung der Übertragungseffizienz in Active IQ Unified Manager . . . 660
Abbrechen einer Übertragung auf der Seite „Volume Beziehungen“ in Active IQ Unified Manager . . . 661
Abbrechen einer Übertragung auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager . . . 662
Eine Schutzbeziehung auf der Seite „Volume Beziehungen“ in Active IQ Unified Manager anhalten . . . 663
Eine Schutzbeziehung auf der Seite „Volume-/Gesundheitsdetails“ in Active IQ Unified Manager anhalten . . . 664
Eine SnapMirror Beziehung auf der Seite „Volume Beziehungen“ von Active IQ Unified Manager aufheben . . . 664
Das Entfernen einer Schutzbeziehung von der Seite „Volume Relationships“ in Active IQ Unified Manager . . . 665
Geplante Transfers für eine ruhende Beziehung können auf der Seite „Volumenbeziehungen“ in Active IQ Unified Manager fortgesetzt werden . . . 665
Fortsetzen von Übertragungen in einer angehaltenen Beziehung auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager . . . 666
Schutzbeziehungen können auf der Seite „Volume Beziehungen“ in Active IQ Unified Manager initialisiert oder aktualisiert werden . . . 667
Schutzbeziehungen können auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager initialisiert oder aktualisiert werden . . . 668
Neusynchronisierung von Schutzbeziehungen auf der Seite „Volume Beziehungen“ in Active IQ Unified Manager . . . 669
Umgekehrte Schutzbeziehungen auf der Seite „Volume Beziehungen“ in Active IQ Unified Manager . . . 670
Die Wiederherstellung von Daten erfolgt mithilfe der Seiten „Volume“ und „Volume/Integritätsdetails“ in Active IQ Unified Manager . . . 671
Informationen zu Ressourcenpools in Active IQ Unified Manager . . . 672

In Active IQ Unified Manager können Ressourcenpools erstellt werden. 673
Ressourcenpools in Active IQ Unified Manager bearbeiten 673
Anzeigen des Ressourcenpool-Inventars in Active IQ Unified Manager 674
Hinzufügen von Ressourcenpoolmitgliedern in Active IQ Unified Manager 674
Aggregate aus Ressourcenpools in Active IQ Unified Manager entfernen 674
Löschen von Ressourcenpools in Active IQ Unified Manager 675
Storage VM Disaster Recovery Schutzbeziehungen überwachen 675
Verwalten von Speicher-VM-Zuordnungen in Active IQ Unified Manager 677
Anforderungen an SVMs und Ressourcenpools zur Unterstützung von Speicherdiensten in Active IQ Unified Manager 680
Informationen zu Jobs in Active IQ Unified Manager 680
Überwachung von Aufträgen in Active IQ Unified Manager 681
Auftragsdetails in Active IQ Unified Manager 681
Abbrechen von Jobs in Active IQ Unified Manager 681
Wiederholen eines fehlgeschlagenen Schutzauftrags in Active IQ Unified Manager 682
Beschreibung der Fenster und Dialogfelder für Schutzbeziehungen 682
Benutzerdefinierte Berichte generieren 725
Unified Manager Berichterstellung 725
Informationen zur Berichtsfunktion von Active IQ Unified Manager 725
Zugriffspunkte zum Generieren von Berichten 725
Berichte in Active IQ Unified Manager verstehen 727
Die Beziehung zwischen Ansicht und Bericht in Active IQ Unified Manager 727
Informationen zu den verschiedenen Berichtstypen in Active IQ Unified Manager 728
Berichtsbeschränkungen in Active IQ Unified Manager verstehen 729
Arbeiten mit Berichten 730
Berichtsworkflows in Active IQ Unified Manager verstehen 730
Erste Schritte mit der Berichtsfunktion in Active IQ Unified Manager 731
Suche nach einem geplanten Bericht in Active IQ Unified Manager 734
Berichte anpassen 734
Herunterladen von Berichten in Active IQ Unified Manager 738
Berichte planen 738
Planen von Berichten in Active IQ Unified Manager 738
Bericht planen 739
Berichtszeitpläne managen 741
Beispielhafte benutzerdefinierte Berichte 743
Informationen zu beispielhaften benutzerdefinierten Berichten in Active IQ Unified Manager 743
Anpassen von Cluster Storage Berichten 744
Anpassen von Berichten zur Aggregatkapazität 747
Volumenkapazitätsberichte anpassen 749
Anpassen von Qtree Kapazitätsberichten 752
NFS-Freigabeberichte anpassen 753
Anpassung von Storage VM Berichten 755
Berichte zu Volume-Beziehungen anpassen 756
Anpassung von Performanceberichten für Volumes 761
Beispielberichte in Microsoft Excel 761

Beispielberichte in Microsoft Excel in Active IQ Unified Manager verstehen . . . 762
Es kann ein Bericht erstellt werden, der eine Tabelle und ein Diagramm der aggregierten Kapazität in Active IQ Unified Manager anzeigt. . . . 762
Diagramme zur gesamten und verfügbaren Kapazität von Aggregaten in Active IQ Unified Manager . . 764
Es kann ein Bericht erstellt werden, um die verfügbaren Volumenkapazitätsdiagramme in Active IQ Unified Manager anzuzeigen. . . . 768
Ein Bericht zum Anzeigen von Aggregaten mit den meisten verfügbaren IOPS in Active IQ Unified Manager . . . 770
Storage mithilfe von REST APIs verwalten . . . 773
Erste Schritte mit Active IQ Unified Manager . . . 773
Erste Schritte mit Active IQ Unified Manager REST APIs . . . 773
Vorgesehene Benutzer der Active IQ Unified Manager REST APIs . . . 773
API-Zugriff und Kategorien in Active IQ Unified Manager verwalten . . . 773
REST Services verstehen, die in Active IQ Unified Manager angeboten werden . . . 775
API-Versionsnummern in Active IQ Unified Manager verstehen . . . 775
Verständnis des ONTAP Speicherressourcenmodells in Active IQ Unified Manager . . . 776
Zugriff über REST API und Authentifizierung in Active IQ Unified Manager . . . 777
Zugriff auf REST APIs und Authentifizierung in Active IQ Unified Manager . . . 777
Informationen zu den HTTP-Statuscodes von Active IQ Unified Manager . . . 780
Empfohlene Vorgehensweisen für die Verwendung von Active IQ Unified Manager APIs . . . 781
Fehlerbehebung mithilfe von Systemprotokollen in Active IQ Unified Manager . . . 782
Informationen dazu, wie Active IQ Unified Manager Jobobjekte für die asynchrone Verarbeitung verwendet . . . 782
Informationen zum Hello API Server Beispielprogramm in Active IQ Unified Manager . . . 783
Unified Manager REST-APIs . . . 787
Kategorien für Active IQ Unified Manager REST APIs verstehen . . . 787
Verwaltung von Speicherobjekten in einem Rechenzentrum mithilfe von APIs in Active IQ Unified Manager . . . 788
Zugriff auf ONTAP APIs über Proxyzugriff in Active IQ Unified Manager . . . 794
Administrative Aufgaben mithilfe von APIs in Active IQ Unified Manager ausführen . . . 797
Benutzerverwaltung in Active IQ Unified Manager mithilfe von APIs . . . 799
Leistungsmetriken mithilfe von APIs in Active IQ Unified Manager anzeigen . . . 800
Aufträge und Systemdetails können über APIs in Active IQ Unified Manager angezeigt werden . . . 810
Verwaltung von Ereignissen und Warnmeldungen mithilfe von APIs in Active IQ Unified Manager . . . 811
Arbeitslasten verwalten . . . 815
Gängige Arbeitsabläufe für das Storage Management . . . 823
Informationen zu gängigen API-Workflows für die Speicherverwaltung in Active IQ Unified Manager . . . 823
Ermittlung von Speicherplatzproblemen in Aggregaten mithilfe der Active IQ Unified Manager APIs . . . 824
Probleme mit Speicherobjekten mithilfe der Event-APIs von Active IQ Unified Manager ermitteln . . . 826
Fehlerbehebung bei ONTAP Volumes mithilfe der Active IQ Unified Manager Gateway APIs . . . 827
Workflows für das Workload-Management . . . 830
Rechtliche Hinweise . . . 855
Copyright . . . 855
Marken . . . 855
Patente . . . 855

Datenschutzrichtlinie 855
Open Source 855

Active IQ Unified Manager Dokumentation

Versionshinweise für Active IQ Unified Manager

Eine Zusammenfassung der neuen Funktionen, Einschränkungen und bekannten Probleme von Active IQ Unified Manager 9.18.

Weitere Informationen sind im "Active IQ Unified Manager Versionshinweise" verfügbar.

Los geht’s

Erste Schritte mit Active IQ Unified Manager auf VMware vSphere

Sie können die `.tar` Datei herunterladen, die ein Stammzertifikat, eine `README` Datei und eine `OVA` Datei enthält, und Unified Manager als virtuelle Appliance einsetzen.

Systemvoraussetzungen

- Betriebssystem: VMware ESXi 8.0
- RAM: 12 GB
- CPU: 9572 MHz insgesamt
- Freier Speicherplatz: 5 GB (Thin Provisionierung), 152 GB (Thick Provisionierung)

Detaillierte Systemanforderungen finden Sie in der Dokumentation "Voraussetzungen für die Installation von Unified Manager" und "Interoperabilitätsmatrix".

Active IQ Unified Manager installieren

Herunterladen des Installationsprogramms

1. Die `.tar`Datei mit einem Stammzertifikat, einer `README`Datei und einer `OVA`Datei steht zum Herunterladen zur Verfügung.
2. Die Datei sollte in einem lokalen Verzeichnis oder Netzwerkverzeichnis gespeichert werden, auf das Ihr vSphere Client zugreifen kann.
3. Im Verzeichnis, in dem die `.tar`Datei heruntergeladen wurde, folgt die Eingabe des `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz`Befehls. + Die benötigte `OVA`Datei, ein Root-Zertifikat und eine `README`Datei werden in das Zielverzeichnis entpackt.

Integrität überprüfen

Sie können die Integrität der `OVA` Datei überprüfen, indem Sie die in der `README` Datei beschriebenen Schritte befolgen.

Installation von Unified Manager

1. Im vSphere Client erfolgt die Auswahl von **Datei > OVF-Vorlage bereitstellen**.
2. Auswahl der OVA-Datei und Verwendung des Assistenten für das Deployment der virtuellen Appliance auf dem ESXi Server.
3. Auf der Seite „Überprüfungsdetails“ bestätigt die Meldung `Entrust Code Signing - OVCS2 (Trusted certificate)` im Abschnitt „Herausgeber“ die Integrität der heruntergeladenen `OVA` Datei. Für die Meldung `Entrust Code Signing - OVCS2 (Invalid certificate)` ist ein Upgrade des VMware vCenter Server auf Version 7.0U3E oder höher erforderlich.
4. Auf der Seite „Vorlage anpassen“ erfolgt im Register „Eigenschaften“ das Ausfüllen der Felder entsprechend der Art der durchgeführten Installation:

- Für die statisch Konfiguration sind in allen Feldern die erforderlichen Informationen einzugeben. Für das Feld **Secondary DNS** sind keine Angaben erforderlich.
- Bei DHCP mit IPv4 bleiben alle Felder leer.
- Für DHCP mit IPv6 muss das Kontrollkästchen „Automatische IPv6-Adressierung aktivieren“ aktiviert sein. In allen anderen Feldern bleiben die Angaben leer.

5. Die VM wird eingeschaltet.
6. Über die Registerkarte Console lässt sich der anfängliche Bootvorgang anzeigen.
7. Die Zeitzone konfigurieren.
8. Ein Benutzername und Passwort für die Unified Manager Wartung müssen eingegeben werden.

Am Ende der Installation werden die Informationen zur Verbindung mit der Unified Manager Weboberfläche angezeigt.

Erste Schritte mit Active IQ Unified Manager unter Linux

Sie können das Installationspaket herunterladen und Unified Manager auf einer physischen oder virtuellen Red Hat Enterprise Linux Plattform installieren.

Systemvoraussetzungen

- Betriebssystem: Red Hat Enterprise Linux Versionen 8.x und 9.4, basierend auf der x86_64-Architektur, installiert mit der Basisumgebung „Server with GUI“ aus der Option **Software Selection** des Betriebssystem-Installationsprogramms
- Arbeitsspeicher: 12 GB, CPU: 9572 MHz gesamt
- Freier Speicherplatz: 100 GB Speicherplatz im `/opt/netapp/data` Verzeichnis, 50 GB in der Root-Partition. Bei separat eingebundenen `/opt` und `/var/log` Verzeichnissen müssen für `/opt` 15 GB, für `/var/log` 16 GB und für `/tmp` 10 GB freier Speicherplatz verfügbar sein.

Ausführliche Systemanforderungen und Informationen zur Installation des Produkts an einem gesicherten Standort finden Sie in der "Voraussetzungen für die Installation von Unified Manager" und der "Interoperabilitätsmatrix".

Active IQ Unified Manager installieren

Herunterladen des Installationsprogramms

1. Zum Download stehen das `ActiveIQUnifiedManager-<version>.zip`Installationspaket sowie das `Code-Signing-Zertifikat (.pem`) und die digitale Signatur (`.sig`) bereit.
2. Führen Sie in dem Verzeichnis, in dem Sie die Installationsdatei heruntergeladen haben, Folgendes aus:

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

Integrität überprüfen

Mit den folgenden Befehlen lässt sich die Integrität des Installationspakets überprüfen:

- Durch Ausführen von `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>` wird eine Datei mit dem öffentlichen Schlüssel aus dem

Code-Signing-Zertifikat erstellt.

- Der Befehl `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip` dient zur Überprüfung der Signatur des Installationspakets.

Repository-Konfiguration überprüfen

Die Vorgehensweise zur Konfiguration eines Red Hat Enterprise Linux-Repositorys ist standortspezifisch. Sie können das `pre_install_check.sh` im Installationspaket enthaltene Skript verwenden, um die Konfiguration Ihres Betriebssystems zu überprüfen. Wenn Ihr System mit dem Internet verbunden ist, erhalten Sie automatisch Anweisungen zur Einrichtung des Red Hat Enterprise Linux-Repositorys.

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

Installation von Unified Manager

Unified Manager verwendet das `yum`Dienstprogramm, um die Software und alle abhängigen Softwarepakete zu installieren. Da es verschiedene Images von Red Hat Enterprise Linux gibt, hängen die installierten Pakete von der in den Images vorhandenen Software ab. Das `yum`Dienstprogramm ermittelt die für die Installation erforderlichen abhängigen Softwarepakete. Weitere Informationen zu den abhängigen Softwarepaketen sind in der Dokumentation "Linux Software und Installationsanforderungen" enthalten.

Zur Installation von Unified Manager ist der folgende Befehl entweder als Root-Benutzer oder unter Verwendung von `sudo`, aus dem Verzeichnis auszuführen, in dem die Installationsdatei entpackt wurde:

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

oder

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

Am Ende der Installation werden die Informationen zum Herstellen einer Verbindung mit der Unified Manager Web-UI angezeigt. Falls keine Verbindung zur Web-UI hergestellt werden kann, finden Sie in der mit der Software gelieferten `README`Datei weitere Informationen zu den Einschränkungen von Port 443.

Erste Schritte mit Active IQ Unified Manager unter Windows

Sie können das Installationspaket herunterladen und Unified Manager installieren, um Probleme mit Storage-Kapazität, Verfügbarkeit, Performance und Schutz zu überwachen und zu beheben.

Systemvoraussetzungen

- Betriebssysteme
  - Microsoft Windows Server 2019 Standard and Datacenter Edition
  - Microsoft Windows Server 2022 Standard und Datacenter Edition

    Unified Manager wird auf 64-Bit-Windows-Betriebssystemen für die folgenden Sprachen unterstützt:

  - Englisch

    - Japanisch
    - Vereinfachtes Chinesisch
- RAM: 12 GB
- CPU: 9572 MHz insgesamt
- Freier Speicherplatz: 100 GB Speicherplatz für das Installationsverzeichnis, 50 GB Speicherplatz für das MySQL Datenverzeichnis

Detaillierte Systemanforderungen finden Sie in "Voraussetzungen für die Installation von Unified Manager" und "Interoperabilitätsmatrix".

Active IQ Unified Manager installieren

Herunterladen des Installationsprogramms

1. Laden Sie das `ActiveIQUnifiedManager-<version>.exe` Installationspaket herunter.
2. Die Installationsdatei wird in ein Verzeichnis auf dem Zielsystem kopiert.

Installation von Unified Manager

Für die Installation von Unified Manager muss Microsoft .NET 4.5.2 oder eine neuere Version installiert sein. Im Rahmen der Installation installiert Unified Manager bei Bedarf weitere Drittanbieterpakete. Weitere Informationen zu den abhängigen Softwarepaketen finden Sie in der "Windows Software und Installationsvoraussetzungen".

1. Die Anmeldung bei Windows erfolgt mit dem standardmäßigen lokalen Administratorkonto.
2. In dem Verzeichnis, in dem Sie die Installationsdatei heruntergeladen haben, wird die Unified Manager Programmdatei (.exe) mit der rechten Maustaste angeklickt und als Administrator ausgeführt.
3. Bei Aufforderung erfolgt die Eingabe von Benutzername und Passwort, um den Unified Manager Wartungsbenutzer zu erstellen.
4. Im Assistenten für die Datenbankverbindung erfolgt die Eingabe des MySQL Root-Passworts.
5. Zum Abschließen der Installation sind die verbleibenden Anweisungen auszuführen.
6. Am Ende der Installation folgt die Auswahl von **Finish**; anschließend wird die Web-Benutzeroberfläche von Unified Manager angezeigt.

Installation von Unified Manager auf VMware vSphere Systemen

Informationen zu Active IQ Unified Manager

Informationen zu Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) ermöglicht es Ihnen, den Systemstatus und die Performance Ihrer ONTAP Storage Systeme über eine zentrale Benutzeroberfläche zu überwachen und zu managen. Unified Manager lässt sich auf einem Linux-Server, auf einem Windows-Server oder als virtuelle Appliance auf einem VMware-Host einsetzen.

Nachdem Sie die Installation abgeschlossen und die Cluster hinzugefügt haben, die Sie managen möchten, bietet Unified Manager eine grafische Benutzeroberfläche, die den Kapazitäts-, Verfügbarkeits-, Schutz- und Performance-Status der überwachten Storage Systeme anzeigt.

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Informationen zu den Funktionen des Active IQ Unified Manager Servers

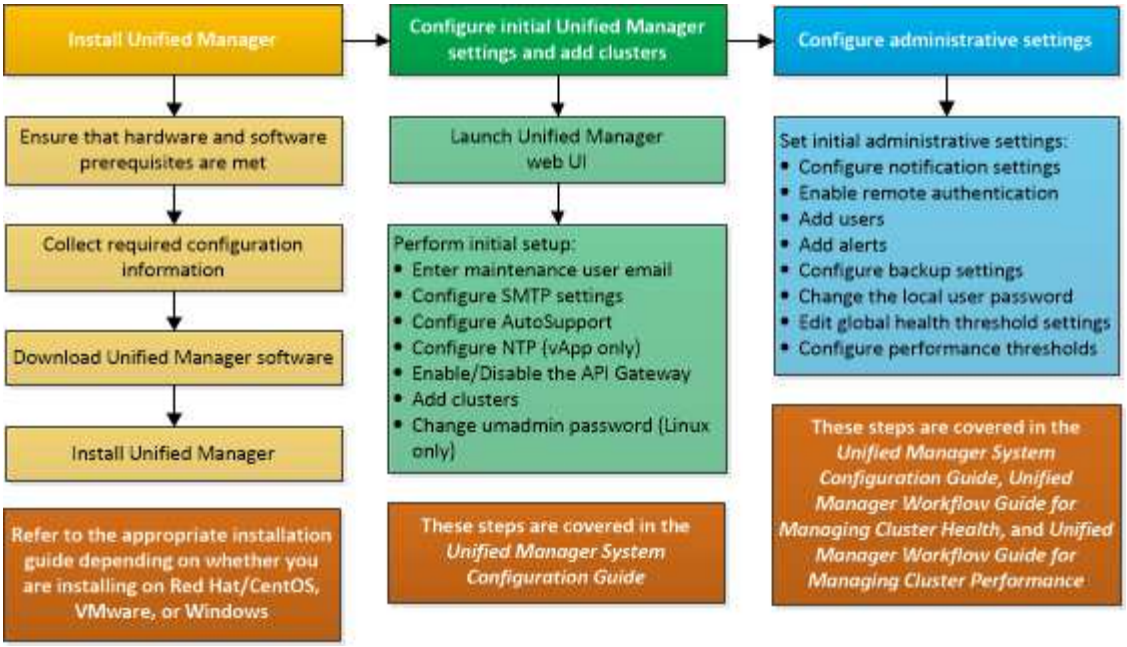
Die Unified Manager Serverinfrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Applikationsserver. Sie bietet Infrastruktur Services wie Erkennung, Überwachung, rollenbasierte Zugriffssteuerung (RBAC), Auditierung und Protokollierung.

Unified Manager sammelt Clusterinformationen, speichert die Daten in der Datenbank und analysiert die Daten, um festzustellen, ob Clusterprobleme vorliegen.

Informationen zur Installationsreihenfolge von Active IQ Unified Manager

Der Installationsablauf beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.

Diese Abschnitte beschreiben die einzelnen Elemente des unten dargestellten Arbeitsablaufs.



Voraussetzungen für die Installation von Unified Manager

Es muss sichergestellt werden, dass der Server die Installationsanforderungen für Active IQ Unified Manager erfüllt.

Vor Beginn des Installationsvorgangs muss der Server, auf dem Sie Unified Manager installieren möchten, die spezifischen Anforderungen an Software, Hardware, CPU und Arbeitsspeicher erfüllen.

NetApp unterstützt keine Änderungen am Code der Unified Manager Applikation. Wenn Sie Sicherheitsmaßnahmen auf dem Unified Manager Server anwenden müssen, sollten Sie diese Änderungen am Betriebssystem vornehmen, auf dem Unified Manager installiert ist.

Weitere Informationen zur Anwendung von Sicherheitsmaßnahmen auf dem Unified Manager Server enthält der Knowledge Base Artikel.

"Unterstützung für Sicherheitsmaßnahmen, die auf Active IQ Unified Manager für Clustered Data ONTAP angewendet werden"

Verwandte Informationen

Weitere Informationen finden Sie unter "NetApp Interoperabilitätsmatrix-Tool"

Informationen zur virtuellen Infrastruktur und zu den Hardwareanforderungen für Active IQ Unified Manager

Für die Installation von Unified Manager auf virtueller Infrastruktur oder einem physischen System müssen die Mindestanforderungen an Arbeitsspeicher, CPU und Festplattenspeicher erfüllt sein.

Die folgende Tabelle zeigt die empfohlenen Werte für Arbeitsspeicher, CPU und Festplattenspeicher. Diese Werte wurden so qualifiziert, dass Unified Manager akzeptable Performancewerte erreicht.

Hardwarekonfiguration	Empfohlene Einstellungen
RAM	12 GB
Prozessoren	4 CPUs
CPU-Zykluskapazität	9572 MHz gesamt (Mindestanforderung 9572 MHz)
Freier Speicherplatz	• 5 GB (mit Thin Provisioning) • 152 GB (thick provisioniert)

Unified Manager kann zwar auch auf Systemen mit wenig Arbeitsspeicher installiert werden, die empfohlenen 12 GB RAM gewährleisten jedoch ausreichend Speicher für optimale Performance, sodass das System bei wachsender Konfiguration zusätzliche Cluster und Storage Objekte aufnehmen kann. Sie sollten keine Speichergrenzen für die VM festlegen, auf der Unified Manager eingesetzt wird, und keine Funktionen (z. B. Ballooning) aktivieren, die die Nutzung des dem System zugewiesenen Arbeitsspeichers durch die Software behindern.

Darüber hinaus gibt es eine Begrenzung für die Anzahl der Knoten, die eine einzelne Instanz von Unified Manager überwachen kann, bevor eine zweite Instanz von Unified Manager installiert wird. Empfehlungen zu Knotenlimits, CPU und Arbeitsspeicher finden sich unter "der Unified Manager Best Practices-Leitfaden".

Das Auslagern von Speicherseiten beeinträchtigt die Performance des Systems und der Verwaltungsapplikation. Der Wettbewerb um CPU-Ressourcen, die aufgrund der Gesamtauslastung des Hosts nicht verfügbar sind, kann die Performance beeinträchtigen.

Anforderung für dedizierte Nutzung

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, sollte ausschließlich für Unified Manager vorgesehen sein und nicht mit anderen Applikationen gemeinsam genutzt werden. Andere Applikationen könnten Systemressourcen beanspruchen und die Performance von Unified Manager erheblich beeinträchtigen.

Speicherplatzbedarf für Backups

Wenn Sie die Backup- und Restore-Funktion von Unified Manager verwenden möchten, weisen Sie zusätzliche Kapazität zu, sodass das Verzeichnis oder die Festplatte “data” über 150 GB Speicherplatz verfügt. Ein Backup kann auf ein lokales Ziel oder auf ein Remote-Ziel geschrieben werden. Die Best Practice besteht darin, einen Remote-Speicherort außerhalb des Unified Manager Host-Systems zu bestimmen, der über mindestens 150 GB Speicherplatz verfügt.

Anforderungen an die Host-Konnektivität

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, muss so konfiguriert sein, dass Sie den Hostnamen vom Host selbst aus erfolgreich `ping` können. Bei einer IPv6-Konfiguration sollten Sie prüfen, ob `ping6` zum Hostnamen erfolgreich ist, damit die Installation von Unified Manager erfolgreich verläuft.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Web-UI des Produkts zuzugreifen. Wenn Sie während des Deployment eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie dem Netzwerkhost einen Namen zugewiesen. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollten Sie den Hostnamen über DNS beziehen.

Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen anstelle des vollqualifizierten Domain-Namens (FQDN) oder der IP-Adresse ermöglichen möchten, muss Ihre Netzwerkkonfiguration diesen Kurznamen in einen gültigen FQDN auflösen.

Informationen zur VMware Software und zu den Installationsvoraussetzungen für Active IQ Unified Manager

Das VMware vSphere System, auf dem Sie Unified Manager installieren, erfordert eine bestimmte Version des Betriebssystems und bestimmte Versionen der unterstützenden Software.

Betriebssystemsoftware

Das unterstützte Betriebssystem ist VMware ESXi 8.0.

> Unified Manager OVA auf VMware vSphere-Systemen verwendet intern Debian OS 13 (Trixie). Informationen zu den von den unterstützten ESXi-Serverversionen unterstützten Versionen der virtuellen Maschinenhardware finden Sie in der VMware-Dokumentation.

Die folgenden Versionen von vSphere werden unterstützt:

- VMware vCenter Server 7.0 und 8.0

Die Interoperability Matrix enthält die vollständige und aktuellste Liste der unterstützten ESXi Versionen.

"mysupport.netapp.com/matrix"

Die VMware ESXi-Serverzeit sollte mit der NTP-Serverzeit übereinstimmen, damit die virtuelle Appliance korrekt funktioniert. Die Synchronisierung der VMware ESXi-Serverzeit mit der NTP-Serverzeit verhindert einen Zeitfehler.

Installationsanforderungen

VMware High Availability für die virtuelle Appliance Unified Manager wird unterstützt.

Wenn Sie auf einem Storage-System mit ONTAP Software einen NFS-Datenspeicher einsetzen, kann mit dem NetApp NFS Plug-in für VMware VAAI die Thick Provisionierung verwendet werden.

Falls das Deployment in Ihrer für High Availability aktivierten Umgebung aufgrund unzureichender Ressourcen fehlschlägt, müssen Sie möglicherweise die Cluster Features Virtual Machine Options ändern, indem Sie VM Restart Priority deaktivieren und Host Isolation Response aktiviert lassen.

> Bei der Installation oder Aktualisierung von Unified Manager werden die erforderlichen Drittanbietersoftware und Sicherheitspatches automatisch auf einem VMware vSphere System installiert bzw. aktualisiert. Da die Installations- und Aktualisierungsprozesse von Unified Manager diese Komponenten steuern, sollten Sie keine eigenständige Installation oder Aktualisierung einer Drittanbieterkomponente vornehmen.

Unterstützte Browser in Active IQ Unified Manager

Der Zugriff auf die Web-Benutzeroberfläche des Unified Manager erfolgt über einen unterstützten Browser.

Die Interoperability Matrix enthält die Liste der unterstützten Browserversionen.

"mysupport.netapp.com/matrix"

Bei allen Browsern gewährleistet das Deaktivieren von Pop-up-Blockern, dass die Softwarefunktionen ordnungsgemäß angezeigt werden.

Wenn Sie Unified Manager für die SAML-Authentifizierung konfigurieren möchten, damit ein Identitätsanbieter (IdP) Benutzer authentifizieren kann, sollten Sie auch die Liste der vom IdP unterstützten Browser überprüfen.

Informationen zu Protokoll- und Portanforderungen für Active IQ Unified Manager

Die erforderlichen Ports und Protokolle ermöglichen die Kommunikation zwischen dem Unified Manager Server und den verwalteten Storage-Systemen, Servern und anderen Komponenten.

Verbindungen zum Unified Manager Server

Bei typischen Installationen müssen Sie beim Verbinden mit der Unified Manager Web-UI keine Portnummern angeben, da immer Standardports verwendet werden. Da Unified Manager beispielsweise immer versucht, auf seinem Standardport zu laufen, können Sie `https://<host>` anstelle von `https://<host>:443` eingeben.

Der Unified Manager Server verwendet spezifische Protokolle, um auf die folgenden Schnittstellen zuzugreifen:

Schnittstelle	Protokoll	Port	Beschreibung
Unified Manager Web-Benutzeroberfläche	HTTP	80	Dient zum Zugriff auf die Web-UI von Unified Manager; die Weiterleitung zum sicheren Port 443 erfolgt automatisch.
Unified Manager Web-Benutzeroberfläche und Programme, die APIs verwenden	HTTPS	443	Dient dem sicheren Zugriff auf die Unified Manager Weboberfläche oder zum Durchführen von API-Aufrufen; API-Aufrufe können nur über HTTPS erfolgen.
Managementplattform	SSH/SFTP	22	Dient zum Zugriff auf die Managementplattform und zum Abrufen von Support-Bundles.
Linux Befehlszeile	SSH/SFTP	22	Dient zum Zugriff auf die Red Hat Enterprise Linux Befehlszeile und zum Abrufen von Support-Bundles.

Schnittstelle	Protokoll	Port	Beschreibung
Syslog	UDP	514	Dient zum Zugriff auf abonnementbasierte EMS-Nachrichten aus ONTAP Systemen und zum Erstellen von Ereignissen auf Basis dieser Nachrichten.
REST	HTTPS	9443	Wird verwendet, um auf EMS-Ereignisse in Echtzeit über die REST API von authentifizierten ONTAP Systemen zuzugreifen.
MySQL Datenbank	MySQL	3306	Dient zum Aktivieren des Zugriffs von OnCommand Workflow Automation und OnCommand API Services auf Unified Manager.
AMQP-QPID-Broker	TCP/IP	56072	Dient der internen Nachrichtenkommunikation.
AMQP-QPID-Broker	WebSocket über TCP	56080	Dient zum Lauschen an diesem Port auf Nachrichten von ONTAP (cloud agent).
AMQP-QPID-Broker	WebSocket über TCP	56443	Dieser Port dient zum Empfangen von Nachrichten von ONTAP (cloud agent). Die Kommunikation über diesen Port unterstützt die Verschlüsselung mittels TLS oder SSL.

Der Standardport für MySQL, 3306, ist bei der Installation von Unified Manager auf VMware vSphere Systemen ausschließlich auf localhost beschränkt. Dies hat keine Auswirkungen auf Upgrade-Szenarien, da die vorherige Konfiguration beibehalten wird. Diese Konfiguration lässt sich ändern, und die Verbindung kann mithilfe der `Control access to MySQL port 3306`Option auf der Managementplattform für andere Hosts verfügbar gemacht werden. Informationen sind unter "Weitere Menüoptionen" verfügbar. Die für die HTTP- und HTTPS-Kommunikation verwendeten Ports (Ports 80 und 443) lassen sich über die Unified Manager Managementplattform ändern. Weitere Informationen sind unter "Menüs der Managementplattform für die Wartung" verfügbar.

Verbindungen vom Unified Manager Server

Ihre Firewall sollte so konfiguriert sein, dass die Ports geöffnet sind, die die Kommunikation zwischen dem Unified Manager Server und verwalteten Storage Systemen, Servern und anderen Komponenten ermöglichen.

Wenn ein Port nicht geöffnet ist, schlägt die Kommunikation fehl.

Je nach Ihrer Umgebung können Sie die Ports und Protokolle, die der Unified Manager-Server für die Verbindung zu bestimmten Zielen verwendet, ändern.

Der Unified Manager Server stellt über die folgenden Protokolle und Ports Verbindungen zu den verwalteten Storage Systemen, Servern und anderen Komponenten her:

Ziel	Protokoll	Port	Beschreibung
Speichersystem	HTTPS	443/TCP	Dient zur Überwachung und zum Managen von Storage Systemen. Wenn Sie diesen Port oder einen anderen Port für die Verbindung mit dem VMware vCenter Server oder ESXi Server verwenden, muss sichergestellt sein, dass der Port verfügbar ist und an einem sicheren Standort eine Verbindung hergestellt werden kann.
Speichersystem	NDMP	10000/TCP	Wird für bestimmte Snapshot-Wiederherstellungsvorgänge verwendet.
AutoSupport Server	HTTPS	443	Dient zum Versenden von AutoSupport Informationen. Für diese Funktion ist ein Internetzugang erforderlich.

Ziel	Protokoll	Port	Beschreibung
Authentifizierungsserver	LDAP	389	Dient zum Stellen von Authentifizierungsanforderungen sowie von Benutzer- und Gruppensuchanfragen.
LDAPS	636	Für die sichere LDAP-Kommunikation verwendet.	Mailserver
SMTP	25	Zum Senden von Benachrichtigungs-E-Mails verwendet.	SNMP-Trap-Sender
SNMPv1 oder SNMPv3	162/UDP	Dient zum Senden von SNMP-Traps für Warnmeldungen.	Server des externen Datenanbieters
TCP	2003	Dient zum Senden von Performance-Daten an einen externen Datenanbieter wie Graphite.	NTP-Server
NTP	123/UDP	Dient zur Synchronisierung der Zeit auf dem Unified Manager Server mit einem externen NTP Zeitserver. (nur VMware Systeme)	AMQP-QPID-Broker
TCP/IP	56072	Dient der internen Nachrichtenkommunikation.	AMQP-QPID-Broker
WebSocket über TCP	56080	Dient zum Lauschen an diesem Port auf Nachrichten von ONTAP (cloud agent).	AMQP-QPID-Broker
WebSocket über TCP	56443	Dieser Port dient zum Empfangen von Nachrichten von ONTAP (cloud agent). Die Kommunikation über diesen Port unterstützt die Verschlüsselung mittels TLS oder SSL.	Syslog

Das Arbeitsblatt in Active IQ Unified Manager wird vervollständigt

Bevor Sie Unified Manager installieren und konfigurieren, sollten Sie spezifische Informationen zu Ihrer Umgebung bereithalten. Sie können diese Informationen im Arbeitsblatt festhalten.

Installationsinformationen für Unified Manager

Die für die Installation von Unified Manager erforderlichen Details.

System, auf dem die Software eingesetzt wird	Ihr Wert
ESXi Server IP-Adresse	
vollqualifizierter Domainname des Hosts	
Host-IP-Adresse	
Netzwerkmaske	
Gateway-IP-Adresse	
Primäre DNS-Adresse	
Sekundäre DNS-Adresse	
Suchdomänen	
Benutzername für Wartungsarbeiten	
Wartungsbenutzerpasswort	

Unified Manager Konfigurationsinformationen

Die Details zur Konfiguration von Unified Manager nach der Installation. Einige Werte sind je nach Ihrer Konfiguration optional.

Einstellung	Ihr Wert
E-Mail-Adresse des Wartungsbenutzers	
NTP-Server	
SMTP Server Hostname oder IP-Adresse	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Port	25 (Standardwert)
E-Mail-Adresse, von der Benachrichtigungen versendet werden	
Hostname oder IP-Adresse des Authentifizierungsservers	
Name des Active Directory Administrators oder individueller Name für die LDAP-Bindung	
Active Directory Passwort oder LDAP Bind-Passwort	
Basis-individueller Name des Authentifizierungsservers	
URL des Identitätsanbieters (IdP)	
Metadaten des Identitätsanbieters (IdP)	
IP-Adressen von SNMP-Trap-Zielhosts	
SNMP-Port	

Clusterinformationen

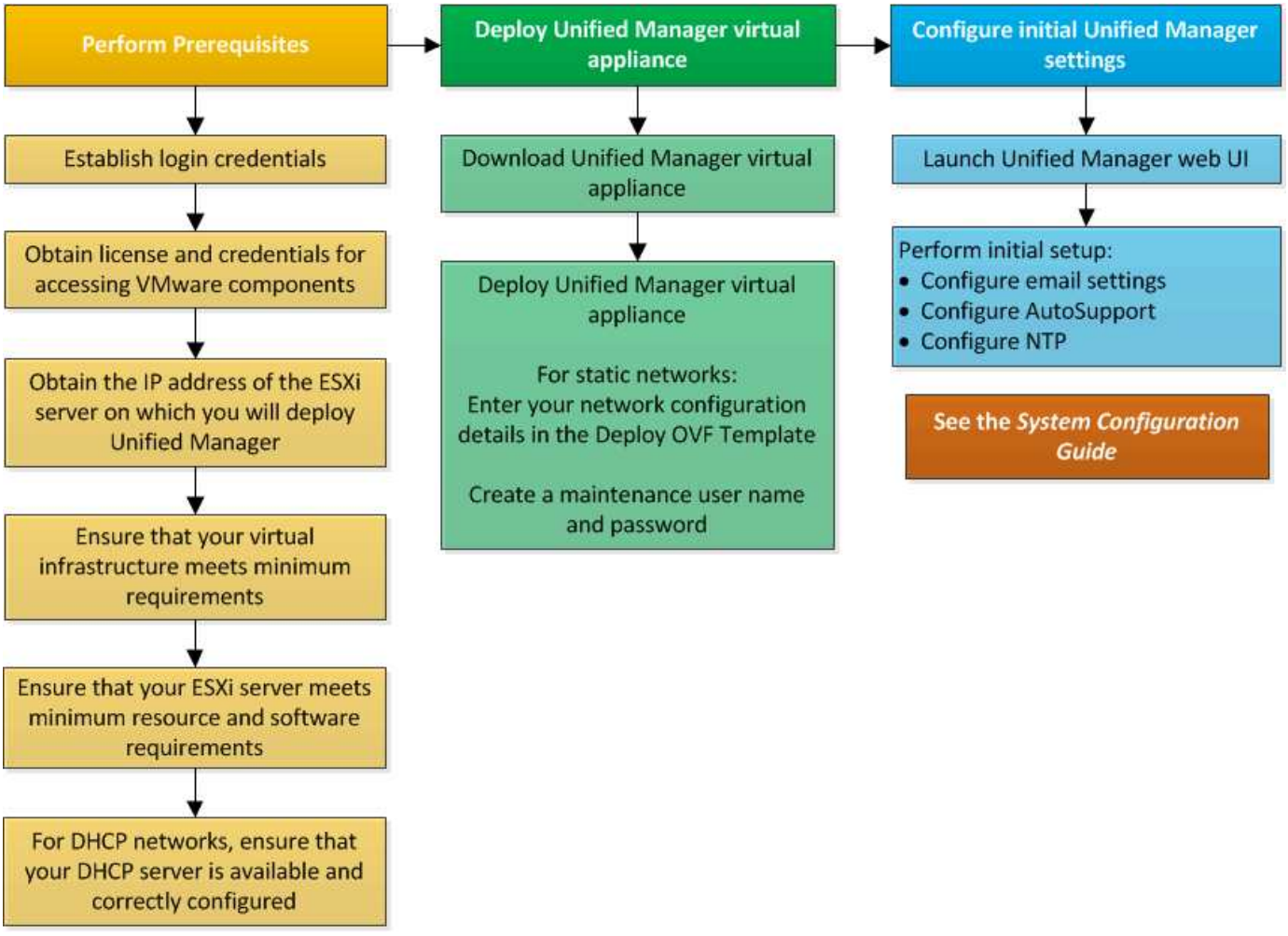
Die Details zu den Storage-Systemen, die Sie mit Unified Manager managen.

Cluster 1 von N	Ihr Wert
Hostname oder Cluster-Management-IP-Adresse	
ONTAP Administrator-Benutzername Dem Administrator muss die Rolle "admin" zugewiesen worden sein.	
ONTAP Administratorpasswort	
Protokoll	HTTPS

Installation, Upgrade und Entfernung von Unified Manager auf VMware vSphere

Informationen zum Active IQ Unified Manager Bereitstellungsprozess

Der Deployment-Workflow beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.



Workflow für die Bereitstellung der virtuellen Unified Manager Appliance

Bereitstellung von Active IQ Unified Manager

Das Deployment von Unified Manager umfasst das Herunterladen der Software, das Einsetzen der virtuellen Appliance, das Erstellen eines Wartungsbenutzernamens und -passworts sowie das Durchführen der Ersteinrichtung in der Web-UI.

Bevor Sie beginnen

- Sie sollten die Systemvoraussetzungen für das Deployment prüfen und vervollständigen.

  Weitere Informationen finden Sie unter "Systemvoraussetzungen".

- Folgende Informationen sollten vorliegen:
  - Anmeldedaten für die NetApp Support Site
  - Anmeldeinformationen für den Zugriff auf den VMware vCenter Server und den vSphere Web Client
  - IP-Adresse des ESXi-Servers, auf dem Sie die virtuelle Unified Manager Appliance bereitstellen
  - Details zum Datacenter, wie z. B. Storage-Platz im Datastore und Arbeitsspeicheranforderungen
  - IPv6 sollte auf dem Host aktiviert sein, wenn Sie IPv6-Adressierung verwenden möchten.

Der Einsatz von Unified Manager als virtuelle Appliance auf einem VMware ESXi Server ist möglich.

Der Zugriff auf die Managementplattform sollte über die VMware Managementplattform und nicht über SSH erfolgen.

> Ab Unified Manager 9.8 wurden die VMware Tools durch Open VM Tools ersetzt `open-vm-tools`). Die Installation der VMware Tools ist nicht mehr erforderlich, da `open-vm-tools` sie im Unified Manager Installationspaket enthalten sind.

Nach Abschluss des Deployments und der Ersteinrichtung können Sie entweder Cluster hinzufügen oder zusätzliche Netzwerkeinstellungen in der Managementplattform für die Wartung konfigurieren und dann auf die Web-UI zugreifen.

Schritte

1. Die entsprechenden Schritte finden Sie in "Download von Unified Manager".
2. Zusätzlich ist gemäß den Schritten in "Einsetzen der virtuellen Unified Manager Appliance" vorzugehen.

Die Installationsdatei für Active IQ Unified Manager wird heruntergeladen.

Für den Einsatz von Unified Manager als virtuelle Appliance wird die Unified Manager Installationsdatei von der NetApp Support Site heruntergeladen.

Bevor Sie beginnen

Sie sollten über die Anmeldedaten für die NetApp Support Site verfügen.

Die Installationsdatei ist eine `.tar`Datei, die ein Stammzertifikat, eine `README`Datei und eine `OVA`Datei enthält, die die für eine virtuelle Appliance konfigurierte Unified Manager Software umfasst.

Schritte

1. Anmeldung bei der NetApp Support Site und Navigation zur Download-Seite für Unified Manager:

   "NetApp Support Site"

2. Die gewünschte Version von Unified Manager ist auszuwählen und die Endbenutzer-Lizenzvereinbarung (EULA) ist zu akzeptieren.
3. Die `.tar`Datei für die VMware vSphere Installation wird heruntergeladen und in einem lokalen Verzeichnis oder Netzwerkverzeichnis gespeichert, auf das Ihr vSphere Client zugreifen kann.
4. Die Überprüfung der Prüfsumme stellt sicher, dass die Software korrekt heruntergeladen wurde.
5. Im Verzeichnis, in dem Sie die `.tar`Datei heruntergeladen haben, ist im Terminalfenster der folgende Befehl zum Entpacken des Unified Manager Bundle einzugeben:

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

   Die benötigte `OVA` Datei, ein Stammzertifikat und eine `README` Datei für Unified Manager werden in das Zielverzeichnis entpackt.

6. Zur Überprüfung der Integrität der `OVA`Datei können die in der `README`Datei beschriebenen Schritte herangezogen werden.

Bereitstellung der Active IQ Unified Manager virtuellen Appliance

Nach dem Herunterladen der Installationsdatei erfolgt das Deployment von Unified Manager als virtuelle Appliance. Für das Deployment der virtuellen Appliance auf einem ESXi-Server wird der vSphere Web Client verwendet. Beim Deployment der virtuellen Appliance wird eine virtuelle Maschine erstellt.

Bevor Sie beginnen

Die Systemvoraussetzungen sollten überprüft werden. Die erforderlichen Änderungen sollten vor dem Deployment der virtuellen Unified Manager Appliance vorgenommen werden.

Weitere Informationen finden Sie unter "Anforderungen an die virtuelle Infrastruktur".

Weitere Informationen finden Sie unter "VMware Software und Installationsanforderungen".

Bei Verwendung des Dynamic Host Configuration Protocol (DHCP) muss der DHCP-Server verfügbar sein, und die Konfigurationen von DHCP und des Netzwerkadapters der virtuellen Maschine (VM) müssen korrekt sein. DHCP ist standardmäßig konfiguriert.

Bei Verwendung einer statischen Netzwerkkonfiguration ist sicherzustellen, dass die IP-Adresse im selben Subnetz nicht doppelt vorhanden ist und dass die entsprechenden DNS-Servereinträge konfiguriert sind.

Vor dem Einsatz der virtuellen Appliance sind die folgenden Informationen erforderlich:

- Anmeldeinformationen für den Zugriff auf den VMware vCenter Server und den vSphere Web Client
- IP-Adresse des ESXi-Servers, auf dem Sie die virtuelle Unified Manager Appliance bereitstellen
- Details zum Datacenter, wie die verfügbare Storage-Kapazität
- Falls Sie DHCP nicht verwenden, benötigen Sie die IPv4- oder IPv6-Adressen der Netzwerkgeräte, mit denen Sie eine Verbindung herstellen möchten:

- Vollständig qualifizierter Domänenname (FQDN) des Hosts
- IP-Adresse des Hosts
- Netzwerkmaske
- IP-Adresse des Standardgateways
- Primäre und sekundäre DNS-Adressen
- Suchdomänen

Ab Unified Manager 9.8 wurden die VMware Tools durch Open VM Tools `open-vm-tools`) ersetzt. Die Installation der VMware Tools ist nicht mehr erforderlich, da `open-vm-tools` sie im Unified Manager Installationspaket enthalten sind.

Wenn die virtuelle Appliance eingesetzt wird, wird ein eindeutiges selbstsigniertes Zertifikat für den HTTPS-Zugriff generiert. Beim Zugriff auf die Unified Manager Web-Benutzeroberfläche wird möglicherweise eine Browserwarnung zu nicht vertrauenswürdigen Zertifikaten angezeigt.

VMware High Availability für die virtuelle Appliance Unified Manager wird unterstützt.

Schritte

1. Im vSphere Client befindet sich die Option unter **Datei** > **OVF-Vorlage bereitstellen**.
2. Zum Deployment der virtuellen Appliance Unified Manager ist der Assistent „OVF-Vorlage bereitstellen“ vollständig auszufüllen.

   Auf der Seite „Prüfungsdetails“:

   - Die Details des Abschnitts Publisher sollten überprüft werden. Die Meldung **Entrust Code Signing - OVCS2 (Trusted certificate)** bestätigt die Integrität der heruntergeladenen `OVA`Datei. + Wenn die Meldung **Entrust Code Signing - OVCS2 (Invalid certificate)** angezeigt wird, ist ein Upgrade des VMware vCenter Server auf Version 7.0U3E oder höher erforderlich.

     Auf der Seite „Vorlage anpassen“:

   - Bei Verwendung von DHCP und IPv4-Adressierung bleiben alle Felder leer.
   - Bei Verwendung von DHCP und IPv6-Adressierung sollte das Kontrollkästchen “Enable Auto IPv6 addressing” aktiviert sein; alle anderen Felder bleiben leer.
   - Wenn Sie eine statische Netzwerkkonfiguration verwenden möchten, können Sie die Felder auf dieser Seite ausfüllen, und diese Einstellungen werden während des Deployment angewendet. Die IP-Adresse muss für den Host, auf dem es eingesetzt wird, eindeutig sein, darf noch nicht verwendet werden und muss über einen gültigen DNS-Eintrag verfügen.
3. Nachdem die virtuelle Appliance Unified Manager auf dem ESXi-Server eingesetzt wurde, kann die VM durch Klicken mit der rechten Maustaste auf die VM und anschließendes Auswählen von **Power On** eingeschaltet werden.

   Falls der Power On-Vorgang aufgrund unzureichender Ressourcen fehlschlägt, sollten zusätzliche Ressourcen hinzugefügt und die Installation anschließend erneut versucht werden.

4. Sie wählen die Registerkarte **Console** aus.

   Der anfängliche Bootvorgang dauert einige Minuten, bis er abgeschlossen ist.

5. Zur Konfiguration Ihrer Zeitzone ist entsprechend den Aufforderungen im Fenster der VM Console Ihr geografisches Gebiet sowie Ihre Stadt oder Region einzugeben.

   Alle angezeigten Datumsangaben verwenden die für Unified Manager konfigurierte Zeitzone, unabhängig von der Zeitzoneneinstellung Ihrer verwalteten Geräte. Wenn Ihre Storage Systeme und der Verwaltungsserver denselben NTP-Server verwenden, beziehen sie sich auf denselben Zeitpunkt, auch wenn sie unterschiedlich angezeigt werden. Wenn Sie beispielsweise eine Snapshot Kopie mit einem Gerät erstellen, das in einer anderen Zeitzone als der Verwaltungsserver konfiguriert ist, entspricht der Zeitstempel dem des Verwaltungsservers.

6. Falls keine DHCP-Services verfügbar sind oder ein Fehler in den Details der statischen Netzwerkkonfiguration vorliegt, stehen folgende Optionen zur Verfügung:

Wenn Sie … verwenden	**Fahren Sie dann wie folgt fort…**
DHCP	Die Option **Retry DHCP** wird ausgewählt. Wenn Sie DHCP verwenden möchten, sollten Sie sicherstellen, dass es korrekt konfiguriert ist. Bei Verwendung eines DHCP-fähigen Netzwerks werden die FQDN- und DNS-Servereinträge der virtuellen Appliance automatisch zugewiesen. Wenn DHCP nicht ordnungsgemäß mit DNS konfiguriert ist, wird der Hostname “UnifiedManager” automatisch zugewiesen und dem Sicherheitszertifikat zugeordnet. Wenn kein DHCP-fähiges Netzwerk eingerichtet wurde, sollten die Netzwerkkonfigurationsinformationen manuell eingegeben werden.
Eine statische Netzwerkkonfiguration	a. Die Option **Details für die statische Netzwerkkonfiguration eingeben** auswählen. Der Konfigurationsprozess dauert einige Minuten. b. Anschließend werden die eingegebenen Werte bestätigt und **J** ausgewählt.

7. An der Eingabeaufforderung erfolgt die Eingabe eines Wartungsbenutzernamens; anschließend wird **Enter** gewählt.

   Der Benutzername für die Wartung sollte mit einem Buchstaben von a-z beginnen, gefolgt von einer beliebigen Kombination aus -, a-z oder 0-9.

8. An der Eingabeaufforderung können Sie ein Passwort eingeben und anschließend auf **Enter** klicken.

   Die VM Managementplattform zeigt die URL für die Unified Manager Web UI an.

Sie können auf die Web UI zugreifen, um die Ersteinrichtung von Unified Manager durchzuführen, wie in der "Konfigurieren von Active IQ Unified Manager" beschrieben.

Upgrade Workflow für die virtuelle Unified Manager Appliance

Aktualisieren von Active IQ Unified Manager

Ein Upgrade von Active IQ Unified Manager auf Version 9.18 ist nur von Version 9.14 oder 9.16 möglich.

Während des Upgrade-Prozesses ist Unified Manager nicht verfügbar. Vor dem Upgrade von Unified Manager sollten Sie alle laufenden Vorgänge abschließen.

Wenn Unified Manager mit einer Instanz von OnCommand Workflow Automation gekoppelt ist und für beide Produkte neue Softwareversionen verfügbar sind, müssen Sie die beiden Produkte trennen und nach den Aktualisierungen eine neue Workflow Automation Verbindung einrichten. Wenn Sie nur eines der Produkte aktualisieren, sollten Sie sich nach der Aktualisierung bei Workflow Automation anmelden und überprüfen, ob Workflow Automation weiterhin Daten aus Unified Manager bezieht.

Wenn Ihr System von Unified Manager 9.7 aktualisiert wurde, ist ein direktes Upgrade von 9.14 auf 9.18 aufgrund von Dateisystemänderungen in den Debian-Versionen nicht möglich. Empfohlen wird stattdessen folgender Upgrade-Pfad: 9.14 → 9.16P2 → 9.18.

Schritte

1. Die entsprechenden Schritte finden Sie in "Herunterladen des Unified Manager ISO-Images".
2. Zusätzlich sind die in "Upgrade von Unified Manager" beschriebenen Schritte auszuführen.

Der unterstützte Upgrade-Pfad für Versionen von Active IQ Unified Manager ist zu verwenden

Active IQ Unified Manager unterstützt für jede Version einen spezifischen Upgrade-Pfad.

Nicht alle Versionen von Unified Manager unterstützen ein direktes Upgrade auf neuere Versionen. Die Upgrades von Unified Manager sind auf ein N-2-Modell beschränkt. Das bedeutet, dass auf allen Plattformen nur Upgrades auf die nächsten beiden Releases möglich sind. Beispielsweise ist ein Upgrade auf Unified Manager 9.18 nur von Unified Manager 9.14 und 9.16 aus möglich.

Falls Sie eine ältere Version als die unterstützten Versionen verwenden, muss Ihre Unified Manager Instanz zunächst auf eine der unterstützten Versionen und anschließend auf die aktuelle Version aktualisiert werden.

Wenn beispielsweise Unified Manager 9.9 installiert ist und eine Aktualisierung auf Unified Manager 9.14 vorgesehen ist, ist dafür eine Abfolge von Upgrades erforderlich.

Beispielhafter Upgrade-Pfad:

1. Upgrade 9.11 → 9.13
2. Upgrade 9.13 → 9.14
3. Upgrade von 9.13 auf 9.16
4. Upgrade 9.14 oder 9.16 → 9.18

Weitere Informationen zur Upgrade-Pfadmatrix finden Sie in diesem "Knowledge Base Artikel (KB)".

Die Upgrade-Datei für Active IQ Unified Manager kann heruntergeladen werden.

Vor dem Upgrade von Unified Manager wird die Unified Manager Upgrade-Datei von der NetApp Support Site heruntergeladen.

Bevor Sie beginnen

Sie sollten über die Zugangsdaten für die NetApp Support Site verfügen.

Schritte

1. Anmeldung bei der NetApp Support Site:

   "NetApp Support Site"

2. Wechseln Sie zur Downloadseite für das Upgrade von Unified Manager auf VMware vSphere.
3. Das `.iso` Image für das Upgrade sollte in ein lokales Verzeichnis oder Netzwerkverzeichnis heruntergeladen und dort gespeichert werden, auf das Ihr vSphere Client zugreifen kann.
4. Die Prüfsumme ist zu überprüfen, um sicherzustellen, dass die Software korrekt heruntergeladen wurde.

Aktualisierung der Active IQ Unified Manager virtuellen Appliance

Sie können die virtuelle Appliance Active IQ Unified Manager von den Versionen 9.14 oder 9.16 auf 9.18 aktualisieren.

Bevor Sie beginnen

Stellen Sie Folgendes sicher:

- Sie haben die Upgrade-Datei, das ISO-Image von der NetApp Support Site heruntergeladen.
- Das System, auf dem Sie Unified Manager aktualisieren, muss die System- und Softwareanforderungen erfüllen.

  Weitere Informationen finden Sie unter "Anforderungen an die virtuelle Infrastruktur".

  Weitere Informationen finden Sie unter "VMware Software und Installationsanforderungen".

- Für Benutzer von vSphere 6.5 und höher haben Sie die VMware Remote Console (VMRC) installiert.
- Während des Upgrades werden Sie möglicherweise aufgefordert zu bestätigen, ob Sie die bisherigen Standardeinstellungen für die Speicherung von Performance-Daten über 13 Monate beibehalten oder auf 6 Monate ändern möchten. Nach der Bestätigung werden die historischen Performance-Daten nach 6 Monaten gelöscht.
- Sie verfügen über folgende Informationen:
  - Anmeldedaten für die NetApp Support Site
  - Anmeldeinformationen für den Zugriff auf den VMware vCenter Server und den vSphere Web Client
  - Anmeldeinformationen für den Wartungsbenutzer von Unified Manager

Während des Upgrade-Prozesses ist Unified Manager nicht verfügbar. Vor dem Upgrade von Unified Manager sollten Sie alle laufenden Vorgänge abschließen.

Wenn Sie Workflow Automation und Unified Manager gekoppelt haben, sollten Sie den Hostnamen in Workflow Automation manuell aktualisieren.

Schritte

1. Im vSphere Client wählen Sie **Startseite** > **Inventar** > **VMs und Vorlagen** aus.
2. Auszuwählen ist die virtuelle Maschine (VM), auf der die virtuelle Appliance Unified Manager installiert ist.
3. Wenn die Unified Manager VM ausgeführt wird, finden Sie die entsprechende Option unter **Zusammenfassung** > **Befehle** > **Gast herunterfahren**.

4. Eine applikationskonsistente Sicherung entsteht durch das Erstellen einer Sicherungskopie der Unified Manager VM, z. B. eines Snapshots oder eines Klons.
5. Im vSphere Client können Sie die Unified Manager VM einschalten.
6. Die VMware Remote Console wird gestartet.
7. Nach einem Klick auf das Symbol **CDROM** ist **Mit Disk-Image-Datei (.iso) verbinden** auszuwählen.
8. Die `ActiveIQUnifiedManager-<version>-virtual-update.iso`Datei wird ausgewählt, und anschließend wird auf **Open** geklickt.
9. Sie wählen die Registerkarte **Console** aus.
10. Die Anmeldung bei der Unified Manager Managementplattform erfolgt.
11. Im Hauptmenü erfolgt die Auswahl der Option **Upgrade**.

    Es wird eine Meldung angezeigt, dass Unified Manager während des Upgrade-Vorgangs nicht verfügbar sein wird und nach Abschluss des Vorgangs wieder verfügbar ist.

12. Zum Fortfahren `y` eingeben.

    Es erscheint eine Warnung, die Sie daran erinnert, die virtuelle Maschine zu sichern, auf der sich die virtuelle Appliance befindet.

13. Zum Fortfahren `y` eingeben.

    Der Aktualisierungsprozess und der Neustart der Unified Manager Services können mehrere Minuten dauern.

14. Zum Fortfahren eine beliebige Taste drücken.

    Sie werden automatisch von der Wartungs-Managementplattform abgemeldet.

15. **Optional:** Eine Anmeldung an der Wartungskonsole sowie die Überprüfung der Version von Unified Manager sind möglich.

Sie können die Web-Benutzeroberfläche in einem neuen Fenster in einem unterstützten Webbrowser starten und sich anmelden, um die aktualisierte Version von Unified Manager zu verwenden. Vor der Ausführung von Aufgaben in der Benutzeroberfläche muss gewartet werden, bis der Erkennungsprozess abgeschlossen ist.

Starten Sie die virtuelle Maschine Active IQ Unified Manager neu.

Ein Neustart der virtuellen Maschine (VM) von Unified Manager über die Managementplattform ist möglich. Nach dem Erstellen eines neuen Sicherheitszertifikats oder bei Problemen mit der VM sollte die VM neu gestartet werden.

Bevor Sie beginnen

- Die virtuelle Appliance sollte eingeschaltet sein.
- Sie sollten bei der Unified Manager Wartungskonsole als Wartungsbenutzer angemeldet sein.

Sie können die virtuelle Maschine auch von vSphere aus mit der VMware Option **Restart Guest** neu starten. Siehe dazu "das Restart-VMGuest cmdlet in Broadcoms VMware vSphere PowerCLI CMDLET reference."

Schritte

1. In der Managementplattform erfolgt die Auswahl von **System Configuration** > **Reboot Virtual Machine**.
2. Sie öffnen die Unified Manager Web UI in Ihrem Browser und melden sich an.

Active IQ Unified Manager entfernen

Sie können Unified Manager deinstallieren, indem Sie die virtuelle Maschine (VM) entfernen, auf der die Unified Manager Software installiert ist.

Bevor Sie beginnen

- Sie benötigen Zugangsdaten für den Zugriff auf VMware vCenter Server und vSphere Web Client.
- Jede aktive Verbindung des Unified Manager Servers zu einem Workflow Automation Server sollte geschlossen sein.
- Bevor die virtuelle Maschine (VM) entfernt wird, sollten alle Cluster (Datenquellen) vom Unified Manager Server entfernt sein.

Schritte

1. Mit der Wartungs-Managementplattform von Unified Manager lässt sich überprüfen, dass der Unified Manager Server keine aktive Verbindung zu einem externen Datenanbieter hat.
2. Im vSphere Client wählen Sie **Startseite** > **Inventar** > **VMs und Vorlagen** aus.
3. Nach Auswahl der VM, die entfernt werden soll, erfolgt ein Klick auf die Registerkarte **Zusammenfassung**.
4. Wenn die VM ausgeführt wird, erfolgt das Herunterfahren über **Power** > **Shut Down Guest**.
5. Mit der rechten Maustaste auf die VM klicken, die entfernt werden soll, und **Delete from Disk** auswählen.

Installation von Unified Manager auf Linux-Systemen

Einführung in Active IQ Unified Manager

Informationen zu Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) ermöglicht die Überwachung und das Managen des Systemstatus und der Performance Ihrer ONTAP Storage Systeme über eine zentrale Benutzeroberfläche. Unified Manager kann auf einem Linux Server, auf einem Windows Server oder als virtuelle Appliance (vApp) auf einem VMware Host eingesetzt werden.

Nachdem Sie die Installation abgeschlossen und die Cluster hinzugefügt haben, die Sie managen möchten, bietet Unified Manager eine grafische Benutzeroberfläche, die den Kapazitäts-, Verfügbarkeits-, Schutz- und Performance-Status der überwachten Storage Systeme anzeigt.

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Was der Active IQ Unified Manager Server bewirkt

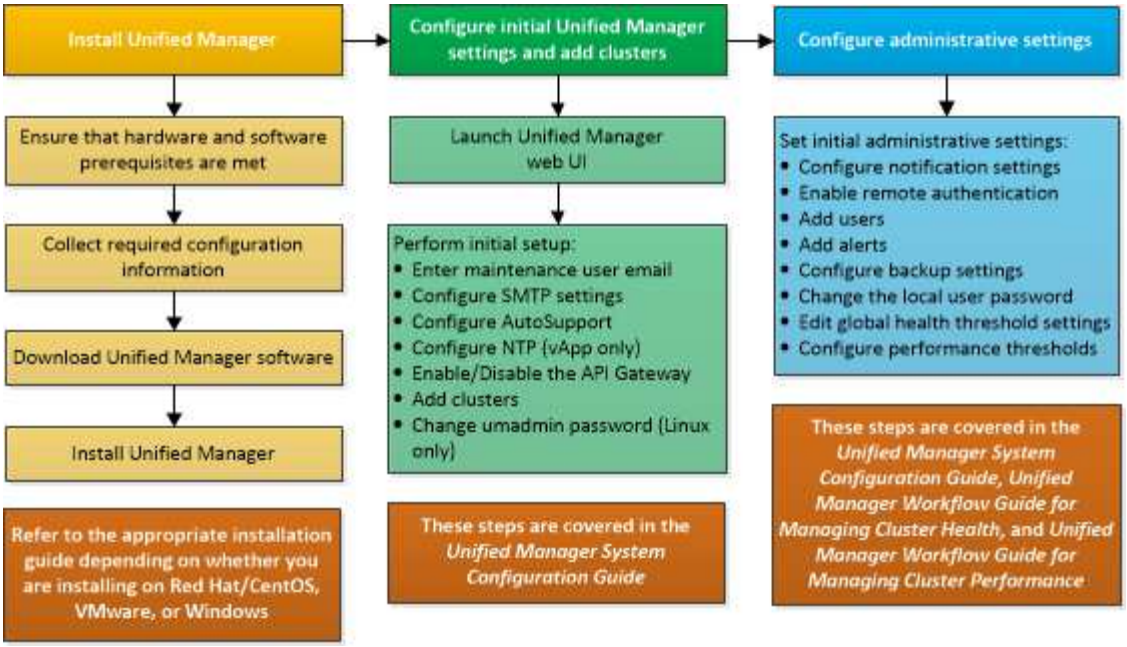
Die Unified Manager Serverinfrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Applikationsserver. Sie bietet Infrastruktur Services wie Erkennung, Überwachung, rollenbasierte Zugriffssteuerung (RBAC), Auditierung und Protokollierung.

Unified Manager sammelt Clusterinformationen, speichert die Daten in der Datenbank und analysiert die Daten, um festzustellen, ob Clusterprobleme vorliegen.

Installationssequenz für Active IQ Unified Manager anzeigen

Der Installationsablauf beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.

Diese Abschnitte beschreiben die einzelnen Elemente des unten dargestellten Arbeitsablaufs.



Voraussetzungen für die Installation von Unified Manager

Die Anforderungen für die Installation von Active IQ Unified Manager verstehen

Vor Beginn des Installationsvorgangs muss der Server, auf dem Sie Unified Manager installieren möchten, die spezifischen Anforderungen an Software, Hardware, CPU und Arbeitsspeicher erfüllen.

NetApp unterstützt keine Änderungen am Code der Unified Manager Applikation. Wenn Sie Sicherheitsmaßnahmen auf dem Unified Manager Server anwenden müssen, sollten Sie diese Änderungen am Betriebssystem vornehmen, auf dem Unified Manager installiert ist.

Weitere Informationen zur Anwendung von Sicherheitsmaßnahmen auf dem Unified Manager Server enthält der Knowledge Base Artikel.

"Unterstützung für Sicherheitsmaßnahmen, die auf Active IQ Unified Manager für Clustered Data ONTAP angewendet werden"

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Informationen zu virtueller Infrastruktur und Hardwareanforderungen für Active IQ Unified Manager

Für die Installation von Unified Manager auf virtueller Infrastruktur oder einem physischen System müssen die Mindestanforderungen an Arbeitsspeicher, CPU und Festplattenspeicher erfüllt sein.

Die folgende Tabelle zeigt die empfohlenen Werte für Arbeitsspeicher, CPU und Festplattenspeicher. Diese Werte wurden so qualifiziert, dass Unified Manager akzeptable Performancewerte erreicht.

Hardwarekonfiguration	Empfohlene Einstellungen
RAM	12 GB
Prozessoren	4 CPUs
CPU-Zykluskapazität	9572 MHz gesamt (Mindestanforderung 9572 MHz)
Freier Speicherplatz	150 GB, wobei die Kapazität wie folgt aufgeteilt ist: • 50 GB für die Root-Partition vorgesehen • 100 GB freier Speicherplatz, die dem `/opt/netapp/data`Verzeichnis zugewiesen sind, das auf einem LVM-Laufwerk oder auf einer separaten lokalen Festplatte, die an das Zielsystem angeschlossen ist, eingehängt ist Bei separat eingebundenen `/opt` und `/var/log` Verzeichnissen müssen in `/opt` 15 GB und in `/var/log` 16 GB freier Speicherplatz verfügbar sein. Im `/tmp` Verzeichnis sollten mindestens 10 GB freier Speicherplatz verfügbar sein.

Unified Manager kann zwar auch auf Systemen mit wenig Arbeitsspeicher installiert werden, die empfohlenen 12 GB RAM gewährleisten jedoch ausreichend Speicher für optimale Performance, sodass das System bei wachsender Konfiguration zusätzliche Cluster und Storage Objekte aufnehmen kann. Sie sollten keine Speichergrenzen für die VM festlegen, auf der Unified Manager eingesetzt wird, und keine Funktionen (z. B. Ballooning) aktivieren, die die Nutzung des dem System zugewiesenen Arbeitsspeichers durch die Software behindern.

Darüber hinaus gibt es eine Begrenzung für die Anzahl der Knoten, die eine einzelne Instanz von Unified Manager überwachen kann, bevor eine zweite Instanz von Unified Manager installiert wird. Empfehlungen zu Knotenlimits, CPU und Arbeitsspeicher finden sich in der "Unified Manager Best Practices-Leitfaden".

Das Auslagern von Speicherseiten beeinträchtigt die Performance des Systems und der Verwaltungsapplikation. Der Wettbewerb um CPU-Ressourcen, die aufgrund der Gesamtauslastung des Hosts nicht verfügbar sind, kann die Performance beeinträchtigen.

Anforderung für dedizierte Nutzung

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, sollte ausschließlich für Unified Manager vorgesehen sein und nicht mit anderen Applikationen gemeinsam genutzt werden. Andere Applikationen könnten Systemressourcen beanspruchen und die Performance von Unified Manager erheblich beeinträchtigen.

Speicherplatzbedarf für Backups

Wenn Sie die Backup- und Restore-Funktion von Unified Manager verwenden möchten, weisen Sie zusätzliche Kapazität zu, sodass das Verzeichnis oder die Festplatte “data” über 150 GB Speicherplatz verfügt. Ein Backup kann auf ein lokales Ziel oder auf ein Remote-Ziel geschrieben werden. Die Best Practice besteht darin, einen Remote-Speicherort außerhalb des Unified Manager Host-Systems zu bestimmen, der über mindestens 150 GB Speicherplatz verfügt.

Anforderungen an die Host-Konnektivität

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, muss so konfiguriert sein, dass Sie den Hostnamen vom Host selbst aus erfolgreich `ping` können. Bei einer IPv6-Konfiguration sollten Sie prüfen, ob `ping6` zum Hostnamen erfolgreich ist, damit die Installation von Unified Manager erfolgreich verläuft.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Web-UI des Produkts zuzugreifen. Wenn Sie während des Deployment eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie dem Netzwerkhost einen Namen zugewiesen. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollten Sie den Hostnamen über DNS beziehen.

Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen anstelle des vollqualifizierten Domain-Namens (FQDN) oder der IP-Adresse ermöglichen möchten, muss Ihre Netzwerkkonfiguration diesen Kurznamen in einen gültigen FQDN auflösen.

Informationen zu Linux-Software und Installationsvoraussetzungen in Active IQ Unified Manager

Das Linux-System, auf dem Sie Unified Manager installieren, erfordert bestimmte Versionen des Betriebssystems und der unterstützenden Software. Bei Linux-Installationen kann Unified Manager nur auf einem Red Hat Enterprise Linux Betriebssystem installiert werden. Es kann auf keinem anderen Betriebssystem installiert werden.

Betriebssystemsoftware

Auf dem Linux-System müssen die folgenden Versionen des Betriebssystems und der zugehörigen Software installiert sein:

- Red Hat Enterprise Linux Versionen 8.x und 9.6, basierend auf der x86_64-Architektur

Die vollständige und aktuellste Liste der unterstützten Red Hat Enterprise Linux Versionen finden Sie in der Interoperability Matrix.

"NetApp Interoperabilitätsmatrix"

Der Server sollte ausschließlich für den Betrieb von Unified Manager reserviert sein. Es dürfen keine weiteren Anwendungen auf dem Server installiert werden. In manchen Umgebungen ist aufgrund von Unternehmensrichtlinien ein Schwachstellenscanner wie Qualys auf dem Linux-System installiert. Um Installationsfehler zu vermeiden, sollte dieser Schwachstellenscanner vor der Installation von Unified Manager deaktiviert werden.

> Schwachstellenscanner (wie z. B. Qualys) können beim Scannen der virtuellen Maschine (VM) entweder intern (wenn Unified Manager und der Schwachstellenscanner auf derselben VM installiert sind) oder extern (wenn Unified Manager und der Schwachstellenscanner auf zwei verschiedenen Servern installiert sind und der Schwachstellenscanner die VM scannt, auf der Unified Manager installiert ist) zu einer hohen CPU-Auslastung führen. Dieses Problem führt häufig dazu, dass die VM nicht mehr reagiert, und beeinträchtigt die Unified Manager Services. Daher empfiehlt NetApp, den Schwachstellenscanner auf der VM, auf der Unified Manager installiert ist, zu deaktivieren. Wenn das Deaktivieren des Scanners nicht möglich ist, sollte die VM außerhalb der Geschäftszeiten gescannt und die Services nach Abschluss des Scans neu gestartet werden.

Software von Drittanbietern

Unified Manager wird auf einem WildFly Webserver bereitgestellt. WildFly 27.0.1.Final ist mit Unified Manager gebündelt und konfiguriert.

Die folgenden Drittanbieterpakete werden benötigt, sind aber nicht im Lieferumfang von Unified Manager enthalten. Diese Pakete werden vom `yum`Installationsprogramm während der Installation automatisch installiert, sofern Sie die Repositories wie in den folgenden Abschnitten beschrieben konfiguriert haben.

- MySQL Community Edition Version 8.4.10 (aus dem MySQL Repository)
- OpenJDK Version 17.0.14+6 (aus dem Repository Red Hat Extra Enterprise Linux Server)
- Python 3.13.3 (aus dem Red Hat Extra Enterprise Linux Server repository)
- 7zip Version 7z2301-linux-x64. Weitere Informationen enthält "Konfiguration des 7-zip Softwarepakets".

> Sie müssen eine laufende Instanz von Unified Manager beenden, bevor Sie Software von Drittanbietern aktualisieren. Nach Abschluss der Installation der Drittanbietersoftware können Sie Unified Manager neu starten.

Anforderungen an die Benutzerberechtigung

Die Installation von Unified Manager auf einem Linux System kann der Root-Benutzer oder können Nicht-Root-Benutzer mithilfe des `sudo` Befehls ausführen.

Zusätzlich enthält die Standardinstallation von Unified Manager den Benutzer umadmin (Standard-Wartungsbenutzer) und den Benutzer jboss in den sudoers-Dateien (`ocum_sudoers` und `ocie_sudoers`) im `/etc/sudoers.d/` Verzeichnis. Wenn Sie diese Inhalte aufgrund von Sicherheitsrichtlinien oder eines Sicherheitsüberwachungstools aus Ihrer Umgebung entfernen, müssen Sie sie wieder hinzufügen. Sie müssen die sudoers-Konfiguration beibehalten, da einige Unified Manager Vorgänge diese sudo-Berechtigungen erfordern.

Installationsanforderungen

Die Best Practices für die Installation von Red Hat Enterprise Linux und den zugehörigen Repositories auf Ihrem System sind nachfolgend aufgeführt. Systeme, die anders installiert oder konfiguriert wurden oder extern (in der Cloud) bereitgestellt werden, erfordern möglicherweise zusätzliche Schritte, und Unified Manager funktioniert in solchen Bereitstellungen unter Umständen nicht ordnungsgemäß.

- Red Hat Enterprise Linux muss gemäß den Best Practices von Red Hat installiert werden, und es sollten die folgenden Standardoptionen ausgewählt werden, wofür die Basisumgebung “Server with GUI” ausgewählt werden muss.
- Bei der Installation von Unified Manager auf Red Hat Enterprise Linux muss das System Zugriff auf das entsprechende Repository haben, damit das Installationsprogramm auf alle erforderlichen Softwareabhängigkeiten zugreifen und diese installieren kann.
- Damit das `yum` Installationsprogramm abhängige Software in den Red Hat Enterprise Linux-Repositories finden kann, müssen Sie das System während der Red Hat Enterprise Linux-Installation oder anschließend mithilfe eines gültigen Red Hat-Abonnements registriert haben.

  Informationen zum Red Hat Subscription Manager enthält die Red Hat Dokumentation.

- Für die erfolgreiche Installation der erforderlichen Drittanbieter-Dienstprogramme auf Ihrem System muss das EPEL-Repository (Extra Packages for Enterprise Linux) aktiviert sein.

Falls das EPEL-Repository auf Ihrem System nicht konfiguriert ist, müssen Sie es manuell herunterladen und konfigurieren.

Weitere Informationen finden Sie unter "Manuelles Konfigurieren des EPEL-Repositorys".

- Wenn die korrekte Version von MySQL nicht installiert ist, ist für die erfolgreiche Installation der MySQL Software auf Ihrem System die Aktivierung des MySQL Repositorys erforderlich.

  Falls das MySQL-Repository auf Ihrem System nicht konfiguriert ist, müssen Sie es manuell herunterladen und konfigurieren.

  Weitere Informationen finden Sie unter "Manuelle Konfiguration des MySQL-Repositorys".

- Auf Ihrem Unified Manager Host darf nur eine Java-Version installiert sein, andernfalls kann das System möglicherweise nicht bestimmen, welche Version verwendet werden soll. Weitere Informationen finden Sie unter "Nach der Aktualisierung von Java auf dem Active IQ Unified Manager Host starten die Services nicht.".

Wenn Ihr System keinen Internetzugang hat und die Repositories nicht von einem System mit Internetverbindung auf das System ohne Verbindung gespiegelt werden, sollten Sie die Installationsanweisungen befolgen, um die externen Softwareabhängigkeiten Ihres Systems zu ermitteln. Anschließend können Sie die benötigte Software auf das System mit Internetverbindung herunterladen und die `.rpm`Dateien auf das System kopieren, auf dem Sie Unified Manager installieren möchten. Zum Herunterladen der Artefakte und Pakete ist der `yum install`Befehl erforderlich. Voraussetzung ist, dass auf beiden Systemen dieselbe Betriebssystemversion ausgeführt wird und dass die Abonnementlizenz für das entsprechende Red Hat Enterprise Linux gilt.

> Sie dürfen die erforderliche Drittanbietersoftware nur aus den hier aufgeführten Repositories installieren. Software aus den Repositories von Red Hat ist speziell für Red Hat Enterprise Linux entwickelt und entspricht den Best Practices von Red Hat (Verzeichnisstruktur, Berechtigungen usw.). Software aus anderen Quellen entspricht diesen Richtlinien möglicherweise nicht, was zum Fehlschlagen der Unified Manager Installation oder zu Problemen bei zukünftigen Upgrades führen kann.

Anforderung für Port 443

Generische Red Hat Enterprise Linux Images können den externen Zugriff auf Port 443 blockieren. Aufgrund dieser Einschränkung ist es nach der Installation von Unified Manager möglicherweise nicht möglich, eine Verbindung zur Administrator-Weboberfläche herzustellen. Der folgende Befehl ermöglicht den Zugriff auf Port 443 für alle externen Benutzer und Anwendungen auf einem generischen Red Hat Enterprise Linux System.

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

Sie müssen Red Hat Enterprise Linux mit der Basisumgebung „Server with GUI“ installieren. Sie stellt die Befehle bereit, die in den Installationsanweisungen für Unified Manager verwendet werden. Bei anderen Basisumgebungen müssen Sie möglicherweise zusätzliche Befehle installieren, um die Installation zu überprüfen oder abzuschließen. Falls `firewall-cmd` auf Ihrem System nicht verfügbar ist, müssen Sie es mit dem folgenden Befehl installieren:

```
# sudo yum install firewalld
```

Wenden Sie sich vor dem Ausführen der Befehle an Ihre IT-Abteilung, um zu klären, ob Ihre Sicherheitsrichtlinien ein anderes Vorgehen erfordern.

THP (Transparent Huge Pages) sollte auf Red Hat-Systemen deaktiviert werden. Wenn es aktiviert ist, kann es in manchen Fällen dazu führen, dass der Unified Manager heruntergefahren wird, wenn bestimmte Prozesse zu viel Arbeitsspeicher belegen und beendet werden.

Unterstützte Browser für Active IQ Unified Manager verwenden

Der Zugriff auf die Web-Benutzeroberfläche des Unified Manager erfolgt über einen unterstützten Browser.

Die Interoperability Matrix enthält die Liste der unterstützten Browserversionen.

"mysupport.netapp.com/matrix"

Bei allen Browsern gewährleistet das Deaktivieren von Pop-up-Blockern, dass die Softwarefunktionen ordnungsgemäß angezeigt werden.

Wenn Sie Unified Manager für die SAML-Authentifizierung konfigurieren möchten, damit ein Identitätsanbieter (IdP) Benutzer authentifizieren kann, sollten Sie auch die Liste der vom IdP unterstützten Browser überprüfen.

Informationen zu Protokoll- und Portanforderungen in Active IQ Unified Manager

Die erforderlichen Ports und Protokolle ermöglichen die Kommunikation zwischen dem Unified Manager Server und den verwalteten Storage-Systemen, Servern und anderen Komponenten.

Verbindungen zum Unified Manager Server

Bei typischen Installationen müssen Sie beim Verbinden mit der Unified Manager Web-UI keine Portnummern angeben, da immer Standardports verwendet werden. Da Unified Manager beispielsweise immer versucht, auf seinem Standardport zu laufen, können Sie `https://<host>` anstelle von `https://<host>:443` eingeben.

Der Unified Manager Server verwendet spezifische Protokolle, um auf die folgenden Schnittstellen zuzugreifen:

Schnittstelle	Protokoll	Port	Beschreibung
Unified Manager Web-Benutzeroberfläche	HTTP	80	Dient zum Zugriff auf die Web-UI von Unified Manager; die Weiterleitung zum sicheren Port 443 erfolgt automatisch.
Unified Manager Web-Benutzeroberfläche und Programme, die APIs verwenden	HTTPS	443	Dient dem sicheren Zugriff auf die Unified Manager Weboberfläche oder zum Durchführen von API-Aufrufen; API-Aufrufe können nur über HTTPS erfolgen.

Schnittstelle	Protokoll	Port	Beschreibung
Managementplattform	SSH/SFTP	22	Dient zum Zugriff auf die Managementplattform und zum Abrufen von Support-Bundles.
Linux Befehlszeile	SSH/SFTP	22	Dient zum Zugriff auf die Red Hat Enterprise Linux Befehlszeile und zum Abrufen von Support-Bundles.
MySQL Datenbank	MySQL	3306	Dient zum Aktivieren des Zugriffs von OnCommand Workflow Automation und OnCommand API Services auf Unified Manager.
Syslog	UDP	514	Dient zum Zugriff auf abonnementbasierte EMS-Nachrichten aus ONTAP Systemen und zum Erstellen von Ereignissen auf Basis dieser Nachrichten.
REST	HTTPS	9443	Wird verwendet, um auf EMS-Ereignisse in Echtzeit über die REST API von authentifizierten ONTAP Systemen zuzugreifen.
MySQL Datenbank	MySQL	3306	Dient zum Aktivieren des Zugriffs von OnCommand Workflow Automation und OnCommand API Services auf Unified Manager.
AMQP-QPID-Broker	TCP/IP	56072	Dient der internen Nachrichtenkommunikation.
AMQP-QPID-Broker	WebSocket über TCP	56080	Dient zum Lauschen an diesem Port auf Nachrichten von ONTAP (cloud agent).
AMQP-QPID-Broker	WebSocket über TCP	56443	Dieser Port dient zum Empfangen von Nachrichten von ONTAP (cloud agent). Die Kommunikation über diesen Port unterstützt die Verschlüsselung mittels TLS oder SSL.

Der Standardport für MySQL, 3306, ist bei der Installation von Unified Manager auf Linux-Systemen nur auf localhost beschränkt. Dies hat keine Auswirkungen auf Upgrade-Szenarien, bei denen die vorherige Konfiguration beibehalten wird. Diese Konfiguration kann geändert werden, und die Verbindung kann mithilfe der `Control access to MySQL port 3306` Option in der Managementplattform für andere Hosts verfügbar gemacht werden. Informationen dazu enthält "Weitere Menüoptionen". Die für die HTTP- und HTTPS-Kommunikation verwendeten Ports (Ports 80 und 443) können über die Unified Manager Managementplattform geändert werden. Weitere Informationen enthält "Menüs der Managementplattform für die Wartung".

Verbindungen vom Unified Manager Server

Ihre Firewall sollte so konfiguriert sein, dass die Ports geöffnet sind, die die Kommunikation zwischen dem Unified Manager Server und verwalteten Storage Systemen, Servern und anderen Komponenten ermöglichen. Wenn ein Port nicht geöffnet ist, schlägt die Kommunikation fehl.

Je nach Ihrer Umgebung können Sie die Ports und Protokolle, die der Unified Manager-Server für die Verbindung zu bestimmten Zielen verwendet, ändern.

Der Unified Manager Server stellt über die folgenden Protokolle und Ports Verbindungen zu den verwalteten Storage Systemen, Servern und anderen Komponenten her:

Ziel	Protokoll	Port	Beschreibung
Speichersystem	HTTPS	443/TCP	Dient zur Überwachung und zum Managen von Storage Systemen.
Speichersystem	NDMP	10000/TCP	Wird für bestimmte Snapshot-Wiederherstellungsvorgänge verwendet.
AutoSupport Server	HTTPS	443	Dient zum Versenden von AutoSupport Informationen. Für diese Funktion ist ein Internetzugang erforderlich.
Authentifizierungsserver	LDAP	389	Dient zum Stellen von Authentifizierungsanforderungen sowie von Benutzer- und Gruppensuchanfragen.
LDAPS	636	Für die sichere LDAP-Kommunikation verwendet.	Mailserver
SMTP	25	Zum Senden von Benachrichtigungs-E-Mails verwendet.	SNMP-Trap-Sender
SNMPv1 oder SNMPv3	162/UDP	Dient zum Senden von SNMP-Traps für Warnmeldungen.	Server des externen Datenanbieters

Ziel	Protokoll	Port	Beschreibung
TCP	2003	Dient zum Senden von Performance-Daten an einen externen Datenanbieter wie Graphite.	NTP-Server
NTP	123/UDP	Dient zur Synchronisierung der Zeit auf dem Unified Manager Server mit einem externen NTP Zeitserver. (nur VMware Systeme)	Syslog
UDP	514	Dient Unified Manager zum Senden von Audit-Protokollen an einen Remote-Syslog-Server.	AMQP-QPID-Broker
TCP/IP	56072	Dient der internen Nachrichtenkommunikation.	AMQP-QPID-Broker
WebSocket über TCP	56080	Dient zum Lauschen an diesem Port auf Nachrichten von ONTAP (cloud agent).	AMQP-QPID-Broker

Das Arbeitsblatt in Active IQ Unified Manager wird vervollständigt

Bevor Sie Unified Manager installieren und konfigurieren, sollten Sie spezifische Informationen zu Ihrer Umgebung bereithalten. Sie können diese Informationen im Arbeitsblatt festhalten.

Installationsinformationen für Unified Manager

Die für die Installation von Unified Manager erforderlichen Details.

System, auf dem die Software eingesetzt wird	Ihr Wert
vollqualifizierter Domainname des Hosts	
Host-IP-Adresse	
Netzwerkmaske	
Gateway-IP-Adresse	
Primäre DNS-Adresse	
Sekundäre DNS-Adresse	
Suchdomänen	
Benutzername für Wartungsarbeiten	
Wartungsbenutzerpasswort	

Unified Manager Konfigurationsinformationen

Die Details zur Konfiguration von Unified Manager nach der Installation. Einige Werte sind je nach Ihrer Konfiguration optional.

Einstellung	Ihr Wert
E-Mail-Adresse des Wartungsbenutzers	
SMTP Server Hostname oder IP-Adresse	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Port	25 (Standardwert)
E-Mail-Adresse, von der Benachrichtigungen versendet werden	
Hostname oder IP-Adresse des Authentifizierungsservers	
Name des Active Directory Administrators oder individueller Name für die LDAP-Bindung	
Active Directory Passwort oder LDAP Bind-Passwort	
Basis-individueller Name des Authentifizierungsservers	
URL des Identitätsanbieters (IdP)	
Metadaten des Identitätsanbieters (IdP)	
IP-Adressen von SNMP-Trap-Zielhosts	
SNMP-Port	

Clusterinformationen

Die Details zu den Storage-Systemen, die Sie mit Unified Manager managen.

Cluster 1 von N	Ihr Wert
Hostname oder Cluster-Management-IP-Adresse	
ONTAP Administrator-Benutzername Dem Administrator muss die Rolle “admin” zugewiesen worden sein.	
ONTAP Administratorpasswort	
Protokoll	HTTPS

Unified Manager Software installieren, aktualisieren und entfernen

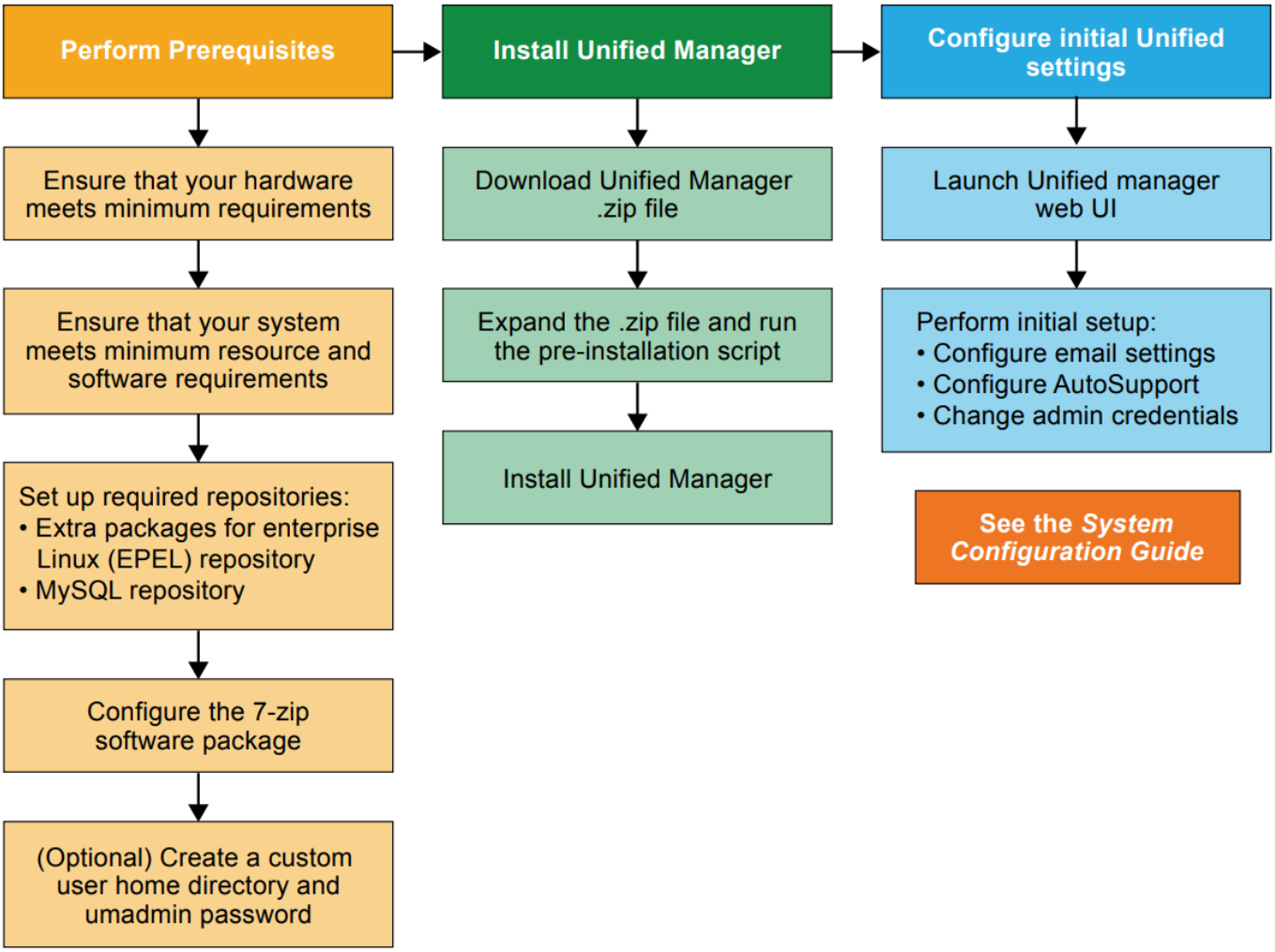
Installation, Aktualisierung und Deinstallation der Active IQ Unified Manager Software

Auf Linux-Systemen können Sie die Unified Manager Software installieren, auf eine neuere Version der Software aktualisieren oder Unified Manager entfernen.

Unified Manager kann auf Red Hat Enterprise Linux Servern installiert werden. Der Linux Server, auf dem Sie Unified Manager installieren, kann entweder auf einem physischen Rechner oder auf einer virtuellen Maschine ausgeführt werden, die unter VMware ESXi, Microsoft Hyper-V oder Citrix XenServer ausgeführt wird.

Die Installationsreihenfolge für Active IQ Unified Manager auf Red Hat Enterprise Linux

Der Installationsablauf beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.



Einrichtung der erforderlichen Software

Die Konfiguration des EPEL-Repositorys für Active IQ Unified Manager

Wenn das System, auf dem Sie Unified Manager installieren, keinen Zugriff auf das

Repository Extra Packages for Enterprise Linux (EPEL) hat, müssen Sie das Repository manuell herunterladen und konfigurieren, um eine erfolgreiche Installation sicherzustellen.

Das EPEL-Repository stellt die erforderlichen Drittanbieter-Dienstprogramme bereit, die auf Ihrem System installiert werden müssen. Sie verwenden das EPEL-Repository, um Unified Manager auf einem Red Hat Enterprise Linux-System zu installieren.

Schritte

1. Das EPEL-Repository für Ihre Installation steht zum Download bereit. Für Version 8 steht es hier zum Download bereit:

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

   Für Version 9 steht der Download hier zur Verfügung:

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

2. Konfiguration des EPEL-Repositorys:

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

Wenn bei Red Hat Enterprise Linux 8 Systemen interne Repositories mit modularen RPM-Paketen verwendet werden, zum Beispiel *javapackages-filesystem-<version>.module.rpm*, müssen die Metadaten für die modularen Pakete ebenfalls im selben Repository verfügbar sein.

Konfiguration des MySQL-Repositorys für Active IQ Unified Manager

Wenn das System, auf dem Sie Unified Manager installieren, keinen Zugriff auf das MySQL Community Edition Repository hat, müssen Sie das Repository manuell herunterladen und konfigurieren, um eine erfolgreiche Installation zu gewährleisten.

Das MySQL-Repository bietet Zugriff auf die erforderliche MySQL-Software, die auf Ihrem System installiert werden muss.

> Diese Aufgabe kann fehlschlagen, wenn das System keine Internetverbindung hat. Wenn das System, auf dem Sie Unified Manager installieren, keinen Internetzugang hat, finden sich entsprechende Informationen in der MySQL-Dokumentation.

Schritte

1. Das passende MySQL-Repository für Ihre Installation steht zum Download bereit. Für Version 8 ist es hier verfügbar:

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

   Für Version 9 steht der Download hier zur Verfügung:

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

2. Konfiguration des MySQL-Repositorys:

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

Wenn Sie auf einem Red Hat Enterprise Linux 8-System interne Repositories mit java-17-openjdk, 7-zip und anderen Softwarepaketen verwenden, die vom AppStream Repository bereitgestellt werden, müssen Sie Ihr AppStream Repository deaktivieren und den MySQL Community Server installieren. Der folgende Befehl ist auszuführen:

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

Falls eine Fehlermeldung wegen eines fehlenden oder nicht übereinstimmenden Schlüssels angezeigt wird und die Installation fehlschlägt, können folgende Schritte hilfreich sein:

- Auf einem verbundenen System lässt sich der aktualisierte MySQL-Schlüssel mit folgendem Befehl importieren:

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

for example:

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

- Auf einem System ohne Internetverbindung ist Ihre MySQL Repository-Datei zu aktualisieren und `gpgcheck` durch Markieren von `gpgcheck=0` zu deaktivieren.

Konfiguration des 7-Zip-Softwarepakets in Active IQ Unified Manager

Für die erfolgreiche Installation von Unified Manager auf einem Red Hat Enterprise Linux System muss Ihr System Zugriff auf das 7-zip Softwarepaket haben. Wenn Netzwerkzugriff verfügbar ist und die 7-zip URL nicht durch eine Firewall blockiert wird, wird 7-zip während eines Installations- oder Upgrade-Prozesses automatisch auf Ihr System heruntergeladen. NetApp empfiehlt die automatische Download-Methode.

Die folgende URL darf in Ihrer Firewall nicht blockiert sein, damit Unified Manager das 7-zip-Softwarepaket automatisch herunterladen kann:
https://7-zip.org/a/7z2301-linux-x64.tar.xz

Alternativ können Sie 7-zip vorinstallieren.

Vorabinstallation des 7-zip-Pakets

7-zip kann vorinstalliert werden, indem es manuell heruntergeladen oder ein mitgeliefertes Skript verwendet wird. Es kann eine der folgenden beiden Methoden gewählt werden:

Download mithilfe eines mitgelieferten Skripts

Schritt

1. Das im Unified Manager ZIP-Archiv enthaltene `install7zip.sh`Skript ist auszuführen.

Manuelles Herunterladen

Das 7-zip Paket sollte ausschließlich von der offiziellen Website heruntergeladen werden.

Schritte

1. Das 7-zip-Paket (Version 23.01) kann von der offiziellen Website heruntergeladen werden:

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

2. Kopieren der Datei auf Ihre virtuelle RHEL-Maschine:

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

3. Archiv extrahieren:

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

4. Verschieben der `7zz`Datei in das `/usr/bin/`Verzeichnis:

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

5. Ausführungsberechtigungen festlegen:

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

Überprüfen Sie die Installation

Zu prüfen ist, ob das 7-zip-Paket erfolgreich auf Ihrem System installiert wurde:

```
7zz -version
```

SELinux für NFS- und CIFS-Freigaben in Active IQ Unified Manager konfigurieren

Wenn Sie planen, `/opt/netapp` oder `/opt/netapp/data` auf einem NAS- oder SAN-Gerät einzubinden, und SELinux aktiviert ist, sind einige Punkte zu beachten.

Wenn Sie planen, `/opt/netapp` oder `/opt/netapp/data` von einem anderen Ort als dem Root-Dateisystem einzubinden und SELinux in Ihrer Umgebung aktiviert ist, sollten Sie den korrekten Kontext für die eingebundenen Verzeichnisse festlegen. Für das in Ihrer Umgebung zutreffende Szenario folgen unten die Schritte zum Festlegen und Bestätigen des korrekten SELinux-Kontexts.

Konfiguration des SELinux-Kontexts, wenn `/opt/netapp/data` eingehängt ist

Wenn Sie `/opt/netapp/data` in Ihrem System eingebunden haben und SELinux auf `Enforcing` gesetzt ist, sollte der SELinux-Kontexttyp für `/opt/netapp/data` auf `mysqld_db_t` gesetzt sein; dies ist das

Standardkontextelement für den Speicherort der Datenbankdateien.

1. Mit diesem Befehl lässt sich der Kontext überprüfen:

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

   Beispielausgabe:

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

   In dieser Ausgabe ist der Kontext `default_t`. Dieser Kontext sollte zu `mysqld_db_t` geändert werden.

2. Die folgenden Schritte dienen dazu, den Kontext entsprechend der Art der Einbindung `/opt/netapp/data` festzulegen.

   a. Zum Festlegen des Kontexts auf `mysqld_db_t` werden die folgenden Befehle ausgeführt:
   `semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"`
   `` `restorecon -R -v /opt/netapp/data ``

   b. Wenn Sie `/opt/netapp/data` in `/etc/fstab` konfiguriert haben, sollten Sie die `/etc/fstab`Datei bearbeiten. Für die `/opt/netapp/data/` Mount-Option erfolgt das Hinzufügen der MySQL-Bezeichnung wie folgt:

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

   c. Aushängen und erneut einbinden `/opt/netapp/data/`, um den Kontext zu aktivieren.

   d. Wenn Sie eine direkte NFS-Einbindung haben, können Sie den folgenden Befehl verwenden, um den Kontext auf `mysqld_db_t` festzulegen:

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

3. Prüfen, ob der Kontext korrekt eingestellt ist:

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

Beispielausgabe:

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

Konfiguration des SELinux-Kontexts, wenn `/opt/netapp` eingebunden ist und `/opt/netapp/data/` ebenfalls separat eingebunden ist

In diesem Szenario sollte zunächst der Kontext für `/opt/netapp/data/` wie im vorherigen Abschnitt beschrieben festgelegt werden. Nach dem Festlegen des korrekten Kontexts für `/opt/netapp/data/` darf für das übergeordnete Verzeichnis `/opt/netapp` der SELinux-Kontext nicht auf `file_t` gesetzt sein.

Schritte

1. Mit diesem Befehl lässt sich der Kontext überprüfen:

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

   Beispielausgabe:

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

   In dieser Ausgabe ist der Kontext `file_t` zu ändern. Die folgenden Befehle setzen den Kontext auf `usr_t`. Sie können den Kontext je nach Ihren Sicherheitsanforderungen auf einen beliebigen anderen Wert als `file_t` setzen.

2. Die folgenden Schritte dienen dazu, den Kontext festzulegen, abhängig davon, wie Sie eingebunden `/opt/netapp` haben.

   a. Zum Festlegen des Kontexts dienen die folgenden Befehle:

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

1. Wenn Sie `/opt/netapp` in `/etc/fstab` konfiguriert haben, sollten Sie die `/etc/fstab` Datei bearbeiten. Für die `/opt/netapp` Mount-Option erfolgt das Hinzufügen der MySQL-Bezeichnung wie folgt:

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

2. Zum Aktivieren des Kontexts ist ein Aushängen und anschließendes erneutes Einhängen `/opt/netapp` erforderlich.
3. Bei einer direkten NFS-Einbindung kann zum Festlegen des Kontexts der folgende Befehl verwendet werden:

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

   a. Prüfen, ob der Kontext korrekt eingestellt ist:

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

   Beispielausgabe

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

Konfiguration des SELinux-Kontexts, wenn `/opt/netapp` eingehängt ist und `/opt/netapp/data/` nicht separat eingehängt ist

Wenn Sie `/opt/netapp` in Ihrem System eingebunden haben und SELinux auf `Enforcing` eingestellt ist, muss der SELinux-Kontexttyp für `/opt/netapp` auf `mysqld_db_t` eingestellt sein, was das Standardkontextelement für den Speicherort der Datenbankdateien ist.

Schritte

1. Mit diesem Befehl lässt sich der Kontext überprüfen:

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

   Beispielausgabe:

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

   In dieser Ausgabe ist der Kontext `default_t`. Dieser Kontext sollte zu `mysqld_db_t` geändert werden.

2. Die folgenden Schritte dienen zum Festlegen des Kontexts entsprechend der Art, wie Sie `/opt/netapp` eingebunden haben.

   a. Die folgenden Befehle dienen zum Festlegen des Kontexts auf `mysqld_db_t`:
   `semanage fcontext -a -t mysqld_db_t "/opt/netapp"`
   `` `restorecon -R -v /opt/netapp ``

   b. Wenn Sie `/opt/netapp` in `/etc/fstab` konfiguriert haben, müssen Sie die Datei `/etc/fstab` bearbeiten. Für die `/opt/netapp/` Mount-Option können Sie die MySQL-Bezeichnung wie folgt hinzufügen:
   `context=system_u:object_r:mysqld_db_t:s0`

   c. Aushängen und dann erneut einbinden `/opt/netapp/`, um den Kontext zu aktivieren.

   d. Bei einer direkten NFS-Einbindung kann der folgende Befehl verwendet werden, um den Kontext auf `mysqld_db_t`:
   `mount <nfsshare>:/<mountpoint> /opt/netapp -o context=system_u:object_r:mysqld_db_t:s0` festzulegen.

3. Prüfen, ob der Kontext korrekt eingestellt ist:

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

Beispielausgabe:

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

Installation von Unified Manager auf Linux-Systemen

Erstellen Sie vor der Installation von Active IQ Unified Manager ein benutzerdefiniertes Home-Verzeichnis für den Benutzer und ein umadmin Passwort

Vor der Installation von Unified Manager kann ein benutzerdefiniertes Home-Verzeichnis erstellt und ein eigenes Benutzerpasswort für umadmin definiert werden. Diese Aufgabe ist optional, aber an manchen Standorten ist möglicherweise die Flexibilität erforderlich, die Standardinstallationseinstellungen von Unified Manager zu überschreiben.

Bevor Sie beginnen

- Das System muss die in "Hardwaresystemanforderungen" beschriebenen Anforderungen erfüllen.
- Sie müssen sich als Root-Benutzer beim Red Hat Enterprise Linux System anmelden können.

Die Standardinstallation des Unified Manager führt folgende Aufgaben aus:

- Erstellt den Benutzer umadmin mit `/home/umadmin`als Home-Verzeichnis.
- Weist dem Benutzer umadmin das Standardpasswort “admin” zu.

Da manche Installationsumgebungen den Zugriff auf `/home` das Home-Verzeichnis einschränken, schlägt die Installation fehl. Das Home-Verzeichnis ist an einem anderen Ort zu erstellen. Darüber hinaus gelten an manchen Standorten möglicherweise Regeln zur Passwortkomplexität, oder es wird verlangt, dass Passwörter von lokalen Administratoren statt vom Installationsprogramm festgelegt werden.

Wenn Ihre Installationsumgebung das Überschreiben dieser Standardinstallationseinstellungen erfordert, dienen die folgenden Schritte zum Erstellen eines benutzerdefinierten Home-Verzeichnisses und zum Festlegen des Passworts des Benutzers umadmin.

Wenn diese Informationen vor der Installation definiert werden, erkennt das Installationsskript diese Einstellungen und verwendet die definierten Werte anstelle der Standardeinstellungen der Installation.

Zusätzlich enthält die Standardinstallation von Unified Manager den Benutzer umadmin in den sudoers-Dateien (`ocum_sudoers` und `ocie_sudoers`) im `/etc/sudoers.d/` Verzeichnis. Wenn Sie diese Einträge aufgrund von Sicherheitsrichtlinien oder eines Sicherheitsüberwachungstools aus Ihrer Umgebung entfernen, müssen Sie sie wieder hinzufügen. Sie müssen die sudoers-Konfiguration beibehalten, da einige Unified Manager-Operationen diese sudo-Berechtigungen erfordern.

Die Sicherheitsrichtlinien Ihrer Umgebung dürfen die sudo-Berechtigungen des Unified Manager-Wartungsbenutzers nicht einschränken. Einige Unified Manager-Vorgänge können fehlschlagen, wenn die Berechtigungen eingeschränkt sind. Nach erfolgreicher Installation sollte bei der Anmeldung als umadmin-Benutzer überprüft werden, dass der folgende sudo-Befehl ausgeführt werden kann.

```
sudo systemctl status ocie
```

Dieser Befehl sollte den entsprechenden Status des ocie Service ohne Fehler zurückgeben.

Schritte

1. Die Anmeldung am Server erfolgt als Root-Benutzer.
2. Erstellung des umadmin Gruppenkontos mit dem Namen “maintenance”:

   ```
   groupadd maintenance
   ```

3. Die Erstellung des Benutzerkontos “umadmin” erfolgt in der Wartungsgruppe unter einem Home-Verzeichnis Ihrer Wahl:

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

4. Definition des umadmin Passworts:

   ```
   passwd umadmin
   ```

   Das System fordert Sie auf, eine neue Passwortzeichenfolge für den Benutzer umadmin einzugeben.

Nach der Installation von Unified Manager müssen Sie die Login-Shell des Benutzers umadmin angeben.

Download von Active IQ Unified Manager

Sie müssen die Unified Manager `.zip` Datei von der NetApp Support Site herunterladen, um Unified Manager zu installieren.

Bevor Sie beginnen

Sie benötigen Anmeldedaten für die NetApp Support Site.

Sie laden das Unified Manager Installationspaket für das Red Hat Enterprise Linux System herunter.

Schritte

1. Anmeldung bei der NetApp Support Site und Navigation zur Download-Seite für Unified Manager:

   "NetApp Support Site"

2. Die gewünschte Version von Unified Manager ist auszuwählen und die Endbenutzer-Lizenzvereinbarung (EULA) ist zu akzeptieren.
3. Die Unified Manager Installationsdatei für Linux kann heruntergeladen und die `.zip`Datei in einem Verzeichnis auf dem Zielsystem gespeichert werden.

   - Für Ihr Red Hat Enterprise Linux-System muss die richtige Version der Installationsdatei heruntergeladen werden. Je nachdem, ob Red Hat Enterprise Linux 8 oder 9 installiert ist, muss die entsprechende Version der Unified Manager `.zip` Datei heruntergeladen werden.
   - NetApp empfiehlt, das Code-Signaturzertifikat (`.pem`) und die digitale Signatur (`.sig`) zusammen mit der `.zip` Datei herunterzuladen.

4. Die Prüfsumme der heruntergeladenen Software auf Integrität überprüfen.
5. Wenn Sie das Codesignaturzertifikat und die digitale Signatur heruntergeladen haben, können Sie die Integrität der Installationsdatei überprüfen. Für die Überprüfung der Integrität der Installationsdatei stehen die folgenden Befehle zur Verfügung:
   - Dieser Befehl erstellt eine Datei mit dem öffentlichen Schlüssel aus dem Code-Signing-Zertifikat:

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

     - Dabei ist **AIQUM-RHEL-CLIENT-INTER-ROOT.pem** die Datei, die das Codesignaturzertifikat enthält.
   - Dieser Befehl überprüft die Signatur der Installationsdatei:

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

     Eine Meldung ähnlich wie `Verified Ok` bestätigt, dass die Installationsdatei sicher verwendet werden kann.

Installieren von Active IQ Unified Manager auf Red Hat Enterprise Linux

Sie können Unified Manager auf einer physischen oder virtuellen Red Hat Enterprise Linux Plattform installieren.

Bevor Sie beginnen

- Das System, auf dem Sie Unified Manager installieren möchten, muss die System- und Softwareanforderungen erfüllen.

  Weitere Informationen finden Sie unter "Hardwaresystemanforderungen".

  Weitere Informationen finden Sie unter "Linux Software und Installationsanforderungen".

- Sie müssen die Unified Manager `.zip` Datei von der NetApp Support Site auf das Zielsystem heruntergeladen haben.
- Sie sollten die Integrität der heruntergeladenen `.zip` Datei überprüft haben.
- Sie benötigen einen unterstützten Webbrowser.
- Ihre Emulationssoftware muss die Scrollback-Funktion aktiviert haben.

Das Red Hat Enterprise Linux System verfügt möglicherweise über alle erforderlichen Versionen der benötigten unterstützenden Software (Java, MySQL, zusätzliche Dienstprogramme), nur über einen Teil der benötigten Software oder ist ein neu installiertes System, auf dem keine der benötigten Software installiert ist.

Schritte

1. Die Anmeldung auf dem Server, auf dem Sie Unified Manager installieren, ist erforderlich.
2. Mit den entsprechenden Befehlen lässt sich ermitteln, welche Software auf dem Zielsystem möglicherweise installiert oder aktualisiert werden muss, um die Installation zu unterstützen:

Erforderliche Software und Mindestversion	Befehl zur Überprüfung von Software und Version
OpenJDK Version 17.0.14+6	`java -version`
MySQL 8.4.10 Community Edition	`rpm -qa
grep -i mysql`	7-zip

3. Falls die installierte Version von MySQL älter als MySQL 8.4.10 Community Edition ist, muss folgender Befehl eingegeben werden, um sie zu deinstallieren:

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

   Falls Abhängigkeitsfehler auftreten, müssen Sie die `--nodeps` Option zum Deinstallieren der Komponente hinzufügen.

4. Zum Verzeichnis, in das Sie die Installations `.zip`datei heruntergeladen haben, navigieren und das Unified Manager Bundle entpacken:

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

   Die für Unified Manager erforderlichen `.rpm` Module werden in das Zielverzeichnis entpackt.

5. Zu überprüfen ist, ob das folgende Modul im Verzeichnis verfügbar ist:

   ```
   ls *.rpm
   ```

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

6. Zum Sicherstellen, dass keine Systemkonfigurationseinstellungen oder installierte Software vorhanden sind, die mit der Installation von Unified Manager in Konflikt stehen könnten, wird das Vorinstallationsskript ausgeführt:

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

   Das Vorinstallationsskript prüft, ob das System über ein gültiges Red Hat Enterprise Linux-Abonnement verfügt und Zugriff auf die erforderlichen Software-Repositories hat. Falls das Skript Probleme feststellt, ist vor der Installation von Unified Manager eine Behebung dieser Probleme erforderlich.

   Wenn Sie für ein Red Hat Enterprise Linux 8 System interne Repositories mit JDK 17 - OpenJDK, 7-zip und anderen Softwarepaketen verwenden, die vom AppStream Repository bereitgestellt werden, müssen Sie Ihr AppStream Repository deaktivieren und MySQL Community Server installieren. Hierfür dient der folgende Befehl:

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

7. **Optional:** Schritt 7 ist nur erforderlich, wenn Ihr System nicht mit dem Internet verbunden ist und Sie die für Ihre Installation erforderlichen Pakete manuell herunterladen müssen. Wenn Ihr System über Internetzugriff verfügt und alle erforderlichen Pakete verfügbar sind, ist mit Schritt 8 fortzufahren. Bei Systemen ohne Internetverbindung oder ohne Nutzung der Red Hat Enterprise Linux Repositories sind die folgenden Schritte auszuführen, um festzustellen, ob erforderliche Pakete fehlen, und diese Pakete anschließend herunterzuladen:

   a. Auf dem System, auf dem Sie Unified Manager installieren, können Sie die Liste der verfügbaren und nicht verfügbaren Pakete einsehen:
      `yum install netapp-um<version>.x86_64.rpm --assumeno`

      Die Einträge im Abschnitt “Installing:” sind die Pakete, die im aktuellen Verzeichnis verfügbar sind, und die Einträge im Abschnitt “Installing for dependencies:” sind die Pakete, die auf Ihrem System fehlen.

   b. Auf einem System mit Internetzugang können die fehlenden Pakete heruntergeladen werden:

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

      Da das Plugin “yum-plugin-downloadonly” auf Red Hat Enterprise Linux Systemen nicht immer aktiviert ist, kann es erforderlich sein, die Funktion zum Herunterladen eines Pakets ohne Installation zu aktivieren:
      `yum install yum-plugin-downloadonly`

   a. Das Kopieren der fehlenden Pakete vom mit dem Internet verbundenen System auf das Installationssystem ist erforderlich.

8. Als Root-Benutzer oder unter Verwendung von `sudo` wird der folgende Befehl ausgeführt, um die Software zu installieren:

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

Dieser Befehl installiert die .rpm-Pakete, alle weiteren erforderlichen Zusatzsoftwarepakete und die Unified Manager Software.

Falls die Installation mit dem GPG NOKEY Fehler fehlschlägt, kann `rpm --import` zum Importieren der Schlüssel von einer URL verwendet werden:

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

> Von einer Installation mit alternativen Befehlen (wie `rpm -ivh`) ist abzusehen. Eine erfolgreiche Installation von Unified Manager auf einem Red Hat Enterprise Linux System setzt voraus, dass alle Unified Manager Dateien und zugehörigen Dateien in einer bestimmten Reihenfolge in einer bestimmten Verzeichnisstruktur installiert werden, und der `yum install netapp-um<version>.x86_64.rpm` Befehl setzt diese Struktur automatisch durch.

9. Die E-Mail-Benachrichtigung, die unmittelbar nach den Installationsmeldungen angezeigt wird, kann unberücksichtigt bleiben.

   Die E-Mail benachrichtigt den Root-Benutzer über einen anfänglichen Ausfall eines Cron-Jobs, der jedoch keine negativen Auswirkungen auf die Installation hat.

10. Nachdem die Installationsmeldungen abgeschlossen sind, können Sie in den Meldungen zurückblättern, bis die Meldung angezeigt wird, in der das System eine IP-Adresse oder URL für die Unified Manager Weboberfläche, den Wartungsbenutzernamen (umadmin) und ein Standardpasswort anzeigt.

    Die Nachricht lautet in etwa wie folgt:

    ```
    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. Zu erfassen sind die IP-Adresse oder URL, der zugewiesene Benutzername (umadmin) und das aktuelle Passwort.
12. Wenn Sie vor der Installation von Unified Manager ein umadmin-Benutzerkonto mit einem benutzerdefinierten Home-Verzeichnis erstellt haben, müssen Sie die Anmelde-Shell des umadmin-Benutzers angeben:

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

Für die Änderung des Standardpassworts des Benutzers „umadmin“ und die Durchführung der Ersteinrichtung von Unified Manager steht die Web-Benutzeroberfläche wie in "Konfigurieren von Active IQ Unified Manager"

beschrieben zur Verfügung. Die Änderung des Standardpassworts des Benutzers „umadmin“ ist zwingend erforderlich.

Informationen zu den Benutzern, die während der Installation von Active IQ Unified Manager erstellt wurden

Bei der Installation von Unified Manager auf Red Hat Enterprise Linux werden durch Unified Manager und Drittanbieter-Dienstprogramme die folgenden Benutzer erstellt: umadmin, jboss und mysql.

- **umadmin**

  Wird für die erste Anmeldung bei Unified Manager verwendet. Diesem Benutzer ist die Benutzerrolle “Application Administrator” zugewiesen, und er ist als Typ “Maintenance User” konfiguriert. Unified Manager erstellt diesen Benutzer.

- **jboss**

  Dient zum Ausführen von Unified Manager Services im Zusammenhang mit dem JBoss-Dienstprogramm. Dieser Benutzer wird von Unified Manager erstellt.

- **mysql**

  Dient zum Ausführen von MySQL-Datenbankabfragen von Unified Manager. Das MySQL-Drittanbieter-Dienstprogramm erstellt diesen Benutzer.

Zusätzlich zu diesen Benutzern erstellt Unified Manager auch entsprechende Gruppen: maintenance, jboss und mysql. Die Gruppen maintenance und jboss werden von Unified Manager erstellt, während die Gruppe mysql von einem Drittanbieter-Tool erstellt wird.

Wenn Sie vor der Installation von Unified Manager ein benutzerdefiniertes Home-Verzeichnis erstellt und Ihr eigenes umadmin-Benutzerkennwort definiert haben, werden die Wartungsgruppe und der umadmin-Benutzer vom Installationsprogramm nicht neu erstellt.

Das JBoss-Passwort in Active IQ Unified Manager ändern

Sie können das während der Installation festgelegte instanzspezifische JBoss Passwort zurücksetzen. Das Zurücksetzen des Passworts ist optional, falls Ihr Standort diese Sicherheitsfunktion benötigt, um die Installationseinstellung von Unified Manager zu überschreiben. Durch diesen Vorgang wird auch das Passwort geändert, das JBoss für den Zugriff auf MySQL verwendet.

- Sie benötigen Root-Benutzerzugriff auf das Red Hat Enterprise Linux-System, auf dem Unified Manager installiert ist.
- Sie müssen auf das von NetApp `password.sh` bereitgestellte Skript im Verzeichnis `/opt/netapp/essentials/bin` zugreifen können.

Schritte

1. Am System ist eine Anmeldung als Root-Benutzer erforderlich.
2. Die folgenden Befehle dienen dazu, die Unified Manager Services in der angegebenen Reihenfolge zu beenden:

```
systemctl stop ocieau

systemctl stop ocie
```

Die zugehörige MySQL-Software darf nicht angehalten werden.

3. Der Prozess zum Ändern des Passworts beginnt mit folgendem Befehl:

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

4. Wenn Sie dazu aufgefordert werden, erfolgt die Eingabe des neuen JBoss Passworts und anschließend dessen erneute Eingabe zur Bestätigung.

   Das Passwort sollte zwischen 8 und 16 Zeichen lang sein und mindestens eine Ziffer, einen Groß- und einen Kleinbuchstaben sowie mindestens eines der folgenden Sonderzeichen enthalten:

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

5. Nach Abschluss des Skripts erfolgt der Start der Unified Manager Services mit den folgenden Befehlen in der angegebenen Reihenfolge:

```
systemctl start ocie

systemctl start ocieau
```

6. Sobald alle Services gestartet sind, können Sie sich bei der Unified Manager Benutzeroberfläche anmelden.

Upgrade von Unified Manager auf Red Hat Enterprise Linux

Upgrade von Active IQ Unified Manager auf Red Hat Enterprise Linux

Sie können Unified Manager aktualisieren, sobald eine neue Version verfügbar ist.

Patch-Releases der Unified Manager-Software werden, sofern sie von NetApp bereitgestellt werden, nach dem gleichen Verfahren installiert wie neue Releases.

Wenn Unified Manager mit einer Instanz von OnCommand Workflow Automation gekoppelt ist und für beide Produkte neue Softwareversionen verfügbar sind, müssen Sie die beiden Produkte trennen und nach den Aktualisierungen eine neue Workflow Automation Verbindung einrichten. Wenn Sie nur eines der Produkte aktualisieren, sollten Sie sich nach der Aktualisierung bei Workflow Automation anmelden und überprüfen, ob Workflow Automation weiterhin Daten aus Unified Manager bezieht.

Der unterstützte Upgrade-Pfad für Versionen von Active IQ Unified Manager ist zu verwenden

Active IQ Unified Manager unterstützt für jede Version einen spezifischen Upgrade-Pfad.

Nicht alle Versionen von Unified Manager unterstützen ein direktes Upgrade auf neuere Versionen. Die Upgrades von Unified Manager sind auf ein N-2-Modell beschränkt. Das bedeutet, dass auf allen Plattformen nur Upgrades auf die nächsten beiden Releases möglich sind. Beispielsweise ist ein Upgrade auf Unified Manager 9.18 nur von Unified Manager 9.14 und 9.16 aus möglich.

Falls Sie eine ältere Version als die unterstützten Versionen verwenden, muss Ihre Unified Manager Instanz zunächst auf eine der unterstützten Versionen und anschließend auf die aktuelle Version aktualisiert werden.

Wenn beispielsweise Unified Manager 9.9 installiert ist und eine Aktualisierung auf Unified Manager 9.14 vorgesehen ist, ist dafür eine Abfolge von Upgrades erforderlich.

Beispielhafter Upgrade-Pfad:

1. Upgrade 9.11 → 9.13
2. Upgrade 9.13 → 9.14
3. Upgrade von 9.13 auf 9.16
4. Upgrade 9.14 oder 9.16 → 9.18

Weitere Informationen zur Upgrade-Pfadmatrix finden Sie in diesem "Knowledge Base Artikel (KB)".

Aktualisieren von Active IQ Unified Manager

Sie können von Unified Manager 9.14 oder 9.16 auf 9.18 aktualisieren, indem Sie die Installationsdatei auf der Linux-Plattform herunterladen und ausführen.

Bevor Sie beginnen

- Das System, auf dem Sie Unified Manager aktualisieren, muss die System- und Softwareanforderungen erfüllen.

  Weitere Informationen finden Sie unter "Hardwaresystemanforderungen".

  Weitere Informationen finden Sie unter "Linux Software und Installationsanforderungen".

- Sie benötigen ein Abonnement für den Red Hat Enterprise Linux Subscription Manager.
- Vor dem Upgrade von Unified Manager müssen Sie die korrekte Version von OpenJDK installieren oder auf diese aktualisieren.

  Weitere Informationen finden Sie unter "JRE-Aktualisierung unter Linux".

- Vor dem Upgrade von Unified Manager muss die richtige Version von 7-zip installiert oder aktualisiert werden. Weitere Informationen finden Sie unter "Konfiguration des 7-zip Softwarepakets".
- Um Datenverlust zu vermeiden, muss für den Fall, dass während des Upgrades ein Problem auftritt, eine Sicherungskopie der Unified Manager Datenbank erstellt worden sein. NetApp empfiehlt, die Sicherungsdatei aus dem `/opt/netapp/data` Verzeichnis an einen externen Speicherort zu verschieben.
- Während des Upgrades werden Sie möglicherweise aufgefordert, zu bestätigen, ob Sie die bisherigen Standardeinstellungen für die Aufbewahrung von Performance-Daten für 13 Monate beibehalten oder auf 6 Monate ändern möchten. Nach der Bestätigung werden die historischen Performance-Daten nach 6 Monaten gelöscht.
- Alle laufenden Vorgänge sollten abgeschlossen sein, da Unified Manager während des Upgrade-Prozesses nicht verfügbar ist.
- Die MySQL Community Edition wird während des Unified Manager Upgrades automatisch aktualisiert. Wenn die auf Ihrem System installierte MySQL-Version älter als 8.4.10 ist, wird MySQL durch den Unified Manager Upgrade-Prozess automatisch auf 8.4.10 aktualisiert.

Schritte

1. Anmeldung am Zielserver Red Hat Enterprise Linux.
2. Das Unified Manager Bundle wird auf den Server heruntergeladen.

Weitere Informationen finden Sie unter "Herunterladen von Unified Manager für Linux".

3. Zum Zielverzeichnis wechseln und das Unified Manager Bundle erweitern:

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

   Die für Unified Manager benötigten RPM-Module werden in das Zielverzeichnis entpackt.

4. Zu überprüfen ist, ob das folgende Modul im Verzeichnis verfügbar ist:

   ```
   ls *.rpm
   ```

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

5. Vor dem Upgrade empfiehlt sich die Ausführung des Vorinstallationsskripts, um sicherzustellen, dass keine Systemkonfigurationseinstellungen oder installierte Software vorhanden sind, die zu Konflikten mit dem Upgrade führen könnten:

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

   Das Vorinstallationsskript prüft, ob das System über ein gültiges Red Hat Enterprise Linux-Abonnement verfügt und Zugriff auf die erforderlichen Software-Repositories hat. Falls das Skript Probleme feststellt, müssen Sie diese beheben, bevor Sie mit dem Upgrade fortfahren können.

   Falls fehlende Pakete erkannt werden, sind die in "Zusätzliche durchzuführende Schritte für fehlende Pakete" genannten Schritte durchzuführen. Wenn keine fehlenden Pakete vorhanden sind, kann mit den nächsten Schritten fortgefahren werden.

6. Die Aktualisierung von Unified Manager erfolgt mithilfe des folgenden Skripts:

   ```
   upgrade.sh
   ```

   Dieses Skript führt die RPM-Module automatisch aus und aktualisiert die erforderliche unterstützende Software sowie die Unified Manager Module, die darauf ausgeführt werden. Darüber hinaus prüft das Upgrade-Skript, ob Systemkonfigurationseinstellungen oder installierte Software vorhanden sind, die mit dem Upgrade in Konflikt stehen könnten. Wenn das Skript Probleme erkennt, müssen Sie diese beheben, bevor Sie Unified Manager aktualisieren. Wenn Sie bereits vor dem Upgrade von Unified Manager Pakete wie *net-snmp* installiert haben, kann die MySQL-Abhängigkeit das Paket während des Upgrades deinstallieren. Sie müssen das Paket manuell erneut installieren, damit Sie es weiterhin verwenden können.

7. Nach Abschluss des Upgrades können Sie in den Meldungen zurückblättern, bis die Meldung mit einer IP-Adresse oder URL für die Unified Manager web UI, dem Wartungsbenutzernamen (umadmin) und dem Standardkennwort angezeigt wird.

   Die Nachricht lautet in etwa wie folgt:

   ```
   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/
```

Nach dem Öffnen der angegebenen IP-Adresse oder URL in einem neuen Fenster eines unterstützten Webbrowsers startet die Unified Manager Web UI; anschließend können Sie sich mit demselben Wartungsbenutzernamen (umadmin) und Passwort anmelden, die Sie zuvor festgelegt haben.

Zusätzliche durchzuführende Schritte für fehlende Pakete

Falls während des Upgrades an Ihrem Standort fehlende Pakete erkannt werden, Ihr System nicht mit dem Internet verbunden ist oder Sie die Red Hat Enterprise Linux Repositories nicht verwenden, können Sie anhand der folgenden Schritte feststellen, ob erforderliche Pakete fehlen, und diese Pakete herunterladen.

> Diese Schritte müssen nach Schritt *5* des Hauptverfahrens durchgeführt werden. Dieses Verfahren aktualisiert Unified Manager, und für das Upgrade sind keine weiteren Schritte erforderlich.

1. Liste der verfügbaren und nicht verfügbaren Pakete:

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

   Die Einträge im Abschnitt “Installing:” sind die Pakete, die im aktuellen Verzeichnis verfügbar sind, und die Einträge im Abschnitt “Installing for dependencies:” sind die Pakete, die auf Ihrem System fehlen.

2. Auf einem anderen System mit Internetzugang kann der folgende Befehl zum Herunterladen der fehlenden Pakete ausgeführt werden.

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

   Die Pakete werden in das als `--downloaddir=` angegebene Verzeichnis heruntergeladen.

   Da das Plug-in “yum-plugin-downloadonly” auf Red Hat Enterprise Linux Systemen nicht immer aktiviert ist, muss möglicherweise die Funktionalität aktiviert werden, um ein Paket herunterzuladen, ohne es zu installieren:

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

3. Als Ziel für die heruntergeladenen Pakete dient das Verzeichnis, in dem Sie das Unified Manager Bundle auf dem Installationssystem entpackt haben.
4. Nach dem Wechsel in dieses Verzeichnis kann der folgende Befehl ausgeführt werden, um die fehlenden Pakete einschließlich ihrer Abhängigkeiten zu installieren.

   ```
   yum install *.rpm
   ```

5. Start des Unified Manager Servers. Dafür werden folgende Befehle verwendet:

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

Damit ist das Upgrade von Unified Manager abgeschlossen. Für den Start der Unified Manager Web-Benutzeroberfläche dient die Eingabe der angegebenen IP-Adresse oder URL in ein neues Fenster eines unterstützten Webbrowsers; die Anmeldung erfolgt anschließend mit demselben Wartungsbenutzernamen

(umadmin) und Passwort, die zuvor festgelegt wurden.

Aktualisierung des Red Hat Enterprise Linux Hostbetriebssystems für Active IQ Unified Manager

Wenn Sie Unified Manager zuvor auf einem Red Hat Enterprise Linux 7.x-System installiert haben und ein Upgrade auf Red Hat Enterprise Linux 8.x durchführen müssen, ist eine der in diesem Thema beschriebenen Vorgehensweisen erforderlich. In beiden Fällen müssen Sie eine Sicherungskopie von Unified Manager auf dem Red Hat Enterprise Linux 7.x-System erstellen und diese anschließend auf dem Red Hat Enterprise Linux 8.x-System wiederherstellen. Unterstützt werden Red Hat Enterprise Linux Versionen von 8.0 bis 8.10.

Der Unterschied zwischen den beiden unten aufgeführten Optionen besteht darin, dass Sie in einem Fall den Unified Manager auf einem neuen 8.x-Server wiederherstellen und im anderen Fall auf demselben Server.

Da für diese Aufgabe eine Sicherung von Unified Manager auf dem Red Hat Enterprise Linux 7.x System erforderlich ist, sollten Sie die Sicherung nur dann erstellen, wenn Sie bereit sind, den gesamten Upgrade-Prozess abzuschließen, damit Unified Manager so kurz wie möglich offline ist. Für den Zeitraum, in dem das Red Hat Enterprise Linux 7.x System heruntergefahren ist und bevor das neue Red Hat Enterprise Linux 8.x gestartet wird, erscheinen in der Unified Manager UI Datenlücken.

Detaillierte Anweisungen für die Sicherungs- und Wiederherstellungsprozesse finden Sie bei Bedarf unter "Verwaltung von Sicherungs- und Wiederherstellungsvorgängen".

Diese Schritte gelten, wenn Sie über ein Ersatzsystem verfügen, auf dem sich die Software Red Hat Enterprise Linux 8.x installieren lässt, sodass Sie die Unified Manager-Wiederherstellung auf diesem System durchführen können, während das Red Hat Enterprise Linux 7.x-System noch verfügbar ist.

1. Installation und Konfiguration eines neuen Servers mit der Software Red Hat Enterprise Linux 8.x.

   Weitere Informationen finden Sie unter "Linux Software und Installationsanforderungen".

2. Auf dem Red Hat Enterprise Linux 8.x-System ist dieselbe Version der Unified Manager Software zu installieren, die auch auf dem vorhandenen Red Hat Enterprise Linux 7.x-System vorhanden ist.

   Weitere Informationen finden Sie unter "Installation von Unified Manager unter Linux".

   Nach Abschluss der Installation erfolgen weder ein Start der UI noch eine Konfiguration von Clustern, Benutzern oder Authentifizierungseinstellungen. Die Sicherungsdatei ergänzt diese Informationen während des Wiederherstellungsprozesses.

3. Auf dem Red Hat Enterprise Linux 7.x-System wird im Administrationsmenü der Web-UI eine Sicherung von Unified Manager erstellt. Anschließend werden die Sicherungsdatei (`.7z` Datei) und der Inhalt des Datenbank-Repository-Verzeichnisses (`/database-dumps-repo` Unterverzeichnisses) an einen externen Speicherort kopiert.
4. Auf dem System Red Hat Enterprise Linux 7.x erfolgt das Herunterfahren von Unified Manager.
5. Auf dem Red Hat Enterprise Linux 8.x-System erfolgt das Kopieren der Sicherungsdatei (`.7z` Datei) vom externen Speicherort nach `/opt/netapp/data/ocum-backup/` sowie der Datenbank-Repository-Dateien in das `/database-dumps-repo` Unterverzeichnis unter dem `/ocum-backup` Verzeichnis.
6. Mit dem folgenden Befehl wird die Unified Manager Datenbank aus der Sicherungsdatei wiederhergestellt:

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

7. Zum Starten der Web-Benutzeroberfläche von Unified Manager wird die IP-Adresse oder URL in den Webbrowser eingegeben, anschließend erfolgt die Anmeldung am System.

Sobald Sie sich vergewissert haben, dass das System ordnungsgemäß funktioniert, können Sie Unified Manager vom Red Hat Enterprise Linux 7.x System entfernen.

Aktualisierung des Host-Betriebssystems auf demselben Server

Die folgenden Schritte gelten, wenn Sie kein Ersatzsystem haben, auf dem Sie die Software Red Hat Enterprise Linux 8.x installieren können.

1. Im Administrationsmenü der Web-UI werden ein Unified Manager Backup erstellt und anschließend die Backup-Datei (`.7z` Datei) sowie der Inhalt des Datenbank-Repository-Verzeichnisses (`/database-dumps-repo` Unterverzeichnis) an einen externen Speicherort kopiert.
2. Entfernung des Red Hat Enterprise Linux 7.x Image aus dem System und vollständiges Löschen des Systems.
3. Die Installation und Konfiguration der Red Hat Enterprise Linux 8.x Software erfolgt auf demselben System.

   Weitere Informationen finden Sie unter "Linux Software und Installationsanforderungen".

4. Auf dem Red Hat Enterprise Linux 8.x-System ist dieselbe Version der Unified Manager Software zu installieren, die auf dem Red Hat Enterprise Linux 7.x-System verwendet wurde.

   Weitere Informationen finden Sie unter "Installation von Unified Manager unter Linux".

   Nach Abschluss der Installation erfolgen weder ein Start der UI noch eine Konfiguration von Clustern, Benutzern oder Authentifizierungseinstellungen. Die Sicherungsdatei ergänzt diese Informationen während des Wiederherstellungsprozesses.

5. Kopieren der Sicherungsdatei (`.7z`Datei) vom externen Speicherort nach `/opt/netapp/data/ocum-backup/` und der Datenbank-Repository-Dateien in das `/database-dumps-repo` Unterverzeichnis unter dem `/ocum-backup` Verzeichnis.
6. Mit dem folgenden Befehl wird die Unified Manager Datenbank aus der Sicherungsdatei wiederhergestellt:

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

7. Zum Starten der Web-Benutzeroberfläche von Unified Manager wird die IP-Adresse oder URL in den Webbrowser eingegeben, anschließend erfolgt die Anmeldung am System.

Aktualisierung von Drittanbieterprodukten nach der Installation von Unified Manager

Aktualisierung von Drittanbieterprodukten nach der Installation von Active IQ Unified Manager

Sie können Drittanbieterprodukte wie JRE aktualisieren, wenn Unified Manager bereits auf Linux-Systemen installiert ist.

Die Unternehmen, die diese Drittanbieterprodukte entwickeln, melden regelmäßig Sicherheitslücken. Sie können die Software nach eigenem Zeitplan auf neuere Versionen aktualisieren.

Upgrade von OpenJDK unter Linux für Active IQ Unified Manager

Sie können auf dem Linux-Server, auf dem Unified Manager installiert ist, auf eine neuere Version von OpenJDK aktualisieren, um Fehlerbehebungen für Sicherheitslücken zu erhalten.

Bevor Sie beginnen

Sie benötigen Root-Rechte für das Linux-System, auf dem Unified Manager installiert ist.

Sie können OpenJDK-Versionen innerhalb einer Versionsfamilie aktualisieren. Beispielsweise können Sie von OpenJDK 11.0.14 auf OpenJDK 11.0.17 aktualisieren, aber nicht direkt von OpenJDK 11 auf OpenJDK 12.

Schritte

1. Sie melden sich auf dem Unified Manager Hostrechner als Root-Benutzer an.
2. Die passende Version von OpenJDK (64-Bit) wird auf das Zielsystem heruntergeladen.
3. Die Unified Manager Services werden beendet:

```
systemctl stop ocieau

systemctl stop ocie
```

4. Auf dem System ist die aktuelle Version von OpenJDK zu installieren.
5. Starten der Unified Manager Services:

```
systemctl start ocie

systemctl start ocieau
```

Active IQ Unified Manager neu starten

Möglicherweise müssen Sie Unified Manager nach der Vornahme von Konfigurationsänderungen neu starten.

Bevor Sie beginnen

Sie benötigen Root-Benutzerzugriff auf den Red Hat Enterprise Linux Server, auf dem Unified Manager installiert ist.

Schritte

1. Die Anmeldung als Root-Benutzer beim Server, auf dem der Unified Manager Service neu gestartet werden soll, ist erforderlich.
2. Das Stoppen des Unified Manager Service und des zugehörigen MySQL Service erfolgt in dieser Reihenfolge:

```
systemctl stop ocieau

systemctl stop ocie

systemctl stop mysqld
```

3. Der Start der MySQL und Unified Manager Services erfolgt in dieser Reihenfolge:

```
systemctl start mysqld

systemctl start ocie

systemctl start ocieau
```

`mysqld` ist ein Daemon-Programm, das zum Starten und Stoppen des MySQL-Servers benötigt wird.

Active IQ Unified Manager entfernen

Unified Manager kann mit einem einzigen Befehl vom Red Hat Enterprise Linux Host gestoppt und deinstalliert werden.

Bevor Sie beginnen

- Sie müssen über Root-Benutzerzugriff auf den Server verfügen, von dem Sie Unified Manager entfernen möchten.
- Security-Enhanced Linux (SELinux) muss auf dem Linux-System deaktiviert sein. Der SELinux-Laufzeitmodus wird mit dem entsprechenden `setenforce 0` Befehl auf „Permissive“ gesetzt.
- Vor dem Entfernen der Software müssen alle Cluster (Datenquellen) vom Unified Manager Server entfernt werden.
- Die zum Zulassen oder Blockieren von MySQL Port 3306 erstellten Firewall-Regeln sollten manuell gelöscht werden. Die Firewall-Regeln werden nicht automatisch gelöscht.

Schritte

1. Die Anmeldung als Root-Benutzer auf dem Server, auf dem Sie Unified Manager entfernen möchten, ist erforderlich.
2. Anhalten und Entfernen von Unified Manager vom Server:

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

   Dieser Schritt entfernt alle zugehörigen NetApp RPM-Pakete. Die erforderlichen Softwaremodule wie Java, MySQL und 7zip werden dabei nicht entfernt.

3. **Optional:** Gegebenenfalls sind die unterstützenden Softwaremodule wie Java, MySQL und 7zip zu entfernen:

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

Nach Abschluss dieses Vorgangs wird die Software entfernt. Alle Daten aus dem `/opt/netapp/data` Verzeichnis werden nach der Deinstallation in den `/opt/netapp/data/BACKUP` Ordner verschoben. Die Deinstallation von Unified Manager entfernt auch die Java- und MySQL-Pakete, es sei denn, diese werden von anderen Applikationen auf dem System benötigt und verwendet. Die MySQL-Daten selbst bleiben jedoch erhalten.

Der benutzerdefinierte Benutzer „umadmin“ und die Wartungsgruppe für Active IQ Unified Manager werden entfernt

Wenn Sie vor der Installation von Unified Manager ein benutzerdefiniertes Home-Verzeichnis erstellt haben, um Ihren eigenen umadmin-Benutzer und Ihr Wartungskonto zu definieren, sollten Sie diese Elemente nach der Deinstallation von Unified Manager entfernen.

Bei der Standarddeinstallation von Unified Manager werden ein benutzerdefinierter Benutzer umadmin und ein Wartungskonto nicht entfernt. Diese Elemente müssen manuell gelöscht werden.

Schritte

1. Für die Anmeldung am Red Hat Enterprise Linux Server ist der Root-Benutzer zu verwenden.
2. Der Benutzer umadmin wird gelöscht:

   ```
   userdel umadmin
   ```

3. Löschen der Wartungsgruppe:

   ```
   groupdel maintenance
   ```

Unified Manager auf Windows-Systemen installieren

Einführung in Active IQ Unified Manager

Informationen zu Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) ermöglicht es Ihnen, den Systemstatus und die Performance Ihrer ONTAP Storage Systeme über eine zentrale Benutzeroberfläche zu überwachen und zu managen. Unified Manager lässt sich auf einem Linux-Server, auf einem Windows-Server oder als virtuelle Appliance auf einem VMware-Host einsetzen.

Nachdem Sie die Installation abgeschlossen und die Cluster hinzugefügt haben, die Sie managen möchten, bietet Unified Manager eine grafische Benutzeroberfläche, die den Kapazitäts-, Verfügbarkeits-, Schutz- und Performance-Status der überwachten Storage Systeme anzeigt.

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Informationen zu den Funktionen des Active IQ Unified Manager Servers

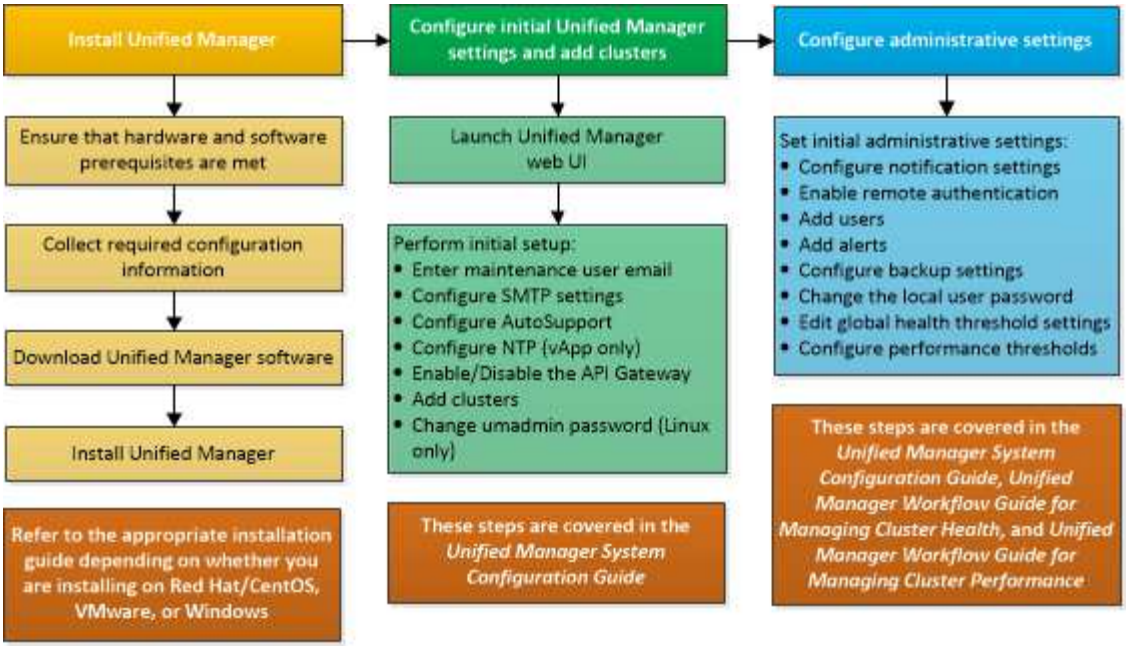
Die Unified Manager Serverinfrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Applikationsserver. Sie bietet Infrastruktur Services wie Erkennung, Überwachung, rollenbasierte Zugriffssteuerung (RBAC), Auditierung und Protokollierung.

Unified Manager sammelt Clusterinformationen, speichert die Daten in der Datenbank und analysiert die Daten, um festzustellen, ob Clusterprobleme vorliegen.

Informationen zur Installationsreihenfolge für Active IQ Unified Manager

Der Installationsablauf beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.

Diese Abschnitte beschreiben die einzelnen Elemente des unten dargestellten Arbeitsablaufs.



Voraussetzungen für die Installation von Unified Manager

Es muss sichergestellt werden, dass der Server die Installationsanforderungen für Active IQ Unified Manager erfüllt.

Vor Beginn des Installationsvorgangs muss der Server, auf dem Sie Unified Manager installieren möchten, die spezifischen Anforderungen an Software, Hardware, CPU und Arbeitsspeicher erfüllen.

NetApp unterstützt keine Änderungen am Code der Unified Manager Applikation. Wenn Sie Sicherheitsmaßnahmen auf dem Unified Manager Server anwenden müssen, sollten Sie diese Änderungen am Betriebssystem vornehmen, auf dem Unified Manager installiert ist.

Weitere Informationen zur Anwendung von Sicherheitsmaßnahmen auf dem Unified Manager Server enthält der Knowledge Base Artikel.

"Unterstützung für Sicherheitsmaßnahmen, die auf Active IQ Unified Manager für Clustered Data ONTAP angewendet werden"

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Informationen zu virtueller Infrastruktur und Hardwareanforderungen für Active IQ Unified Manager

Für die Installation von Unified Manager auf virtueller Infrastruktur oder einem physischen System müssen die Mindestanforderungen an Arbeitsspeicher, CPU und Festplattenspeicher erfüllt sein.

Die folgende Tabelle zeigt die empfohlenen Werte für Arbeitsspeicher, CPU und Festplattenspeicher. Diese Werte wurden so qualifiziert, dass Unified Manager akzeptable Performancewerte erreicht.

Hardwarekonfiguration	Empfohlene Einstellungen
RAM	12 GB
Prozessoren	4 CPUs
CPU-Zykluskapazität	9572 MHz gesamt (Mindestanforderung 9572 MHz)
Freier Speicherplatz	150 GB, wobei die Kapazität wie folgt aufgeteilt ist: • Für das Installationsverzeichnis werden 100 GB Festplattenspeicher benötigt. • 50 GB Speicherplatz für das MySQL-Datenverzeichnis

Unified Manager kann zwar auch auf Systemen mit wenig Arbeitsspeicher installiert werden, die empfohlenen 12 GB RAM gewährleisten jedoch ausreichend Speicher für optimale Performance, sodass das System bei wachsender Konfiguration zusätzliche Cluster und Storage Objekte aufnehmen kann. Sie sollten keine Speichergrenzen für die VM festlegen, auf der Unified Manager eingesetzt wird, und keine Funktionen (z. B. Ballooning) aktivieren, die die Nutzung des dem System zugewiesenen Arbeitsspeichers durch die Software behindern.

Darüber hinaus gibt es eine Begrenzung für die Anzahl der Knoten, die eine einzelne Instanz von Unified Manager überwachen kann, bevor eine zweite Instanz von Unified Manager installiert wird. Empfehlungen zu Knotenlimits, CPU und Arbeitsspeicher sind unter "der Unified Manager Best Practices-Leitfaden" zu finden.

Das Auslagern von Speicherseiten beeinträchtigt die Performance des Systems und der Verwaltungsapplikation. Der Wettbewerb um CPU-Ressourcen, die aufgrund der Gesamtauslastung des Hosts nicht verfügbar sind, kann die Performance beeinträchtigen.

Anforderung für dedizierte Nutzung

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, sollte ausschließlich für Unified Manager vorgesehen sein und nicht mit anderen Applikationen gemeinsam genutzt werden. Andere Applikationen könnten Systemressourcen beanspruchen und die Performance von Unified Manager erheblich beeinträchtigen.

Speicherplatzbedarf für Backups

Wenn Sie die Backup- und Restore-Funktion von Unified Manager verwenden möchten, weisen Sie zusätzliche Kapazität zu, sodass das Verzeichnis oder die Festplatte “data” über 150 GB Speicherplatz verfügt. Ein Backup kann auf ein lokales Ziel oder auf ein Remote-Ziel geschrieben werden. Die Best Practice besteht darin, einen Remote-Speicherort außerhalb des Unified Manager Host-Systems zu bestimmen, der über mindestens 150 GB Speicherplatz verfügt.

Anforderungen an die Host-Konnektivität

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, muss so konfiguriert sein, dass Sie den Hostnamen vom Host selbst aus erfolgreich `ping` können. Bei einer IPv6-Konfiguration sollten Sie prüfen, ob `ping6` zum Hostnamen erfolgreich ist, damit die Installation von Unified Manager erfolgreich verläuft.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Web-UI des Produkts zuzugreifen. Wenn Sie während des Deployment eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie dem Netzwerkhost einen Namen zugewiesen. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollten Sie den Hostnamen über DNS beziehen.

Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen anstelle des vollqualifizierten Domain-Namens (FQDN) oder der IP-Adresse ermöglichen möchten, muss Ihre Netzwerkkonfiguration diesen Kurznamen in einen gültigen FQDN auflösen.

Informationen zu den Windows-Software- und Installationsanforderungen für Active IQ Unified Manager

Für eine erfolgreiche Installation von Unified Manager unter Windows muss das System, auf dem Unified Manager installiert wird, die Softwareanforderungen erfüllen.

Betriebssystemsoftware

Sie können Unified Manager auf den folgenden Windows-Editionen installieren:

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

Unified Manager wird auf 64-Bit-Windows-Betriebssystemen für die folgenden Sprachen unterstützt:

- Englisch
- Japanisch
- Vereinfachtes Chinesisch

Die vollständige und aktuellste Liste der unterstützten Windows-Versionen ist in der Interoperabilitätsmatrix aufgeführt.

"mysupport.netapp.com/matrix"

NetApp unterstützt die Installation von Unified Manager mithilfe von Tools von Drittanbietern wie Microsoft System Center Configuration Manager (SCCM) nicht.

Der Server sollte ausschließlich für den Betrieb von Unified Manager reserviert sein. Es dürfen keine weiteren Anwendungen auf dem Server installiert sein. Möglicherweise ist aufgrund von Unternehmensrichtlinien bereits eine Antivirensoftware auf Ihrem Windows-System installiert. Um Installationsfehler zu vermeiden, sollten Sie diese vor der Installation von Unified Manager deaktivieren.

Software von Drittanbietern

Die folgenden Drittanbieterpakete sind im Unified Manager enthalten. Falls diese Drittanbieterpakete nicht auf Ihrem System installiert sind, installiert Unified Manager sie im Rahmen der Installation.

- Microsoft Visual C++ Redistributable Packages für Visual Studio 2015 Version 14.29.30133.0
- MySQL Community Edition Version 8.4.10
- Python 3.13.3
- OpenJDK Version 17.0.15+6
- 7-zip Version 25.01 oder höher

Ab Unified Manager 9.5 ist OpenJDK im Unified Manager Installationspaket enthalten und wird automatisch installiert. Oracle Java wird ab Unified Manager 9.5 nicht mehr unterstützt.

Wenn MySQL vorinstalliert ist, sollte Folgendes sichergestellt sein:

- Es verwendet den Standardport.
- Die Beispieldatenbanken sind nicht installiert.
- Der Dienstname lautet “MYSQL84”.

Unified Manager wird auf einem WildFly Webserver bereitgestellt. WildFly 27.0.1.Final ist mit Unified Manager gebündelt und konfiguriert.

> Vor der Aktualisierung von Software von Drittanbietern sollte eine laufende Instanz von Unified Manager beendet werden. Nach Abschluss der Installation der Drittanbietersoftware können Sie Unified Manager neu starten.

Installationsanforderungen

- Microsoft .NET 4.5.2 oder höher sollte installiert sein.
- Das `temp` Verzeichnis sollte für das Extrahieren der Installationsdateien mit 2 GB Storage konfiguriert sein. Zur Überprüfung, ob das Verzeichnis erstellt wurde, kann der folgende Befehl auf der Befehlszeilenschnittstelle ausgeführt werden: `echo %temp%`
- Auf dem Windows-Laufwerk sollten 2 GB Speicherplatz zum Zwischenspeichern der Unified Manager MSI-Dateien reserviert sein.
- Der Microsoft Windows Server, auf dem Sie Unified Manager installieren möchten, sollte mit einer vollqualifizierten Domain (FQDN) konfiguriert sein, sodass `ping`Antworten auf den Hostnamen und den FQDN erfolgreich sind.
- Es empfiehlt sich, den Microsoft IIS worldwide web publishing service zu deaktivieren und sicherzustellen, dass die Ports 80 und 443 frei sind.
- Während der Installation sollte die Einstellung „Remote Desktop Session Host“ für “Windows Installer RDS Compatibility” deaktiviert sein.
- Der UDP-Port 514 sollte frei sein und von keinem anderen Dienst verwendet werden.
- Vor der Installation von Unified Manager sollten Sie sämtliche Antiviren-Software auf Ihrem System deaktivieren. Nach Abschluss der Installation müssen Sie die folgenden Pfade manuell vom Virenscan ausschließen:
  - Unified Manager Datenverzeichnis, zum Beispiel `C:\ProgramData\NetApp\OnCommandAppData\`
  - Installationsverzeichnis von Unified Manager, zum Beispiel `\C:\Program Files\NetApp\`
  - MySQL Datenverzeichnis, zum Beispiel, `C:\ProgramData\MySQL\MySQLServerData`

Unterstützte Browser in Active IQ Unified Manager

Der Zugriff auf die Web-Benutzeroberfläche des Unified Manager erfolgt über einen unterstützten Browser.

Die Interoperability Matrix enthält die Liste der unterstützten Browserversionen.

"mysupport.netapp.com/matrix"

Bei allen Browsern gewährleistet das Deaktivieren von Pop-up-Blockern, dass die Softwarefunktionen ordnungsgemäß angezeigt werden.

Wenn Sie Unified Manager für die SAML-Authentifizierung konfigurieren möchten, damit ein Identitätsanbieter (IdP) Benutzer authentifizieren kann, sollten Sie auch die Liste der vom IdP unterstützten Browser überprüfen.

Protokoll- und Portanforderungen für Active IQ Unified Manager verstehen

Die erforderlichen Ports und Protokolle ermöglichen die Kommunikation zwischen dem Unified Manager Server und den verwalteten Storage-Systemen, Servern und anderen Komponenten.

Verbindungen zum Unified Manager Server

Bei typischen Installationen müssen Sie beim Verbinden mit der Unified Manager Web-UI keine Portnummern angeben, da immer Standardports verwendet werden. Da Unified Manager beispielsweise immer versucht, auf seinem Standardport zu laufen, können Sie `https://<host>` anstelle von `https://<host>:443` eingeben.

Der Unified Manager Server verwendet spezifische Protokolle, um auf die folgenden Schnittstellen zuzugreifen:

Schnittstelle	Protokoll	Port	Beschreibung
Unified Manager Web-Benutzeroberfläche	HTTP	80	Dient zum Zugriff auf die Web-UI von Unified Manager; die Weiterleitung zum sicheren Port 443 erfolgt automatisch.
Unified Manager Web-Benutzeroberfläche und Programme, die APIs verwenden	HTTPS	443	Dient dem sicheren Zugriff auf die Unified Manager Weboberfläche oder zum Durchführen von API-Aufrufen; API-Aufrufe können nur über HTTPS erfolgen.
Managementplattform	SSH/SFTP	22	Dient zum Zugriff auf die Managementplattform und zum Abrufen von Support-Bundles.
Linux Befehlszeile	SSH/SFTP	22	Dient zum Zugriff auf die Red Hat Enterprise Linux Befehlszeile und zum Abrufen von Support-Bundles.
Syslog	UDP	514	Dient zum Zugriff auf abonnementbasierte EMS-Nachrichten aus ONTAP Systemen und zum Erstellen von Ereignissen auf Basis dieser Nachrichten.

Schnittstelle	Protokoll	Port	Beschreibung
REST	HTTPS	9443	Wird verwendet, um auf EMS-Ereignisse in Echtzeit über die REST API von authentifizierten ONTAP Systemen zuzugreifen.
MySQL Datenbank	MySQL	3306	Dient zum Aktivieren des Zugriffs von OnCommand Workflow Automation und OnCommand API Services auf Unified Manager.
AMQP-QPID-Broker	TCP/IP	56072	Dient der internen Nachrichtenkommunikation.
AMQP-QPID-Broker	WebSocket über TCP	56080	Dient zum Lauschen an diesem Port auf Nachrichten von ONTAP (cloud agent).
AMQP-QPID-Broker	WebSocket über TCP	56443	Dieser Port wird verwendet, um auf diesem Port auf Nachrichten zu warten, die von ONTAP (cloud agent) empfangen werden.Die Kommunikation über diesen Port unterstützt die durch TLS oder SSL bereitgestellte Verschlüsselung.

Der Standardport für MySQL, 3306, ist bei der Installation von Unified Manager auf Windows Systemen nur auf localhost beschränkt. Nach Abschluss der Installation sollte die Firewall aktiviert werden, um den Zugriff auf den MySQL Port 3306 einzuschränken. Dies hat keine Auswirkungen auf Upgrade-Szenarien, da die vorherige Konfiguration beibehalten wird. Diese Konfiguration kann geändert werden, und die Verbindung kann über die `Control access to MySQL port 3306` Option auf der Managementplattform für andere Hosts verfügbar gemacht werden. Informationen sind unter "Weitere Menüoptionen" verfügbar. Die für die HTTP- und HTTPS-Kommunikation verwendeten Ports (Ports 80 und 443) können über die Unified Manager Managementplattform geändert werden. Weitere Informationen sind unter "Konfigurieren von Active IQ Unified Manager" verfügbar.

Verbindungen vom Unified Manager Server

Ihre Firewall sollte so konfiguriert sein, dass die Ports geöffnet sind, die die Kommunikation zwischen dem Unified Manager Server und verwalteten Storage Systemen, Servern und anderen Komponenten ermöglichen. Wenn ein Port nicht geöffnet ist, schlägt die Kommunikation fehl.

Je nach Ihrer Umgebung können Sie die Ports und Protokolle, die der Unified Manager-Server für die

Verbindung zu bestimmten Zielen verwendet, ändern.

Der Unified Manager Server stellt über die folgenden Protokolle und Ports Verbindungen zu den verwalteten Storage Systemen, Servern und anderen Komponenten her:

Ziel	Protokoll	Port	Beschreibung
Speichersystem	HTTPS	443/TCP	Dient zur Überwachung und zum Managen von Storage Systemen.
Speichersystem	NDMP	10000/TCP	Wird für bestimmte Snapshot-Wiederherstellungsvorgänge verwendet.
AutoSupport Server	HTTPS	443	Dient zum Versenden von AutoSupport Informationen. Für diese Funktion ist ein Internetzugang erforderlich.
Authentifizierungsserver	LDAP	389	Dient zum Stellen von Authentifizierungsanforderungen sowie von Benutzer- und Gruppensuchanfragen.
LDAPS	636	Für die sichere LDAP-Kommunikation verwendet.	Mailserver
SMTP	25	Zum Senden von Benachrichtigungs-E-Mails verwendet.	SNMP-Trap-Sender
SNMPv1 oder SNMPv3	162/UDP	Dient zum Senden von SNMP-Traps für Warnmeldungen.	Server des externen Datenanbieters
TCP	2003	Dient zum Senden von Performance-Daten an einen externen Datenanbieter wie Graphite.	NTP-Server
NTP	123/UDP	Dient zur Synchronisierung der Zeit auf dem Unified Manager Server mit einem externen NTP Zeitserver. (nur VMware Systeme)	AMQP-QPID-Broker
TCP/IP	56072	Dient der internen Nachrichtenkommunikation.	AMQP-QPID-Broker

Ziel	Protokoll	Port	Beschreibung
WebSocket über TCP	56080	Dient zum Lauschen an diesem Port auf Nachrichten von ONTAP (cloud agent).	AMQP-QPID-Broker
WebSocket über TCP	56443	Dieser Port dient zum Empfangen von Nachrichten von ONTAP (Cloud-Agent). Die Kommunikation über diesen Port unterstützt die Verschlüsselung mittels TLS oder SSL.	Syslog

Das Arbeitsblatt in Active IQ Unified Manager wird vervollständigt

Bevor Sie Unified Manager installieren und konfigurieren, sollten Sie spezifische Informationen zu Ihrer Umgebung bereithalten. Sie können diese Informationen im Arbeitsblatt festhalten.

Installationsinformationen für Unified Manager

Die für die Installation von Unified Manager erforderlichen Details.

System, auf dem die Software eingesetzt wird	Ihr Wert
vollqualifizierter Domainname des Hosts	
Host-IP-Adresse	
Netzwerkmaske	
Gateway-IP-Adresse	
Primäre DNS-Adresse	
Sekundäre DNS-Adresse	
Suchdomänen	
Benutzername für Wartungsarbeiten	
Wartungsbenutzerpasswort	

Unified Manager Konfigurationsinformationen

Die Details zur Konfiguration von Unified Manager nach der Installation. Einige Werte sind je nach Ihrer Konfiguration optional.

Einstellung	Ihr Wert
E-Mail-Adresse des Wartungsbenutzers	
SMTP Server Hostname oder IP-Adresse	
SMTP-Benutzername	
SMTP-Passwort	

Einstellung	Ihr Wert
SMTP-Port	25 (Standardwert)
E-Mail-Adresse, von der Benachrichtigungen versendet werden	
Hostname oder IP-Adresse des Authentifizierungsservers	
Name des Active Directory Administrators oder individueller Name für die LDAP-Bindung	
Active Directory Passwort oder LDAP Bind-Passwort	
Basis-individueller Name des Authentifizierungsservers	
URL des Identitätsanbieters (IdP)	
Metadaten des Identitätsanbieters (IdP)	
IP-Adressen von SNMP-Trap-Zielhosts	
SNMP-Port	

Clusterinformationen

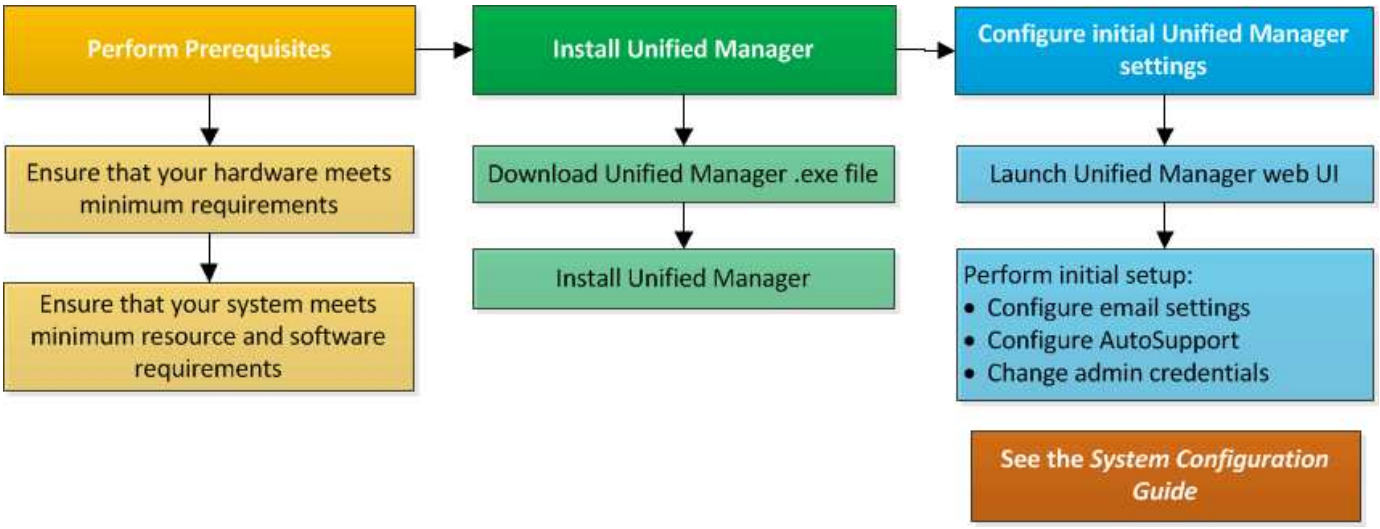
Die Details zu den Storage-Systemen, die Sie mit Unified Manager managen.

Cluster 1 von N	Ihr Wert
Hostname oder Cluster-Management-IP-Adresse	
ONTAP Administrator-Benutzername Dem Administrator muss die Rolle “admin” zugewiesen worden sein.	
ONTAP Administratorpasswort	
Protokoll	HTTPS

Unified Manager Software installieren, aktualisieren und entfernen

Informationen zum Installationsprozess für Active IQ Unified Manager unter Windows

Der Installationsablauf beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.



Unified Manager unter Windows installieren

Installation von Active IQ Unified Manager unter Windows

Sie können Unified Manager installieren, um Storage-Kapazität, Verfügbarkeit, Performance und Schutzprobleme zu überwachen und zu beheben.

Bevor Sie beginnen

- Das System, auf dem Sie Unified Manager installieren möchten, muss die System- und Softwareanforderungen erfüllen.

  Weitere Informationen finden Sie unter "Hardwaresystemanforderungen".

  Weitere Informationen finden Sie unter "Windows Software und Installationsvoraussetzungen".

  Ab Unified Manager 9.5 ist OpenJDK im Installationspaket enthalten und wird automatisch installiert. Oracle Java wird ab Unified Manager 9.5 nicht mehr unterstützt.

- Sie sollten über Windows-Administratorrechte verfügen. Ihr Benutzername darf nicht mit einem Ausrufezeichen “!”. Installation of Unified Manager might fail if the user name of user running the installation begins with “!” beginnen.
- Alle Cluster werden unterstützt, mit Ausnahme von ASA r2 Systemen.
- Sie benötigen einen unterstützten Webbrowser.
- Das Passwort des Unified Manager Wartungsbenutzers sollte zwischen 8 und 20 Zeichen lang sein und Groß- oder Kleinbuchstaben, Ziffern und Sonderzeichen enthalten.
- Die folgenden Sonderzeichen sind in der Passwortzeichenfolge für den Wartungsbenutzer oder den MySQL Root-Benutzer nicht zulässig: " ' ` % , = & < > | ^ \ / ( ) [ ] ;:

  Die folgenden Sonderzeichen sind zulässig: ~ ! @ # $ * - ? . + { }

Schritte

1. Die Anmeldung bei Windows erfolgt mit dem standardmäßigen lokalen Administratorkonto.
2. Anmeldung bei der NetApp Support Site und Navigation zur Download-Seite für Unified Manager:

   "NetApp Support Site"

3. Die gewünschte Version von Unified Manager ist auszuwählen und die Endbenutzer-Lizenzvereinbarung (EULA) ist zu akzeptieren.
4. Sie laden die Unified Manager Windows-Installationsdatei oder die ZIP-Datei in ein Zielverzeichnis auf dem Windows-System herunter.
5. Falls erforderlich, erfolgt zunächst das Entpacken der ZIP-Datei und anschließend der Wechsel in das Verzeichnis, in dem sich die Installationsdatei befindet.
6. Die ausführbare Installationsdatei (.exe) des Unified Manager wird per Rechtsklick als Administrator ausgeführt.

   Unified Manager erkennt fehlende oder vorinstallierte Drittanbieterpakete und listet diese auf. Falls die benötigten Drittanbieterpakete nicht im System installiert sind, installiert Unified Manager sie im Rahmen der Installation.

7. Klicken Sie auf **Weiter**.
8. Für das Erstellen des Wartungsbenutzers werden Benutzername und Passwort benötigt.
9. Im Assistenten für die Datenbankverbindung erfolgt die Eingabe des MySQL Root-Passworts.
10. Über **Ändern** kann ein neuer Speicherort für das Unified Manager Installationsverzeichnis und das MySQL-Datenverzeichnis angegeben werden.

    Wenn Sie das Installationsverzeichnis nicht ändern, wird Unified Manager im Standardinstallationsverzeichnis installiert.

11. Klicken Sie auf **Weiter**.
12. Im Assistenten „Ready to Install Shield“ folgt ein Klick auf **Install**.
13. Nach Abschluss der Installation ist **Fertigstellen** auszuwählen.
14. Wenn auf Ihrem Windows-System eine aktive Antivirensoftware installiert ist, ist nach Abschluss der Installation ein manueller Ausschluss der folgenden Pfade vom Virenscan erforderlich:
    - Unified Manager Datenverzeichnis
    - Unified Manager Installationsverzeichnis
    - MySQL Datenverzeichnis

Bei der Installation entstehen mehrere Verzeichnisse:

- Installationsverzeichnis

  Dies ist das Stammverzeichnis für Unified Manager, das Sie während der Installation angegeben haben. Beispiel: `C:\Program Files\NetApp\`

- MySQL Datenverzeichnis

  Dies ist das Verzeichnis, in dem die MySQL-Datenbanken gespeichert sind, das Sie während der Installation angegeben haben. Beispiel: `C:\ProgramData\MySQL\MySQLServerData\`

- Java Verzeichnis

  Dies ist das Verzeichnis, in dem OpenJDK installiert ist. Beispiel: `C:\Program Files\NetApp\JDK\`

- Anwendungsdatenverzeichnis der Unified Manager Applikation (appDataDir)

Dies ist das Verzeichnis, in dem alle von der Applikation generierten Daten gespeichert werden. Dazu gehören Protokolle, Support Bundles, Backups und alle anderen zusätzlichen Daten. Beispiel: `C:\ProgramData\NetApp\OnCommandAppData\`

Sie können auf die Web UI zugreifen, um die Ersteinrichtung von Unified Manager durchzuführen, wie in der "Konfigurieren von Active IQ Unified Manager" beschrieben.

Unbeaufsichtigte Installation von Active IQ Unified Manager

Sie können Unified Manager ohne Benutzereingriff über die Befehlszeile installieren. Sie können die unbeaufsichtigte Installation abschließen, indem Sie die Parameter als Schlüssel-Wert-Paare übergeben.

Schritte

1. Für die Anmeldung an der Windows-Befehlszeilenschnittstelle wird das standardmäßige lokale Administratorkonto verwendet.
2. Wechseln Sie zu dem Speicherort, an dem Unified Manager installiert werden soll, und wählen Sie eine der folgenden Optionen:

Option	Anweisungen

Wenn Drittanbieterpakete vorinstalliert sind	`ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qn /l*v CompletePathForLogFile"`
	
	Beispiel:
	
	`ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MYSQL\MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qn /l*v C:\install.log"`

Option	Anweisungen

Wenn keine Drittanbieterpakete installiert sind	`ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qr /l*v CompletePathForLogFile"`
	
	Beispiel:
	
	`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"`

Die `/qr` Option aktiviert den stillen Modus mit reduzierter Benutzeroberfläche. Es wird eine einfache Benutzeroberfläche angezeigt, die den Installationsfortschritt anzeigt. Sie werden nicht zur Eingabe aufgefordert. Wenn Drittanbieterpakete wie JRE, MySQL und 7zip nicht vorinstalliert sind, empfiehlt sich die `/qr` Option. Die Installation schlägt fehl, wenn die `/qn` Option auf einem Server verwendet wird, auf dem keine Drittanbieterpakete installiert sind.

Die `/qn` Option aktiviert den stillen Modus ohne Benutzeroberfläche. Während der Installation werden weder eine Benutzeroberfläche noch Details angezeigt. Wenn keine Drittanbieterpakete installiert sind, sollte die `/qn` Option nicht verwendet werden.

3. Die Anmeldung bei der Unified Manager Webbenutzeroberfläche ist über die folgende URL möglich:

   `https://IP address`

Änderung des JBoss Passworts unter Windows in Active IQ Unified Manager

Sie können das während der Installation festgelegte instanzspezifische JBoss Passwort zurücksetzen. Das Zurücksetzen des Passworts ist optional, falls Ihr Standort diese Sicherheitsfunktion benötigt, um die Installationseinstellung von Unified Manager zu überschreiben. Durch diesen Vorgang wird auch das Passwort geändert, das JBoss für den Zugriff auf MySQL verwendet.

Bevor Sie beginnen

- Sie benötigen Windows-Administratorrechte für das System, auf dem Unified Manager installiert ist.
- Sie sollten das Passwort für den MySQL Root-Benutzer haben.
- Sie sollten auf das von NetApp bereitgestellte `password.bat` Skript im Verzeichnis zugreifen können.

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

Schritte

1. Sie melden sich auf dem Unified Manager-Hostrechner als admin-Benutzer an.
2. Beenden der folgenden Unified Manager Services in der Windows Services Managementplattform:
   - NetApp Active IQ Acquisition Service (Ocie-au)
   - NetApp Active IQ Management Server Service (Oncommandsvc)
3. Der Passwortänderungsprozess beginnt mit dem Starten des `password.bat` Skripts:

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

4. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort des MySQL Root-Benutzers ein.
5. Bei der entsprechenden Aufforderung ist das neue JBoss-Benutzerpasswort einzugeben und anschließend zur Bestätigung erneut einzugeben.

   Das Passwort sollte zwischen 8 und 16 Zeichen lang sein und mindestens eine Ziffer, einen Groß- und einen Kleinbuchstaben sowie mindestens eines der folgenden Sonderzeichen enthalten:

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

6. Nach Abschluss des Skripts erfolgt der Start der Unified Manager Services über die Windows Services Managementplattform:
   - NetApp Active IQ Management Server Service (Oncommandsvc)
   - NetApp Active IQ Acquisition Service (Ocie-au)
7. Sobald alle Services gestartet sind, können Sie sich bei der Unified Manager Benutzeroberfläche anmelden.

Der unterstützte Upgrade-Pfad für Versionen von Active IQ Unified Manager ist zu verwenden

Active IQ Unified Manager unterstützt für jede Version einen spezifischen Upgrade-Pfad.

Nicht alle Versionen von Unified Manager unterstützen ein direktes Upgrade auf neuere Versionen. Die Upgrades von Unified Manager sind auf ein N-2-Modell beschränkt. Das bedeutet, dass auf allen Plattformen nur Upgrades auf die nächsten beiden Releases möglich sind. Beispielsweise ist ein Upgrade auf Unified Manager 9.18 nur von Unified Manager 9.14 und 9.16 aus möglich.

Falls Sie eine ältere Version als die unterstützten Versionen verwenden, muss Ihre Unified Manager Instanz zunächst auf eine der unterstützten Versionen und anschließend auf die aktuelle Version aktualisiert werden.

Wenn beispielsweise Unified Manager 9.9 installiert ist und eine Aktualisierung auf Unified Manager 9.14 vorgesehen ist, ist dafür eine Abfolge von Upgrades erforderlich.

Beispielhafter Upgrade-Pfad:

1. Upgrade 9.11 → 9.13
2. Upgrade 9.13 → 9.14
3. Upgrade von 9.13 auf 9.16
4. Upgrade 9.14 oder 9.16 → 9.18

Weitere Informationen zur Upgrade-Pfadmatrix finden Sie in diesem "Knowledge Base Artikel (KB)".

Aktualisierung von Active IQ Unified Manager unter Windows

Sie können Unified Manager 9.14 oder 9.16 auf Version 9.18 aktualisieren, indem Sie die Installationsdatei herunterladen und unter Windows ausführen.

Bevor Sie beginnen

- Das System, auf dem Sie Unified Manager aktualisieren, muss die System- und Softwareanforderungen erfüllen.

  Weitere Informationen finden Sie unter "Hardwaresystemanforderungen".

  Weitere Informationen finden Sie unter "Windows Software und Installationsvoraussetzungen".

  Ab Unified Manager 9.5 ist OpenJDK im Installationspaket enthalten und wird automatisch installiert. Oracle Java wird ab Unified Manager 9.5 nicht mehr unterstützt.

  Vor dem Start des Upgrades muss Microsoft .NET 4.5.2 oder höher auf Ihrem System installiert sein.

- Die MySQL Community Edition wird während des Unified Manager Upgrades automatisch aktualisiert. Wenn die auf Ihrem System installierte MySQL-Version älter als 8.4.10 ist, wird MySQL durch den Unified Manager Upgrade-Prozess automatisch auf 8.4.10 aktualisiert. Ein eigenständiges Upgrade einer älteren MySQL-Version auf 8.4.10 darf nicht durchgeführt werden.
- Alle Cluster werden unterstützt, mit Ausnahme von ASA r2 Systems.
- Sie sollten über Windows-Administratorrechte verfügen. Ihr Benutzername darf nicht mit einem Ausrufezeichen “!”. Installation of Unified Manager might fail if the user name of user running the installation begins with “!” beginnen.
- Sie sollten über gültige Zugangsdaten verfügen, um sich bei der NetApp Support Site anzumelden.
- Um Datenverlust zu vermeiden, sollten Sie vorab eine Sicherungskopie des Unified Manager Rechners erstellt haben, falls während des Upgrades ein Problem auftritt.
- Für die Durchführung des Upgrades sollte ausreichend Festplattenspeicher zur Verfügung stehen.

  Der verfügbare Speicherplatz auf dem Installationslaufwerk muss 2,5 GB größer sein als die Größe des Datenverzeichnisses. Ist nicht genügend freier Speicherplatz vorhanden, wird das Upgrade abgebrochen und eine Fehlermeldung angezeigt, die den zusätzlich benötigten Speicherplatz angibt.

- Während des Upgrades werden Sie möglicherweise aufgefordert zu bestätigen, ob Sie die bisherigen Standardeinstellungen für die Aufbewahrung von Performance-Daten für 13 Monate beibehalten oder auf 6 Monate ändern möchten. Nach der Bestätigung werden die historischen Performance-Daten nach 6 Monaten gelöscht.
- Vor dem Upgrade sollten alle geöffneten Dateien oder Ordner in *<InstallDir>\JDK* und *MySQL Data Directory* geschlossen werden.
- Wenn auf Ihrem Windows-System eine aktive Antivirensoftware installiert ist, kann das Upgrade von Unified Manager fehlschlagen. Vor dem Upgrade von Unified Manager sollte jegliche Virenscanner-Software auf Ihrem System deaktiviert sein.

Während des Upgrade-Prozesses ist Unified Manager nicht verfügbar. Vor dem Upgrade von Unified Manager sollten Sie alle laufenden Vorgänge abschließen.

Wenn Unified Manager mit einer Instanz von OnCommand Workflow Automation gekoppelt ist und für beide

Produkte neue Softwareversionen verfügbar sind, müssen Sie die beiden Produkte trennen und nach den Aktualisierungen eine neue Workflow Automation Verbindung einrichten. Wenn Sie nur eines der Produkte aktualisieren, sollten Sie sich nach der Aktualisierung bei Workflow Automation anmelden und überprüfen, ob Workflow Automation weiterhin Daten aus Unified Manager bezieht.

Schritte

1. Anmeldung bei der NetApp Support Site und Navigation zur Download-Seite für Unified Manager:

   "NetApp Support Site".

2. Die gewünschte Version von Unified Manager ist auszuwählen und die Endbenutzer-Lizenzvereinbarung (EULA) ist zu akzeptieren.
3. Die Unified Manager Windows Installationsdatei oder ZIP-Datei wird in ein Zielverzeichnis auf dem Windows System heruntergeladen. Die ZIP-Datei wird bei Bedarf entpackt, anschließend erfolgt ein Wechsel in das Verzeichnis, in dem sich die Installationsdatei befindet. Die Unified Manager Installationsdatei (.exe) wird per Rechtsklick als Administrator ausgeführt.

   Unified Manager zeigt Ihnen folgende Meldung an:

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

4. Auf **Ja** und anschließend auf **Weiter** klicken.
5. Nach Eingabe des während der Installation festgelegten MySQL84 Root-Passworts erfolgt ein Klick auf **Weiter**.
6. Die Web-Benutzeroberfläche wird in einem neuen Fenster eines unterstützten Webbrowsers geöffnet, und nach der Anmeldung kann die aktualisierte Version von Unified Manager verwendet werden.
7. Wenn auf Ihrem Windows-System eine aktive Antivirensoftware installiert ist, sollten nach Abschluss des Upgrades die folgenden Pfade manuell vom Virenscan ausgeschlossen werden:
   - Unified Manager Datenverzeichnis
   - Unified Manager Installationsverzeichnis
   - MySQL Datenverzeichnis

> Zum Durchführen eines unbeaufsichtigten Upgrades von Unified Manager ist der folgende Befehl auszuführen:
> `ActiveIQUnifiedManager-<version\>.exe /s /v"MYSQL_PASSWORD=<password> /qn /l*v <system_drive>:\install.log"`

Aktualisierung von Drittanbieterprodukten

Upgrade von Drittanbieterprodukten in Active IQ Unified Manager unter Windows

Sie können Drittanbieterprodukte wie JRE in Unified Manager aktualisieren, wenn Unified Manager auf Windows-Systemen installiert ist.

Die Unternehmen, die diese Drittanbieterprodukte entwickeln, melden regelmäßig Sicherheitslücken. Sie können die Software nach eigenem Zeitplan auf neuere Versionen aktualisieren.

OpenJDK unter Windows für Active IQ Unified Manager aktualisieren

Sie können auf dem Windows Server, auf dem Unified Manager installiert ist, auf eine neuere Version von OpenJDK aktualisieren, um Korrekturen für Sicherheitslücken zu erhalten.

Bevor Sie beginnen

Sie benötigen Windows-Administratorrechte für das System, auf dem Unified Manager installiert ist.

Sie können OpenJDK-Versionen innerhalb einer Versionsfamilie aktualisieren. Beispielsweise können Sie von OpenJDK 11.0.16 auf OpenJDK 11.0.18 aktualisieren, aber nicht direkt von OpenJDK 11 auf OpenJDK 12.

Schritte

1. Sie melden sich auf dem Unified Manager-Hostrechner als admin-Benutzer an.
2. Die entsprechende Version von OpenJDK (64-bit) von der OpenJDK Site auf das Zielsystem herunterladen.

   Beispielsweise lässt sich die `jdk-17.0.15_windows-x64_bin.zip`Datei von "die Seite Oracle Java SE 17 Archive Downloads" herunterladen.

   > Zum Herunterladen der Datei benötigen Sie ein Oracle-Konto. Falls Sie noch kein Oracle-Konto besitzen, können Sie unter "die Anmeldeseite des Oracle Kontos" eines erstellen.

3. Beenden der folgenden Unified Manager Services in der Windows Services Managementplattform:
   - NetApp Active IQ Acquisition Service (Ocie-au)
   - NetApp Active IQ Management Server Service (Oncommandsvc)
4. Entpacken der `zip`Datei.
5. Die Verzeichnisse und Dateien aus dem resultierenden `jdk`Verzeichnis werden (z. B. `jdk-11.0.18` an den Speicherort kopiert, an dem Java installiert ist. Beispiel: `C:\Program Files\NetApp\JDK\`
6. Der Start der Unified Manager Services erfolgt über die Windows Services Managementplattform:
   - NetApp Active IQ Management Server Service (Oncommandsvc)
   - NetApp Active IQ Acquisition Service (Ocie-au)

Deinstallation von Drittanbieterprodukten in Active IQ Unified Manager

Nach dem Upgrade von Unified Manager können Sie Drittanbieterprodukte wie Python oder Microsoft Visual C++ 2013 deinstallieren. Dies ist optional.

Python deinstallieren

Schritte

1. In der **Systemsteuerung** erfolgt die Auswahl von **Programme** > **Programme und Funktionen**.
2. Die Auswahl von Python erfolgt aus der Liste der Programme.
3. Die Auswahl erfolgt über **Dieses Programm deinstallieren**. Zu deinstallieren sind alle Python-Versionen außer 3.13.3. Python Version 3.13.3 bleibt erhalten.

Deinstallation von Microsoft Visual C++ 2013

Schritte

1. In der **Systemsteuerung** erfolgt die Auswahl von **Programme** > **Programme und Funktionen**.
2. Die Auswahl in der Liste der Programme fällt auf **Microsoft Visual C++ 2013**.
3. Die Option **Uninstall this program** wird ausgewählt.

Neustart von Active IQ Unified Manager unter Windows

Möglicherweise müssen Sie Unified Manager nach der Vornahme von Konfigurationsänderungen neu starten.

Bevor Sie beginnen

Sie benötigen Windows-Administratorrechte.

Schritte

1. Die Anmeldung bei Windows erfolgt mit dem standardmäßigen lokalen Administratorkonto.
2. Die Unified Manager Services werden beendet:

Aus dem…	Das Stoppen der Services erfolgt in der folgenden Reihenfolge…
Befehlszeile	a. `sc stop ocie-au` b. `sc stop Oncommandsvc`
Microsoft Service Manager	a. NetApp Active IQ Acquisition Service (Ocie-au) b. NetApp Active IQ Management Server Service (Oncommandsvc)

3. Starten der Unified Manager Services:

Aus dem…	Der Start der Services erfolgt in folgender Reihenfolge…
Befehlszeile	a. `sc start Oncommandsvc` b. `sc start ocie-au`
Microsoft Service Manager	a. NetApp Active IQ Management Server Service (Oncommandsvc) b. NetApp Active IQ Acquisition Service (Ocie-au)

Deinstallation von Active IQ Unified Manager

Sie können Unified Manager mithilfe des Assistenten „Programme und Funktionen“ deinstallieren oder eine unbeaufsichtigte Deinstallation über die Befehlszeilenschnittstelle durchführen.

Bevor Sie beginnen

- Sie benötigen Windows-Administratorrechte.

- Vor der Deinstallation der Software müssen alle Cluster (Datenquellen) vom Unified Manager server entfernt werden.
- Die zum Zulassen oder Blockieren von MySQL Port 3306 erstellten Firewall-Regeln sollten manuell gelöscht werden. Die Firewall-Regeln werden nicht automatisch gelöscht.

Schritte

1. Die Deinstallation von Unified Manager kann über eine der folgenden Optionen erfolgen:
   - Wenn Sie Unified Manager über den Assistenten „Programme und Funktionen“ deinstallieren, sind folgende Schritte erforderlich:
     i. Der Pfad lautet **Systemsteuerung** > **Programme und Funktionen**.
     ii. Nach der Auswahl von Active IQ Unified Manager erfolgt ein Klick auf **Deinstallieren**.
   - Wenn Sie Unified Manager über die Befehlszeile deinstallieren, sind die folgenden Schritte erforderlich:
     i. Für die Anmeldung an der Windows-Befehlszeile sind Administratorrechte erforderlich.
     ii. Dann in das Verzeichnis Active IQ Unified Manager wechseln und den folgenden Befehl ausführen:

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

     Wenn die Benutzerkontensteuerung (UAC) auf dem Server aktiviert ist und Sie als Domänenbenutzer angemeldet sind, müssen Sie die Deinstallationsmethode über die Befehlszeile verwenden.

   Unified Manager wurde von Ihrem System deinstalliert.

2. Die folgenden Drittanbieterpakete und -daten, die bei der Deinstallation von Unified Manager nicht entfernt werden, sind zu deinstallieren:
   - Drittanbieterpakete: JRE, MySQL, Microsoft Visual C++ 2015 Redistributable, Python und 7zip
   - Von Unified Manager generierte MySQL Applikationsdaten
   - Anwendungsprotokolle und Inhalte des Applikationsdatenverzeichnisses

Konfigurations- und Verwaltungsaufgaben durchführen

Konfigurieren von Active IQ Unified Manager

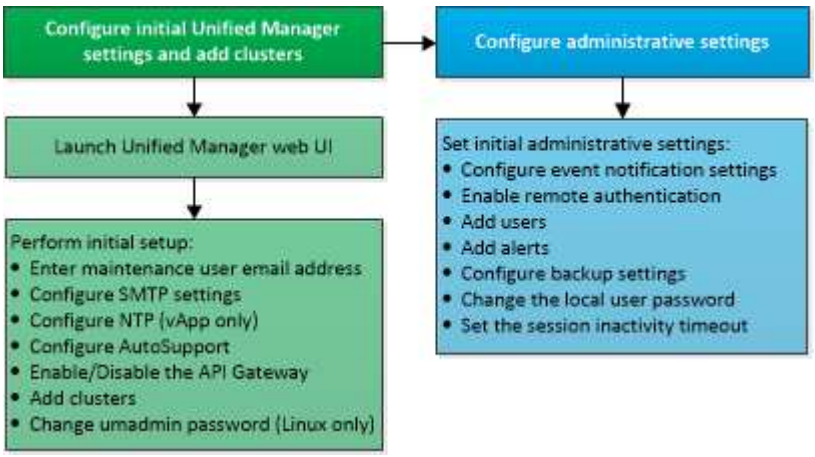
Informationen zur Konfiguration von Active IQ Unified Manager

Nach der Installation von Active IQ Unified Manager (früher OnCommand Unified Manager) müssen Sie die Ersteinrichtung (auch First Experience Wizard genannt) abschließen, um auf die Web-UI zuzugreifen. Anschließend können Sie weitere Konfigurationsaufgaben durchführen, z. B. Cluster hinzufügen, die Remote-Authentifizierung konfigurieren, Benutzer hinzufügen und Warnungen hinzufügen.

Einige der in diesem Handbuch beschriebenen Verfahren sind für die Ersteinrichtung Ihrer Unified Manager Instanz erforderlich. Andere Verfahren sind empfohlene Konfigurationseinstellungen, die für Ihre neue Instanz hilfreich sind oder vor Beginn der regelmäßigen Überwachung Ihrer ONTAP Systeme wissenswert sind.

Informationen zur Konfigurationsreihenfolge in Active IQ Unified Manager

Der Konfigurationsworkflow beschreibt die Aufgaben, die Sie ausführen müssen, bevor Sie Unified Manager verwenden können.



Zugriff auf die Web-Benutzeroberfläche in Active IQ Unified Manager

Nach der Installation von Unified Manager können Sie über die Web-Benutzeroberfläche Unified Manager einrichten, um mit der Überwachung Ihrer ONTAP Systeme zu beginnen.

Bevor Sie beginnen

- Wenn Sie zum ersten Mal auf die Web-Benutzeroberfläche zugreifen, müssen Sie sich als Wartungsbenutzer (bzw. als umadmin-Benutzer bei Linux-Installationen) anmelden.
- Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen anstelle des vollqualifizierten Domainnamens (FQDN) oder der IP-Adresse ermöglichen möchten, muss Ihre Netzwerkkonfiguration diesen Kurznamen in einen gültigen FQDN auflösen.

- Wenn der Server ein selbstsigniertes digitales Zertifikat verwendet, zeigt der Browser möglicherweise eine Warnung an, dass das Zertifikat nicht vertrauenswürdig ist. Sie können entweder das Risiko bestätigen, um den Zugriff fortzusetzen, oder ein von einer Zertifizierungsstelle (CA) signiertes digitales Zertifikat für die Serverauthentifizierung installieren.

Schritte

1. Der Aufruf der Unified Manager Weboberfläche im Browser erfolgt über die URL, die am Ende der Installation angezeigt wird. Die URL ist die IP-Adresse oder die vollqualifizierte Domain (FQDN) des Unified Manager Servers.

   Der Link hat folgendes Format: `https://URL`.

2. Für die Anmeldung bei der Unified Manager Weboberfläche verwenden Sie Ihre Wartungsbenutzerdaten.

   Wenn Sie innerhalb einer Stunde drei aufeinanderfolgende erfolglose Versuche unternehmen, sich bei der Web UI anzumelden, wird Ihr Zugriff auf das System gesperrt, und Sie müssen sich an Ihren Systemadministrator wenden. Dies gilt nur für lokale Benutzer.

Die Ersteinrichtung der Active IQ Unified Manager Weboberfläche wird durchgeführt.

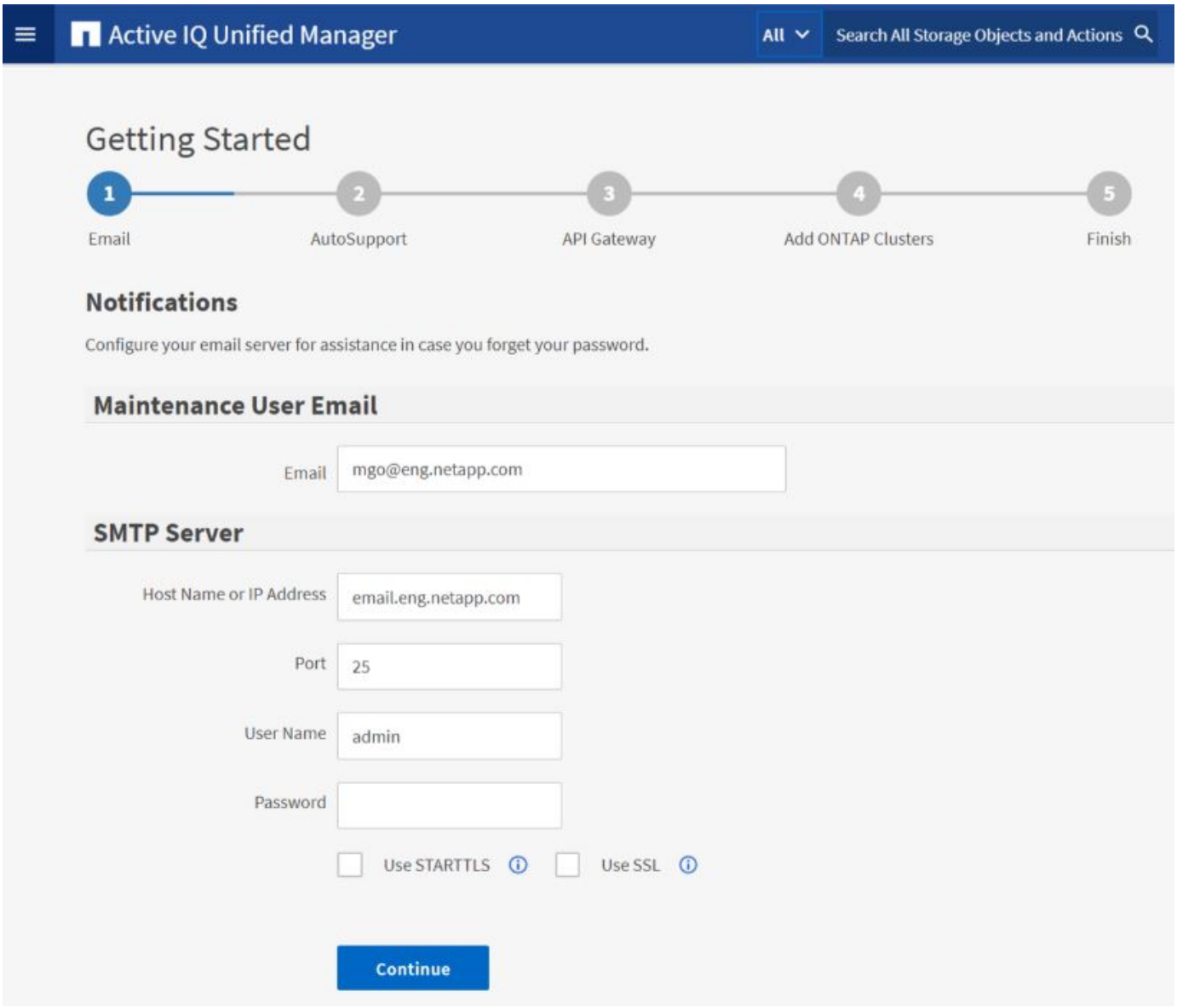
Um Unified Manager nutzen zu können, müssen Sie zunächst die Optionen für die Ersteinrichtung konfigurieren, einschließlich des NTP-Servers, der E-Mail-Adresse des Wartungsbenutzers, des SMTP-Server-Hosts und des Hinzufügens von ONTAP Clustern.

Bevor Sie beginnen

Sie müssen folgende Vorgänge durchgeführt haben:

- Start der Unified Manager Web-UI über die nach der Installation bereitgestellte URL
- Angemeldet mit dem während der Installation erstellten Wartungsbenutzernamen und -passwort (Benutzer umadmin bei Linux-Installationen)

Die Seite „Erste Schritte“ von Active IQ Unified ManagerGetting wird nur angezeigt, wenn Sie erstmals auf die Web-Benutzeroberfläche zugreifen. Die unten stehende Seite stammt aus einer Installation auf VMware.



Wenn Sie eine dieser Optionen später ändern möchten, können Sie Ihre Auswahl im linken Navigationsbereich von Unified Manager unter „Allgemeine Optionen“ treffen. Die NTP-Einstellung gilt nur für VMware-Installationen und kann später über die Unified Manager Managementplattform geändert werden.

Schritte

1. Auf der Seite „Ersteinrichtung“ von Active IQ Unified Manager werden die E-Mail-Adresse des Wartungsbenutzers, der Hostname des SMTP-Servers, alle zusätzlichen SMTP-Optionen sowie der NTP-Server (nur bei VMware Installationen) eingegeben. Danach folgt ein Klick auf **Continue**.

   Wenn Sie die Option **STARTTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Weiter** eine Zertifikatsseite angezeigt. Anschließend können Sie mit den Einstellungen der Ersteinrichtung der Web-Benutzeroberfläche fortfahren, indem Sie die Zertifikatsdetails überprüfen und das Zertifikat akzeptieren.

2. Auf der Seite AutoSupport können Sie **Agree and Continue** auswählen, um das Senden von AutoSupport Nachrichten von Unified Manager an NetAppActive IQ zu aktivieren.

   Wenn ein Proxy für den Internetzugang zum Senden von AutoSupport Inhalten festgelegt werden muss oder wenn AutoSupport deaktiviert werden soll, steht in der Web-Benutzeroberfläche die Option **Allgemein**

> **AutoSupport** zur Verfügung.

3. Auf Red Hat Systemen erfolgt die Änderung des Passworts des Benutzers umadmin von der Standardzeichenfolge “admin” zu einer personalisierten Zeichenfolge.
4. Auf der Seite „API Gateway einrichten“ wählen Sie aus, ob Sie die API Gateway Funktion verwenden möchten, mit der Unified Manager die ONTAP Cluster managen kann, die Sie mithilfe von ONTAP REST APIs überwachen möchten. Anschließend klicken Sie auf **Weiter**.

   Sie können diese Einstellung später in der Web-Benutzeroberfläche unter **Allgemein** > **Funktionseinstellungen** > **API Gateway** aktivieren oder deaktivieren. Weitere Informationen zu den APIs finden Sie unter "Erste Schritte mit Active IQ Unified Manager REST APIs".
5. Die Cluster, die von Unified Manager gemanagt werden sollen, werden hinzugefügt, und anschließend wird auf **Weiter** geklickt. Für jeden Cluster, der gemanagt werden soll, müssen der Hostname oder die Clusterverwaltungs-IP-Adresse (IPv4 oder IPv6) sowie die Anmeldedaten aus Benutzername und Passwort vorliegen - der Benutzer muss über die Rolle “admin” verfügen.

   Dieser Schritt ist optional. Sie können Cluster später in der Web-Benutzeroberfläche unter **Speicherverwaltung** > **Cluster-Einrichtung** hinzufügen.
6. Auf der Übersichtsseite können Sie überprüfen, ob alle Einstellungen korrekt sind, und anschließend auf **Finish** klicken.

Die Seite „Erste Schritte“ wird geschlossen, und die Seite „Unified Manager Dashboard“ wird angezeigt.

Cluster zu Active IQ Unified Manager hinzufügen

Sie können Active IQ Unified Manager einen Cluster hinzufügen, damit Sie den Cluster überwachen können. Dies umfasst die Möglichkeit, Clusterinformationen wie den Systemstatus, die Kapazität, die Performance und die Konfiguration des Clusters abzurufen, damit Sie auftretende Probleme erkennen und beheben können.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie benötigen folgende Informationen:
  - Unified Manager unterstützt lokale ONTAP Cluster, ONTAP Select, Cloud Volumes ONTAP.
  - Hostname oder Cluster-Management-IP-Adresse

    Der Hostname ist der FQDN oder Kurzname, den Unified Manager für die Verbindung zum Cluster verwendet. Der Hostname muss in die Clusterverwaltungs-IP-Adresse aufgelöst werden.

    Die Clusterverwaltungs-IP-Adresse muss die Clusterverwaltungs-LIF der administrativen Storage Virtual Machine (SVM) sein. Wenn eine Knotenverwaltungs-LIF verwendet wird, schlägt der Vorgang fehl.
  - Auf dem Cluster muss mindestens die ONTAP Softwareversion 9.1 oder höher ausgeführt werden.
  - ONTAP Administrator-Benutzername und Passwort

    Dieses Konto muss die Rolle *admin* besitzen, wobei der Anwendungszugriff auf *ontapi*, *amqp*, *console* und *http* festgelegt sein muss.

- Die Portnummer für die Verbindung zum Cluster über das HTTPS-Protokoll (typischerweise Port 443)
- Sie verfügen über die erforderlichen Zertifikate:

  SSL-Zertifikat (HTTPS): Dieses Zertifikat gehört Unified Manager. Bei einer Neuinstallation von Unified Manager wird standardmäßig ein selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt, es für mehr Sicherheit auf ein von einer Zertifizierungsstelle signiertes Zertifikat umzustellen. Wenn das Serverzertifikat abläuft, sollten Sie es neu generieren und Unified Manager neu starten, damit die Services das neue Zertifikat übernehmen. Weitere Informationen zum Regenerieren von SSL-Zertifikaten enthält "Generieren eines HTTPS-Sicherheitszertifikats".

  EMS-Zertifikat: Dieses Zertifikat gehört dem Unified Manager. Es dient zur Authentifizierung von EMS-Benachrichtigungen, die von ONTAP empfangen werden.

  Zertifikate für die gegenseitige TLS-Kommunikation: Werden während der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatbasierte Authentifizierung ist für einen Cluster abhängig von der ONTAP Version aktiviert. Wenn auf einem Cluster eine ONTAP Version niedriger als 9.5 ausgeführt wird, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

  Die zertifikatbasierte Authentifizierung ist für einen Cluster nicht automatisch aktiviert, wenn Sie eine ältere Version von Unified Manager aktualisieren. Sie können sie jedoch aktivieren, indem Sie die Clusterdetails ändern und speichern. Wenn das Zertifikat abläuft, müssen Sie es neu generieren, um das neue Zertifikat einzubinden. Weitere Informationen zum Anzeigen und Neugenerieren des Zertifikats finden Sie unter "Cluster bearbeiten".

  - Über die Web-Benutzeroberfläche lässt sich ein Cluster hinzufügen, und die zertifikatbasierte Authentifizierung wird dabei automatisch aktiviert.
  - Sie können einen Cluster über Unified Manager CLI hinzufügen, die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie einen Cluster mit Unified Manager CLI hinzufügen, müssen Sie den Cluster anschließend über Unified Manager UI bearbeiten. Unter "Unterstützte Unified Manager CLI-Befehle" finden Sie Informationen zum Hinzufügen eines Clusters mit Unified Manager CLI.
  - Wenn die zertifikatbasierte Authentifizierung für einen Cluster aktiviert ist und Sie das Backup von Unified Manager auf einem Server erstellen und es auf einem anderen Unified Manager Server wiederherstellen, bei dem Hostname oder IP-Adresse geändert wurden, kann die Überwachung des Clusters fehlschlagen. Zur Vermeidung dieses Fehlers empfiehlt sich das Bearbeiten und Speichern der Clusterdetails. Weitere Informationen zum Bearbeiten von Clusterdetails finden Sie unter "Cluster bearbeiten".

  +
  Clusterzertifikate: Dieses Zertifikat gehört ONTAP. Sie können keinen Cluster mit einem abgelaufenen Zertifikat zu Unified Manager hinzufügen. Wenn das Zertifikat bereits abgelaufen ist, müssen Sie es vor dem Hinzufügen des Clusters neu generieren. Informationen zur Zertifikatserstellung finden Sie im entsprechenden Knowledge-Base-Artikel "Erneuern eines ONTAP selbstsignierten Zertifikats in der System Manager Benutzeroberfläche".

- Auf dem Unified Manager Server muss ausreichend Speicherplatz vorhanden sein. Ein Cluster kann dem Server nicht hinzugefügt werden, wenn bereits mehr als 90 % des Speicherplatzes im Datenbankverzeichnis belegt sind.

Für eine MetroCluster Konfiguration müssen sowohl die lokalen als auch die Remote-Cluster hinzugefügt werden, und die Cluster müssen korrekt konfiguriert sein.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. Auf der Seite „Cluster Setup“ ist **Add** auszuwählen.
3. Im Dialogfeld „Cluster hinzufügen“ werden die erforderlichen Werte wie Hostname oder IP-Adresse des Clusters, Benutzername, Kennwort und Portnummer angegeben.

   Sie können die Cluster-Management-IP-Adresse von IPv6 auf IPv4 oder von IPv4 auf IPv6 ändern. Die neue IP-Adresse wird nach Abschluss des nächsten Überwachungszyklus im Cluster-Raster und auf der Seite zur Cluster-Konfiguration angezeigt.

4. Anschließend **Absenden** auswählen.
5. Im Dialogfeld „Host autorisieren“ kann über **Zertifikat anzeigen** die Zertifikatsinformation zum Cluster angezeigt werden.
6. Klicken Sie auf **Ja**.

   Nach dem Speichern der Clusterdetails können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für einen Cluster einsehen.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, prüft Unified Manager das Zertifikat nur beim erstmaligen Hinzufügen des Clusters. Unified Manager prüft das Zertifikat nicht bei jedem API-Aufruf an ONTAP.

Nachdem alle Objekte für einen neuen Cluster erkannt wurden, beginnt Unified Manager mit der Erfassung historischer Performance-Daten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Erfassung der Datenkontinuität gesammelt. Diese Funktion stellt Ihnen unmittelbar nach dem Hinzufügen eines Clusters Performance-Informationen für mehr als zwei Wochen zur Verfügung. Nach Abschluss des Erfassungszyklus für die Datenkontinuität werden standardmäßig alle fünf Minuten Echtzeit-Performance-Daten für den Cluster erfasst.

Da die Erfassung von 15 Tagen an Performance-Daten CPU-intensiv ist, empfiehlt es sich, das Hinzufügen neuer Cluster zeitlich zu staffeln, damit Abfragen zur Erfassung der Datenkontinuität nicht gleichzeitig auf zu vielen Clustern ausgeführt werden. Außerdem wird die Erfassung angehalten, wenn Unified Manager während des Zeitraums der Erfassung der Datenkontinuität neu gestartet wird, und in den Performance-Diagrammen sind für den fehlenden Zeitraum Lücken zu sehen.

Wenn Sie eine Fehlermeldung erhalten, dass Sie den Cluster nicht hinzufügen können, ist zu prüfen, ob die Uhren der beiden Systeme nicht synchronisiert sind und ob das Startdatum des Unified Manager HTTPS-Zertifikats nach dem Datum auf dem Cluster liegt. Es muss sichergestellt werden, dass die Uhren mithilfe von NTP oder einem ähnlichen Service synchronisiert sind.

Verwandte Informationen

"Installation eines von einer CA signierten und zurückgegebenen HTTPS-Zertifikats"

Benachrichtigungen konfigurieren

Active IQ Unified Manager wird so konfiguriert, dass Warnmeldungen gesendet werden.

Sie können Unified Manager so konfigurieren, dass Benachrichtigungen gesendet

werden, die Sie über Ereignisse in Ihrer Umgebung informieren. Bevor Benachrichtigungen gesendet werden können, müssen jedoch mehrere weitere Optionen in Unified Manager konfiguriert werden.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Nach dem Deployment von Unified Manager und dem Abschluss der Erstkonfiguration sollte die Konfiguration Ihrer Umgebung so erfolgen, dass beim Empfang von Ereignissen Warnmeldungen ausgelöst und Benachrichtigungs-E-Mails oder SNMP-Traps generiert werden.

Schritte

1. "Konfiguration der Einstellungen für Ereignisbenachrichtigungen".

   Wenn Sie bei bestimmten Ereignissen in Ihrer Umgebung Benachrichtigungen erhalten möchten, müssen Sie einen SMTP-Server konfigurieren und eine E-Mail-Adresse angeben, von der die Benachrichtigungen gesendet werden sollen. Wenn Sie SNMP-Traps verwenden möchten, können Sie diese Option auswählen und die erforderlichen Informationen angeben.

2. "Remote-Authentifizierung aktivieren".

   Wenn Sie möchten, dass entfernte LDAP- oder Active Directory-Benutzer auf die Unified Manager Instanz zugreifen und Warnmeldungen erhalten, müssen Sie die Remote-Authentifizierung aktivieren.

3. "Authentifizierungsserver hinzufügen".

   Sie können Authentifizierungsserver hinzufügen, damit Remote-Benutzer innerhalb des Authentifizierungsservers auf Unified Manager zugreifen können.

4. "Benutzer hinzufügen".

   Sie können verschiedene Arten von lokalen oder Remote-Benutzern hinzufügen und ihnen spezifische Rollen zuweisen. Beim Erstellen einer Warnung weisen Sie einen Benutzer zu, der die Warnungsbenachrichtigungen erhalten soll.

5. "Benachrichtigungen hinzufügen".

   Nachdem Sie die E-Mail-Adresse für den Versand von Benachrichtigungen hinzugefügt, Benutzer zum Empfangen der Benachrichtigungen hinzugefügt, Ihre Netzwerkeinstellungen konfiguriert und die für Ihre Umgebung erforderlichen SMTP- und SNMP-Optionen konfiguriert haben, können Sie Warnungen zuweisen.

Konfiguration der Einstellungen für Ereignisbenachrichtigungen in Active IQ Unified Manager

Sie können Unified Manager so konfigurieren, dass Alarmbenachrichtigungen gesendet werden, sobald ein Ereignis generiert oder einem Benutzer zugewiesen wird. Sie können den SMTP-Server konfigurieren, der zum Senden der Alarmbenachrichtigung verwendet wird, und verschiedene Benachrichtigungsmechanismen festlegen, beispielsweise können Alarmbenachrichtigungen als E-Mails oder SNMP-Traps gesendet werden.

Bevor Sie beginnen

Sie benötigen folgende Informationen:

- E-Mail-Adresse, von der die Alert-Benachrichtigung gesendet wird

  Die E-Mail-Adresse wird im Feld „`From`“ in gesendeten Alarmbenachrichtigungen angezeigt. Falls die E-Mail aus irgendeinem Grund nicht zugestellt werden kann, wird diese E-Mail-Adresse auch als Empfänger für unzustellbare E-Mails verwendet.

- Hostname des SMTP-Servers sowie Benutzername und Passwort für den Zugriff auf den Server
- Hostname oder IP-Adresse des Zielhosts, der den SNMP-Trap empfängt, zusammen mit der SNMP-Version, dem ausgehenden Trap-Port, der Community und anderen erforderlichen SNMP-Konfigurationswerten

  Zur Angabe mehrerer Trap-Ziele dienen Kommas als Trennzeichen zwischen den einzelnen Hosts. In diesem Fall müssen alle anderen SNMP-Einstellungen, wie Version und ausgehender Trap-Port, für alle Hosts in der Liste identisch sein.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benachrichtigungen**.
2. Auf der Seite „Benachrichtigungen“ können Sie die entsprechenden Einstellungen konfigurieren.

   Anmerkungen:

   - Wenn die Absenderadresse mit der Adresse "ActiveIQUnifiedManager@localhost.com" vorausgefüllt ist, sollte sie in eine echte, funktionierende E-Mail-Adresse geändert werden, um sicherzustellen, dass alle E-Mail-Benachrichtigungen erfolgreich zugestellt werden.
   - Kann der Hostname des SMTP-Servers nicht aufgelöst werden, können Sie anstelle des Hostnamens die IP-Adresse (IPv4 oder IPv6) des SMTP-Servers angeben.
3. Auf **Speichern** klicken.
4. Wenn Sie die Option **STARTTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Speichern** eine Zertifikatsseite angezeigt. Zum Speichern der Benachrichtigungseinstellungen ist eine Überprüfung der Zertifikatsdetails sowie die Annahme des Zertifikats erforderlich.

   Über die Schaltfläche **View Certificate Details** können die Zertifikatsdetails angezeigt werden. Wenn das vorhandene Zertifikat abgelaufen ist, kann die Markierung im Kontrollkästchen **Use STARTTLS** oder **Use SSL** entfernt, die Benachrichtigungseinstellungen gespeichert und anschließend das Kontrollkästchen **Use STARTTLS** oder **Use SSL** erneut aktiviert werden, um ein neues Zertifikat anzuzeigen.

Remote Authentifizierung in Active IQ Unified Manager ist aktiviert

Sie können die Remote-Authentifizierung aktivieren, damit der Unified Manager Server mit Ihren Authentifizierungsservern kommunizieren kann. Die Benutzer des Authentifizierungsservers können über die grafische Benutzeroberfläche von Unified Manager auf Storage-Objekte und Daten zugreifen und diese managen.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Der Unified Manager Server muss direkt mit dem Authentifizierungsserver verbunden sein. Sie müssen alle lokalen LDAP-Clients wie SSSD (System Security Services Daemon) oder NSLCD

(Name Service LDAP Caching Daemon) deaktivieren.

Sie können die Remote-Authentifizierung entweder über Open LDAP oder Active Directory aktivieren. Wenn die Remote-Authentifizierung deaktiviert ist, können Remote-Benutzer nicht auf Unified Manager zugreifen.

Die Remote-Authentifizierung wird über LDAP und LDAPS (Secure LDAP) unterstützt. Unified Manager verwendet Port 389 als Standardport für ungesicherte Kommunikation und Port 636 als Standardport für gesicherte Kommunikation.

Das zur Authentifizierung von Benutzern verwendete Zertifikat muss dem X.509-Format entsprechen.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Das Kontrollkästchen für **Remote-Authentifizierung…** aktivieren.
3. Im Feld „Authentifizierungsdienst“ erfolgen die Auswahl des Diensttyps und die Konfiguration des Authentifizierungsdiensts.

Für den Authentifizierungstyp…	Eingabe der folgenden Informationen…
Active Directory	• Name des Administrators des Authentifizierungsservers in einem der folgenden Formate: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (unter Verwendung der entsprechenden LDAP-Notation) • Administratorpasswort • Basis individueller Name (unter Verwendung der entsprechenden LDAP-Notation)
OpenLDAP	• Bind individueller Name (in der entsprechenden LDAP-Notation) • Bind Passwort • Basisindividueller Name

   Wenn die Authentifizierung eines Active Directory-Benutzers lange dauert oder eine Zeitüberschreitung auftritt, benötigt der Authentifizierungsserver wahrscheinlich lange für eine Antwort. Das Deaktivieren der Unterstützung für verschachtelte Gruppen in Unified Manager kann die Authentifizierungszeit verkürzen.

   Wenn für den Authentifizierungsserver die Option „Use Secure Connection“ ausgewählt ist, kommuniziert Unified Manager mit dem Authentifizierungsserver über das Secure Sockets Layer (SSL)-Protokoll.

4. **Optional:** Authentifizierungsserver hinzufügen und die Authentifizierung testen.
5. Auf **Speichern** klicken.

Verschachtelte Gruppen aus der Remote Authentifizierung in Active IQ Unified Manager sind deaktiviert

Wenn die Remote-Authentifizierung aktiviert ist, kann die Authentifizierung verschachtelter Gruppen deaktiviert werden, sodass sich nur einzelne Benutzer und nicht Gruppenmitglieder remote bei Unified Manager authentifizieren können. Verschachtelte Gruppen können deaktiviert werden, wenn die Antwortzeit der Active Directory-Authentifizierung verbessert werden soll.

Bevor Sie beginnen

- Sie benötigen die Rolle des Anwendungsadministrators.
- Die Deaktivierung verschachtelter Gruppen gilt nur bei Verwendung von Active Directory.

Die Deaktivierung der Unterstützung für verschachtelte Gruppen in Unified Manager kann die Authentifizierungszeit verkürzen. Wenn die Unterstützung für verschachtelte Gruppen deaktiviert ist und eine Remote-Gruppe zu Unified Manager hinzugefügt wird, müssen die einzelnen Benutzer Mitglieder der Remote-Gruppe sein, um sich bei Unified Manager zu authentifizieren.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Das Kontrollkästchen für **Verschachtelte Gruppensuche deaktivieren** muss aktiviert sein.
3. Auf **Speichern** klicken.

Einrichtung von Authentifizierungsdiensten in Active IQ Unified Manager

Authentifizierungs Services ermöglichen die Authentifizierung von Remote-Benutzern oder Remote-Gruppen auf einem Authentifizierungsserver, bevor sie Zugriff auf Unified Manager erhalten. Sie können Benutzer mithilfe vordefinierter Authentifizierungs Services (wie Active Directory oder OpenLDAP) authentifizieren oder einen eigenen Authentifizierungsmechanismus konfigurieren.

Bevor Sie beginnen

- Die Remote-Authentifizierung muss aktiviert sein.
- Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Auswahl eines der folgenden Authentifizierung Services:

Wenn Sie auswählen…	Fahren Sie dann wie folgt fort…
Active Directory	a. Administratorname und Passwort eingeben. b. Der Basis-individuelle Name des Authentifizierungsservers ist festzulegen. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann lautet der grundlegende individuelle Name **cn=ou,dc=domain,dc=com**.

Wenn Sie auswählen…	Fahren Sie dann wie folgt fort…
OpenLDAP	a. Sie geben den individuellen Namen für Bind und das Passwort für Bind ein. b. Der Basis-individuelle Name des Authentifizierungsservers ist festzulegen. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann lautet der grundlegende individuelle Name **cn=ou,dc=domain,dc=com**.
Andere	a. Sie geben den individuellen Namen für Bind und das Passwort für Bind ein. b. Der Basis-individuelle Name des Authentifizierungsservers ist festzulegen. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann lautet der grundlegende individuelle Name **cn=ou,dc=domain,dc=com**. c. Die vom Authentifizierungsserver unterstützte LDAP Protokollversion. d. Einzugeben sind Benutzername, Gruppenzugehörigkeit, Benutzergruppe und Mitgliedsattribute.

Wenn Sie den Authentifizierungsdienst ändern möchten, müssen Sie alle vorhandenen Authentifizierungsserver löschen und anschließend neue Authentifizierungsserver hinzufügen.

3. Auf **Speichern** klicken.

Hinzufügen von Authentifizierungsservern zu Active IQ Unified Manager

Sie können Authentifizierungsserver hinzufügen und die Remote-Authentifizierung auf dem Verwaltungsserver aktivieren, sodass Remote-Benutzer innerhalb des Authentifizierungsservers auf Unified Manager zugreifen können.

Bevor Sie beginnen

- Folgende Informationen müssen verfügbar sein:
  - Hostname oder IP-Adresse des Authentifizierungsservers
  - Portnummer des Authentifizierungsservers
- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst so konfiguriert haben, dass der Verwaltungsserver Remote-Benutzer oder -Gruppen im Authentifizierungsserver authentifizieren kann.
- Sie benötigen die Rolle des Anwendungsadministrators.

Wenn der Authentifizierungsserver, den Sie hinzufügen, Teil eines Hochverfügbarkeitspaars (HA-Paar) ist (mit

derselben Datenbank), können Sie auch den Partner-Authentifizierungsserver hinzufügen. Dadurch kann der Verwaltungsserver mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Die Option **Sichere Verbindung verwenden** lässt sich aktivieren oder deaktivieren:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Aktivierung	a. Die Option **Sichere Verbindung verwenden** wird ausgewählt. b. Im Bereich „Authentifizierungsserver“ ist auf **Hinzufügen** zu klicken. c. Im Dialogfeld „Authentifizierungsserver hinzufügen“ ist der Authentifizierungsname oder die IP-Adresse (IPv4 oder IPv6) des Servers einzugeben. d. Im Dialogfeld „Host autorisieren“ auf „Zertifikat anzeigen“ klicken. e. Im Dialogfeld „Zertifikat anzeigen“ können Sie die Zertifikatsinformationen überprüfen und anschließend auf **Schließen** klicken. f. Im Dialogfeld „Host autorisieren“ erfolgt die Auswahl von **Ja**. Wenn Sie die Option **Use Secure Connection authentication** aktivieren, kommuniziert Unified Manager mit dem Authentifizierungsserver und zeigt das Zertifikat an. Unified Manager verwendet standardmäßig Port 636 für sichere Kommunikation und Portnummer 389 für nicht sichere Kommunikation.
Deaktivieren	a. Die Option **Sichere Verbindung verwenden** darf nicht aktiviert sein. b. Im Bereich „Authentifizierungsserver“ ist auf **Hinzufügen** zu klicken. c. Im Dialogfeld „Authentifizierungsserver hinzufügen“ erfolgt die Angabe entweder des Hostnamens oder der IP-Adresse (IPv4 oder IPv6) des Servers sowie der Portdetails. d. Klicken Sie auf **Add**.

Der von Ihnen hinzugefügte Authentifizierungsserver wird im Bereich „Server“ angezeigt.

3. Eine Testauthentifizierung bestätigt, dass Benutzer auf dem hinzugefügten Authentifizierungsserver authentifiziert werden können.

Die Konfiguration der Authentifizierungsserver in Active IQ Unified Manager wird getestet

Sie können die Konfiguration Ihrer Authentifizierungsserver überprüfen, um sicherzustellen, dass der Management Server mit ihnen kommunizieren kann. Sie können die Konfiguration überprüfen, indem Sie auf Ihren Authentifizierungsservern nach einem Remote-Benutzer oder einer Remote-Gruppe suchen und diese mithilfe der konfigurierten Einstellungen authentifizieren.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsservice so konfiguriert haben, dass der Unified Manager Server den Remote-Benutzer oder die Remote-Gruppe authentifizieren kann.
- Sie müssen Ihre Authentifizierungsserver hinzugefügt haben, damit der Managementserver auf diesen Servern nach dem Remote-Benutzer oder der Remote-Gruppe suchen und diese authentifizieren kann.
- Sie benötigen die Rolle des Anwendungsadministrators.

Wenn der Authentifizierungsdienst auf Active Directory eingestellt ist und die Authentifizierung von Remote-Benutzern validiert wird, die zur primären Gruppe des Authentifizierungsservers gehören, werden in den Authentifizierungsergebnissen keine Informationen zur primären Gruppe angezeigt.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Dann folgt ein Klick auf **Authentifizierung testen**.
3. Im Dialogfeld „Test User“ geben Sie den Benutzernamen und das Kennwort des Remote-Benutzers oder den Benutzernamen der Remote-Gruppe an und klicken anschließend auf **Test**.

   Bei der Authentifizierung einer Remote-Gruppe dürfen Sie das Passwort nicht eingeben.

Hinzufügen von Benachrichtigungen in Active IQ Unified Manager

Sie können Warnmeldungen so konfigurieren, dass Sie benachrichtigt werden, wenn ein bestimmtes Ereignis generiert wird. Sie können Warnmeldungen für eine einzelne Ressource, für eine Gruppe von Ressourcen oder für Ereignisse eines bestimmten Typs des Schweregrads konfigurieren. Sie können die Häufigkeit angeben, mit der Sie benachrichtigt werden möchten, und der Warnmeldung ein Skript zuordnen.

Bevor Sie beginnen

- Es müssen Benachrichtigungseinstellungen wie die E-Mail-Adresse des Benutzers, der SMTP-Server und der SNMP-Trap-Host konfiguriert sein, damit der Active IQ Unified Manager Server diese Einstellungen verwenden kann, um Benutzern Benachrichtigungen zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Benachrichtigung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn ein Skript basierend auf dem Ereignis ausgeführt werden soll, muss das Skript zuvor über die Seite „Skripte“ zu Unified Manager hinzugefügt worden sein.
- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Es besteht die Möglichkeit, eine Benachrichtigung direkt auf der Seite „Ereignisdetails“ nach dem Empfang eines Ereignisses zu erstellen, zusätzlich zur Erstellung einer Benachrichtigung über die Seite „Benachrichtigungseinrichtung“, wie hier beschrieben.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite „Benachrichtigungseinstellungen“ erfolgt ein Klick auf **Hinzufügen**.
3. Im Dialogfeld „Warnung hinzufügen“ wird auf **Name** geklickt und ein Name sowie eine Beschreibung für die Warnung eingegeben.
4. **Ressourcen** auswählen und die Ressourcen bestimmen, die in die Benachrichtigung einbezogen oder von ihr ausgeschlossen werden.

   Ein Filter kann festgelegt werden, indem im Feld **Name enthält** ein Text-String angegeben wird, um eine Gruppe von Ressourcen auszuwählen. Basierend auf dem angegebenen Text-String werden in der Liste der verfügbaren Ressourcen nur die Ressourcen angezeigt, die der Filterregel entsprechen. Der angegebene Text-String ist Groß-/Kleinschreibungs-empfindlich.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschluss- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschlussregel, und die Warnung wird für Ereignisse, die sich auf die ausgeschlossene Ressource beziehen, nicht generiert.

5. Auf **Ereignisse** klicken und die Ereignisse anhand des Ereignisnamens oder des Typs des Schweregrads auswählen, für die ein Alarm ausgelöst werden soll.

   Um mehr als ein Ereignis auszuwählen, die Strg-Taste gedrückt halten, während die Auswahl getroffen wird.

6. Auf **Aktionen** klicken, die Benutzer auswählen, die benachrichtigt werden sollen, die Benachrichtigungshäufigkeit festlegen, auswählen, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und ein Skript zuweisen, das ausgeführt wird, wenn eine Warnung generiert wird.

   Wenn die für den Benutzer angegebene E-Mail-Adresse geändert und die Benachrichtigung erneut zum Bearbeiten geöffnet wird, bleibt das Namensfeld leer, da die geänderte E-Mail-Adresse nicht mehr dem zuvor ausgewählten Benutzer zugeordnet ist. Auch wenn die E-Mail-Adresse des ausgewählten Benutzers auf der Seite „Benutzer“ geändert wurde, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

   Alternativ ist es möglich, die Benutzer auch über SNMP-Traps zu benachrichtigen.

7. Auf **Speichern** klicken.

Beispiel für das Hinzufügen einer Benachrichtigung

Dieses Beispiel zeigt, wie eine Benachrichtigung erstellt wird, die die folgenden Anforderungen erfüllt:

- Name der Warnung: HealthTest
- Ressourcen: umfasst alle Volumes, deren Name “abc” enthält, und schließt alle Volumes aus, deren Name “xyz” enthält
- Ereignisse: umfasst alle kritischen Gesundheitsereignisse
- Aktionen: umfasst "sample@domain.com", ein “Test”-Skript, und der Benutzer muss alle 15 Minuten benachrichtigt werden

Im Dialogfeld „Warnung hinzufügen“ sind die folgenden Schritte auszuführen:

Schritte

1. Unter **Name** erfolgt die Eingabe von **HealthTest** in das Feld **Alarmname**.
2. **Ressourcen** auswählen und im Tab „Einschließen“ **Volumes** aus der Dropdown-Liste wählen.
   a. Durch Eingabe von **abc** in das Feld **Name enthält** werden die Volumes angezeigt, deren Name “abc” enthält.
   b. **<<All Volumes whose name contains 'abc'>>** im Bereich „Verfügbare Ressourcen“ auswählen und in den Bereich „Ausgewählte Ressourcen“ verschieben.
   c. Nach Auswahl von **Exclude** erfolgt die Eingabe von **xyz** in das Feld **Name contains**; anschließend wird **Add** ausgewählt.
3. Auf **Ereignisse** klicken und im Feld **Ereignisschweregrad Kritisch** auswählen.
4. Im Bereich „Übereinstimmende Ereignisse“ **Alle kritischen Ereignisse** auswählen und in den Bereich „Ausgewählte Ereignisse“ verschieben.
5. Unter **Actions** wird im Feld **Alert these users sample@domain.com** eingetragen.
6. **Alle 15 Minuten erinnern** benachrichtigt den Benutzer alle 15 Minuten.

   Sie können eine Benachrichtigung so konfigurieren, dass sie über einen festgelegten Zeitraum wiederholt an die Empfänger gesendet wird. Es sollte der Zeitpunkt festgelegt werden, ab dem die Ereignisbenachrichtigung für die Benachrichtigung aktiv ist.
7. Im Menü „Auszuführendes Skript auswählen“ das Skript **Test** auswählen.
8. Auf **Speichern** klicken.

Das lokale Benutzerkennwort in Active IQ Unified Manager kann geändert werden.

Sie können Ihr Passwort für die Anmeldung als lokaler Benutzer ändern, um potenziellen Sicherheitsrisiken vorzubeugen.

Bevor Sie beginnen

Sie müssen als lokaler Benutzer angemeldet sein.

Die Passwörter für den Wartungsbenutzer und für Remote-Benutzer können mit diesen Schritten nicht geändert werden. Die Änderung eines Remote-Benutzerpassworts erfolgt über Ihren Passwortadministrator. Informationen zum Ändern des Passworts des Wartungsbenutzers enthält "Verwenden der Managementplattform".

Schritte

1. Sie sind bei Unified Manager angemeldet.
2. In der oberen Menüleiste erfolgt die Auswahl zunächst über das Benutzersymbol und anschließend über **Passwort ändern**.

   Bei Remote-Benutzern ist die Option **Passwort ändern** nicht verfügbar.
3. Im Dialogfeld „Passwort ändern“ erfolgt die Eingabe des aktuellen Passworts und des neuen Passworts.
4. Auf **Speichern** klicken.

Wenn Unified Manager in einer Hochverfügbarkeitskonfiguration eingerichtet ist, müssen Sie das Passwort auf

dem zweiten Knoten des Setups ändern. Beide Instanzen müssen dasselbe Passwort verwenden.

Die Zeitüberschreitung bei Sitzungsinaktivität in Active IQ Unified Manager festlegen

Sie können für Unified Manager den Wert für die Inaktivitäts-Zeitüberschreitung festlegen, sodass die Sitzung nach einer bestimmten Zeit der Inaktivität automatisch beendet wird. Standardmäßig ist die Zeitüberschreitung auf 4.320 Minuten (72 Stunden) festgelegt.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Diese Einstellung betrifft alle angemeldeten Benutzersitzungen.

Diese Option ist nicht verfügbar, wenn Sie die Security Assertion Markup Language (SAML) Authentifizierung aktiviert haben.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Funktionseinstellungen**.
2. Auf der Seite **Feature Settings** können Sie die Inaktivitäts-Zeitüberschreitung festlegen, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Es ist keine Zeitüberschreitung festgelegt, sodass die Sitzung niemals automatisch geschlossen wird.	Im Bereich **Inactivity Timeout** den Schieberegler nach links (aus) verschieben und auf **Apply** klicken.
Festlegen einer bestimmten Anzahl von Minuten als Wert für die Zeitüberschreitung	Im Bereich **Inactivity Timeout** den Schieberegler nach rechts (Ein) bewegen, den Wert für die Inaktivitäts-Zeitüberschreitung in Minuten angeben und **Apply** auswählen.

Die Zeitüberschreitung der Sitzung kann über die CLI in Active IQ Unified Manager festgelegt werden.

Über die Befehlszeilenschnittstelle (CLI) kann für Unified Manager ein maximaler Wert für die Sitzungs-Zeitüberschreitung festgelegt werden, sodass die Sitzung nach einer bestimmten Zeit automatisch beendet wird. Standardmäßig ist die Sitzungs-Zeitüberschreitung auf den Maximalwert von 4.320 Minuten (72 Stunden) eingestellt. Das bedeutet, dass Ihre Sitzung nach 72 Stunden automatisch endet, selbst wenn Sie angemeldet sind und Unified Manager aktiv nutzen.

Über diese Aufgabe

Sie benötigen die Rolle des Anwendungsadministrators.

Die Einstellung für die Zeitüberschreitung von Sitzungen betrifft alle angemeldeten Benutzersitzungen.

Schritte

1. Die Anmeldung bei der Unified Manager CLI erfolgt durch Eingabe des `um cli login` Befehls. Für die Authentifizierung werden ein gültiger Benutzername und ein gültiges Passwort benötigt.

2. Der `um option set max.session.timeout.value=<in mins>` Befehl dient zum Ändern des Werts der Sitzungs-Zeitüberschreitung.

Der Hostname von Unified Manager kann geändert werden

Der Hostname der virtuellen Active IQ Unified Manager Appliance kann geändert werden.

Dem Netzwerkhost wird beim ersten Deployment der virtuellen Unified Manager Appliance ein Name zugewiesen. Sie können den Hostnamen nach dem Deployment ändern. Wenn Sie den Hostnamen ändern, müssen Sie auch das HTTPS-Zertifikat neu generieren.

Bevor Sie beginnen

Um diese Aufgaben ausführen zu können, müssen Sie bei Unified Manager als Wartungsbenutzer angemeldet sein oder Ihnen muss die Rolle Application Administrator zugewiesen sein.

Der Hostname (oder die Host-IP-Adresse) kann für den Zugriff auf die Unified Manager Web-Benutzeroberfläche verwendet werden. Wenn während des Deployment eine statisch IP-Adresse für Ihr Netzwerk konfiguriert wurde, wurde dem Netzwerkhost ein Name zugewiesen. Wenn das Netzwerk mit DHCP konfiguriert wurde, sollte der Hostname aus dem DNS übernommen werden. Wenn DHCP oder DNS nicht ordnungsgemäß konfiguriert sind, wird der Hostname “Unified Manager” automatisch zugewiesen und dem Sicherheitszertifikat zugeordnet.

Unabhängig davon, wie der Hostname zugewiesen wurde, müssen Sie ein neues Sicherheitszertifikat generieren, wenn Sie den Hostnamen ändern und beabsichtigen, mit dem neuen Hostnamen auf die Unified Manager web UI zuzugreifen.

Wenn Sie über die IP-Adresse des Servers anstatt über den Hostnamen auf die Web-Oberfläche zugreifen, müssen Sie kein neues Zertifikat generieren, wenn Sie den Hostnamen ändern. Es empfiehlt sich jedoch, das Zertifikat zu aktualisieren, sodass der Hostname im Zertifikat mit dem tatsächlichen Hostnamen übereinstimmt.

Wenn Sie den Hostnamen in Unified Manager ändern, müssen Sie den Hostnamen in OnCommand Workflow Automation (WFA) manuell aktualisieren. Der Hostname wird in WFA nicht automatisch aktualisiert.

Das neue Zertifikat tritt erst nach einem Neustart der virtuellen Maschine des Unified Manager in Kraft.

Schritte

1. Generierung eines HTTPS-Sicherheitszertifikats

   Wenn Sie den neuen Hostnamen für den Zugriff auf die Unified Manager Weboberfläche verwenden möchten, müssen Sie das HTTPS-Zertifikat neu generieren, um es dem neuen Hostnamen zuzuordnen.

2. Neustart der virtuellen Maschine von Unified Manager

   Nach der Neugenerierung des HTTPS-Zertifikats ist ein Neustart der virtuellen Maschine von Unified Manager erforderlich.

In Active IQ Unified Manager kann ein HTTPS-Sicherheitszertifikat generiert werden

Wenn Active IQ Unified Manager zum ersten Mal installiert wird, wird ein Standard HTTPS Zertifikat installiert. Es kann ein neues HTTPS Sicherheitszertifikat generiert werden, das das vorhandene Zertifikat ersetzt.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Es kann verschiedene Gründe für die Neugenerierung des Zertifikats geben, beispielsweise wenn Sie bessere Werte für den individuellen Namen (DN) wünschen, eine höhere Schlüssellänge oder eine längere Gültigkeitsdauer benötigen oder wenn das aktuelle Zertifikat abgelaufen ist.

Wenn Sie keinen Zugriff auf die Unified Manager Web-UI haben, können Sie das HTTPS-Zertifikat über die Managementplattform mit denselben Werten neu generieren. Beim Neugenerieren von Zertifikaten können Sie die Schlüssellänge und die Gültigkeitsdauer des Schlüssels festlegen. Wenn Sie in der Managementplattform die Option `Reset Server Certificate` verwenden, wird ein neues HTTPS-Zertifikat mit einer Gültigkeit von 397 Tagen erstellt. Dieses Zertifikat verfügt über einen RSA-Schlüssel mit einer Länge von 2048 Bit.

Schritte

1. Im linken Navigationsbereich auf **General** > **HTTPS Certificate** klicken.
2. **Regenerate HTTPS Certificate** auswählen.

   Das Dialogfeld „HTTPS-Zertifikat neu generieren“ wird angezeigt.

3. Je nachdem, wie das Zertifikat generiert werden soll, ist eine der folgenden Optionen auszuwählen:

Wenn Sie möchten…	Folgendes ist zu tun…
Neugenerierung des Zertifikats mit den aktuellen Werten	Die Option **Neu generieren mit aktuellen Zertifikatsattributen** auswählen.

Wenn Sie möchten…	Folgendes ist zu tun…
Erzeugen des Zertifikats mit verschiedenen Werten	Auswahl der Option **Aktuelle Zertifikatsattribute aktualisieren**. Die Felder „Allgemeiner Name“ und „Alternative Namen“ verwenden die Werte des vorhandenen Zertifikats, wenn Sie keine neuen Werte eingeben. Der „`Common Name`“ sollte auf den FQDN des Hosts gesetzt werden. Die anderen Felder erfordern keine Werte, Sie können jedoch Werte eingeben, z. B. für E-MAIL, COMPANY, DEPARTMENT, Stadt, Bundesland und Land, wenn diese Werte im Zertifikat eingetragen werden sollen. Außerdem kann aus der verfügbaren KEY SIZE (der Schlüsselalgorithmus ist „`RSA`“) und dem VALIDITY PERIOD ausgewählt werden. • Die zulässigen Werte für die Schlüssellänge sind `2048`, `3072` und `4096`. • Die Gültigkeitsdauer beträgt mindestens 1 Tag und maximal 36500 Tage. Obwohl eine Gültigkeitsdauer von 36.500 Tagen zulässig ist, empfiehlt sich eine Gültigkeitsdauer von maximal 397 Tagen bzw. 13 Monaten. Wenn Sie eine Gültigkeitsdauer von mehr als 397 Tagen wählen und planen, einen CSR für dieses Zertifikat zu exportieren und von einer bekannten CA signieren zu lassen, beträgt die Gültigkeit des von der CA zurückgegebenen signierten Zertifikats nur 397 Tage. • Sie können das Kontrollkästchen „Lokale Identifikationsinformationen ausschließen (z. B. localhost)“ aktivieren, wenn Sie die lokalen Identifikationsinformationen aus dem Feld „Alternative Namen“ im Zertifikat entfernen möchten. Wenn dieses Kontrollkästchen aktiviert ist, wird im Feld „Alternative Namen“ nur das verwendet, was Sie in das Feld eingeben. Wenn das Feld leer bleibt, enthält das resultierende Zertifikat überhaupt kein Feld

4. Mit **Ja** kann das Zertifikat neu generiert werden.
5. Damit das neue Zertifikat wirksam wird, ist ein Neustart des Unified Manager Server erforderlich.
6. Die neuen Zertifikatsinformationen können durch Anzeige des HTTPS-Zertifikats überprüft werden.

Starten Sie die virtuelle Maschine Active IQ Unified Manager neu.

Sie können die virtuelle Maschine über die Managementplattform von Unified Manager neu starten. Ein Neustart ist erforderlich, nachdem ein neues Sicherheitszertifikat generiert wurde oder wenn ein Problem mit der virtuellen Maschine auftritt.

Bevor Sie beginnen

Die virtuelle Appliance ist eingeschaltet.

Sie sind bei der Managementplattform für die Wartung als Wartungsbenutzer angemeldet.

Sie können die virtuelle Maschine auch von vSphere aus mit der Option **Restart Guest** neu starten. Weitere Informationen finden Sie in der VMware-Dokumentation.

Schritte

1. Auf die Wartungskonsole zugreifen.
2. Für den Neustart der virtuellen Maschine ist **System Configuration** > **Reboot Virtual Machine** auszuwählen.

Ändern des Hostnamens von Active IQ Unified Manager auf Linux Systemen

Gegebenenfalls möchten Sie den Hostnamen des Red Hat Enterprise Linux Rechners ändern, auf dem Unified Manager installiert ist. Beispielsweise können Sie den Host umbenennen, um Ihre Unified Manager Server beim Auflisten Ihrer Linux Rechner leichter nach Typ, Arbeitsgruppe oder überwachter Clustergruppe zu identifizieren.

Bevor Sie beginnen

Sie benötigen Zugriff als Root-Benutzer auf das Linux-System, auf dem Unified Manager installiert ist.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Web UI von Unified Manager zuzugreifen. Wenn Sie während des Deployment eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie dem Netzwerkhost einen Namen zugewiesen. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollte der Hostname vom DNS-Server übernommen werden.

Unabhängig davon, wie der Hostname zugewiesen wurde, müssen Sie ein neues Sicherheitszertifikat generieren, wenn Sie den Hostnamen ändern und beabsichtigen, den neuen Hostnamen für den Zugriff auf die Unified Manager Weboberfläche zu verwenden.

Wenn Sie über die IP-Adresse des Servers anstatt über den Hostnamen auf die Web-Oberfläche zugreifen, müssen Sie bei einer Änderung des Hostnamens kein neues Zertifikat generieren. Es empfiehlt sich jedoch, das Zertifikat zu aktualisieren, sodass der Hostname im Zertifikat mit dem tatsächlichen Hostnamen übereinstimmt. Das neue Zertifikat wird erst nach einem Neustart des Linux-Rechners wirksam.

Wenn Sie den Hostnamen in Unified Manager ändern, müssen Sie den Hostnamen in OnCommand Workflow Automation (WFA) manuell aktualisieren. Der Hostname wird in WFA nicht automatisch aktualisiert.

Schritte

1. Sie melden sich als Root-Benutzer bei dem Unified Manager System an, das Sie ändern möchten.
2. Zum Beenden der Unified Manager Software und der zugehörigen MySQL Software ist der folgende Befehl einzugeben:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Die Änderung des Hostnamens erfolgt mit dem Linux `hostnamectl` Befehl:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Das HTTPS-Zertifikat für den Server neu generieren:

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

5. Neustart des Netzwerkservice:

   ```
   systemctl restart NetworkManager.service
   ```

6. Nach dem Neustart des Dienstes sollte geprüft werden, ob der neue Hostname sich selbst anpingen kann:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Dieser Befehl sollte dieselbe IP-Adresse zurückgeben, die zuvor für den ursprünglichen Hostnamen festgelegt wurde.

7. Nachdem Sie die Änderung Ihres Hostnamens abgeschlossen und überprüft haben, muss Unified Manager mit dem folgenden Befehl neu gestartet werden:

   ```
   systemctl start mysqld ocie ocieau
   ```

Aktivieren und Deaktivieren der richtlinienbasierten Speicherverwaltung in Active IQ Unified Manager

Ab Unified Manager 9.7 können Sie Storage Workloads (Volumes und LUNs) auf Ihren ONTAP Clustern provisionieren und diese Workloads anhand zugewiesener Performance Service Levels managen. Diese Funktionalität ähnelt der Erstellung von Workloads in ONTAP System Manager und dem Anhängen von QoS Richtlinien, bei der Verwendung von Unified Manager können Sie Workloads jedoch clusterübergreifend auf allen Clustern provisionieren und managen, die von Ihrer Unified Manager Instanz überwacht werden.

Sie benötigen die Rolle des Anwendungsadministrators.

Diese Option ist standardmäßig aktiviert, kann jedoch deaktiviert werden, wenn Sie Workloads nicht mit Unified Manager provisionieren und managen möchten.

Wenn diese Option aktiviert ist, stehen viele neue Elemente in der Benutzeroberfläche zur Verfügung:

Neue Inhalte	Standort
Eine Seite zum Provisionieren neuer Workloads	Verfügbar unter **Allgemeine Aufgaben** > **Provisionierung**
Eine Seite zum Erstellen von Performance Service Level-Richtlinien	Verfügbar unter **Einstellungen** > **Richtlinien** > **Performance Service Levels**
Eine Seite zum Erstellen von Performance Storage Effizienzrichtlinien	Verfügbar unter **Einstellungen** > **Richtlinien** > **Speichereffizienz**
Bereiche, die Ihre aktuelle Workload Performance und Workload IOPS beschreiben	Im Dashboard verfügbar

Weitere Informationen zu diesen Seiten und dieser Funktionalität finden Sie in der Online-Hilfe des Produkts.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Funktionseinstellungen**.
2. Auf der Seite **Funktionseinstellungen** können Sie die richtlinienbasierte Storage-Verwaltung deaktivieren oder aktivieren, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Deaktivierung der richtlinienbasierten Storage-Verwaltung	Im Bedienfeld **Policy-based storage management** den Schieberegler nach links verschieben.
Aktivierung der richtlinienbasierten Storage-Verwaltung	Im Bedienfeld **Policy-based storage management** lässt sich der Schieberegler nach rechts verschieben.

Active IQ Unified Manager Sicherung konfigurieren

Die Backup-Funktion in Unified Manager lässt sich durch eine Reihe von Konfigurationsschritten auf den Hostsystemen und über die Managementplattform konfigurieren.

Informationen zu den Konfigurationsschritten finden Sie unter "Verwaltung von Sicherungs- und Wiederherstellungsvorgängen".

Funktionseinstellungen managen

Informationen zu Funktionseinstellungen in Active IQ Unified Manager

Die Seite „Funktionseinstellungen“ ermöglicht das Aktivieren und Deaktivieren bestimmter Funktionen in Active IQ Unified Manager. Dazu gehören das Erstellen und Managen von Storage-Objekten auf der Grundlage von Richtlinien, das Aktivieren von API Gateway und Login Banner, das Hochladen von Skripten zum Managen von Warnungen, die Zeitüberschreitung einer Web UI-Sitzung auf der Grundlage der Inaktivitätsdauer sowie das Deaktivieren des Empfangs von Plattformereignissen von Active IQ.

Die Seite „Feature Settings“ ist nur für Benutzer mit der Rolle „Application Administrator“

verfügbar.

Weitere Informationen zu Scripts Upload sind unter "Hochladen von Skripten aktivieren und deaktivieren" verfügbar.

Die richtlinienbasierte Speicherverwaltung in Active IQ Unified Manager kann aktiviert werden

Die Option **Richtlinienbasierte Storage Verwaltung** ermöglicht das Management von Storage auf Grundlage von Service Level Objectives (SLOs). Diese Option ist standardmäßig aktiviert.

Nach der Aktivierung dieser Funktion können Sie Storage Workloads auf den ONTAP Clustern provisionieren, die Ihrer Active IQ Unified Manager Instanz hinzugefügt wurden, und diese Workloads anhand der zugewiesenen Performance Service Levels und Storage Efficiency Policies managen.

Sie können diese Funktion unter **Allgemein** > **Funktionseinstellungen** > **richtlinienbasierte Storage Verwaltung** aktivieren oder deaktivieren. Nach der Aktivierung dieser Funktion stehen die folgenden Seiten für Betrieb und Überwachung zur Verfügung:

- Provisionierung (Provisionierung von Storage Workloads)
- **Richtlinien** > **Performance Service Levels**
- **Richtlinien** > **Speichereffizienz**
- Workloads, die von der Spalte „Performance Service Level“ auf der Seite „Clusters Setup“ verwaltet werden
- Bereich „Workload Performance“ im **Dashboard**

Mithilfe der Bildschirme können Sie Performance Service Levels und Storage Efficiency Policies erstellen und Storage Workloads provisionieren. Sie können außerdem die Storage Workloads überwachen, die den zugewiesenen Performance Service Levels entsprechen, sowie diejenigen, die nicht entsprechen. Der Bereich „Workload Performance und Workload IOPS“ ermöglicht Ihnen außerdem, die Gesamt-, verfügbare und genutzte Kapazität sowie die Performance (IOPS) der Cluster in Ihrem Datacenter auf Grundlage der darauf provisionierten Storage Workloads zu bewerten.

Nach der Aktivierung dieser Funktion können Sie die Unified Manager REST APIs ausführen, um einige dieser Funktionen über **Menu Bar** > **Help button** > **API Documentation** > Kategorie **storage-provider** auszuführen. Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL eingeben, um im Format https://<hostname>/docs/api/ auf die REST API-Seite zuzugreifen.

Weitere Informationen zu den APIs sind unter "Erste Schritte mit Active IQ Unified Manager REST APIs" verfügbar.

Informationen zur API Gateway Funktion in Active IQ Unified Manager

Die API Gateway Funktion ermöglicht es, dass Active IQ Unified Manager als eine einzige Kontrollebene dient, über die Sie mehrere ONTAP Cluster managen können, ohne sich bei jedem einzelnen anmelden zu müssen.

Sie können diese Funktion auf den Konfigurationsseiten aktivieren, die bei der ersten Anmeldung bei Unified Manager angezeigt werden. Alternativ können Sie diese Funktion unter **General** > **Feature Settings** > **API Gateway** aktivieren oder deaktivieren.

Die Unified Manager REST APIs unterscheiden sich von den ONTAP REST APIs, und nicht alle Funktionen der ONTAP REST APIs können mit den Unified Manager REST APIs genutzt werden. Wenn jedoch eine spezifische geschäftliche Anforderung für den Zugriff auf die ONTAP APIs besteht, um bestimmte Funktionen zu managen, die in Unified Manager nicht verfügbar gemacht werden, kann die API Gateway Funktion aktiviert und die ONTAP APIs ausgeführt werden. Das Gateway fungiert als Proxy, um die API-Anfragen weiterzuleiten, wobei Header und Body der Anfragen im selben Format wie in den ONTAP APIs beibehalten werden. Sie können Ihre Unified Manager Anmeldeinformationen verwenden und die spezifischen APIs ausführen, um auf die ONTAP Cluster zuzugreifen und sie zu managen, ohne individuelle Anmeldeinformationen für Cluster übergeben zu müssen. Unified Manager fungiert als zentraler Managementpunkt für die Ausführung der APIs über die ONTAP Cluster hinweg, die von Ihrer Unified Manager Instanz gemanagt werden. Die von den APIs zurückgegebene Antwort ist dieselbe wie die Antwort, die von den jeweiligen ONTAP REST APIs zurückgegeben wird, wenn sie direkt über ONTAP ausgeführt werden.

Nach dem Aktivieren dieser Funktion können Sie die Unified Manager REST APIs über **Menüleiste** > **Hilfe** > **API-Dokumentation** > Kategorie **gateway** ausführen. Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL eingeben, um im folgenden Format auf die REST API-Seite zuzugreifen `https://<hostname>/docs/api/`

Weitere Informationen zu den APIs sind unter "Erste Schritte mit Active IQ Unified Manager REST APIs" verfügbar.

Angeben der Zeitüberschreitung bei Inaktivität in Active IQ Unified Manager

Sie können den Wert für die Zeitüberschreitung bei Inaktivität für Active IQ Unified Manager festlegen. Nach der angegebenen Dauer der Inaktivität wird die Applikation automatisch abgemeldet. Diese Option ist standardmäßig aktiviert.

Sie können diese Funktion unter **Allgemein** > **Funktionseinstellungen** > **Inaktivitäts-Timeout** deaktivieren oder die Zeit anpassen. Nach der Aktivierung sollten Sie im Feld **ABMELDEN NACH** die maximale Inaktivitätszeit (in Minuten) festlegen, nach der das System Sie automatisch abmeldet. Der Standardwert beträgt 4320 Minuten (72 Stunden).

Diese Option ist nicht verfügbar, wenn Sie die Security Assertion Markup Language (SAML) Authentifizierung aktiviert haben.

Aktivierung von Active IQ Portalereignissen in Active IQ Unified Manager

Sie können festlegen, ob Ereignisse des Active IQ Portals aktiviert oder deaktiviert werden sollen. Diese Einstellung ermöglicht es dem Active IQ Portal, zusätzliche Ereignisse zur Systemkonfiguration, Verkabelung usw. zu identifizieren und anzuzeigen. Diese Option ist standardmäßig aktiviert.

Nach der Aktivierung dieser Funktion zeigt Active IQ Unified Manager Ereignisse an, die vom Active IQ Portal identifiziert wurden. Diese Ereignisse werden durch die Ausführung einer Reihe von Regeln auf AutoSupport Meldungen erstellt, die von allen überwachten Storage Systemen generiert werden. Diese Ereignisse unterscheiden sich von den anderen Unified Manager Ereignissen und identifizieren Vorfälle oder Risiken im Zusammenhang mit Systemkonfiguration, Verkabelung, Best Practices und Verfügbarkeitsproblemen.

Sie können diese Funktion unter **General** > **Feature Settings** > **Active IQ Portal Events** aktivieren oder deaktivieren. An Standorten ohne externen Netzwerkzugriff müssen Sie die Regeln manuell unter **Storage Management** > **Event Setup** > **Upload Rules** hochladen.

Diese Funktion ist standardmäßig aktiviert. Die Deaktivierung dieser Funktion bewirkt, dass Active IQ Ereignisse nicht mehr von Unified Manager identifiziert oder dort angezeigt werden. Wenn diese Funktion deaktiviert ist, kann Unified Manager nach ihrer Aktivierung Active IQ Ereignisse auf einem Cluster zu einer vordefinierten Zeit von 00:15 Uhr in der Zeitzone dieses Clusters empfangen.

Aktivieren und Deaktivieren von Sicherheitseinstellungen für die Compliance in Active IQ Unified Manager

Mithilfe der Schaltfläche **Anpassen** im Bereich **Sicherheits-Dashboard** der Seite „Funktionseinstellungen“ können Sie die Sicherheitsparameter für die Compliance-Überwachung in Unified Manager aktivieren oder deaktivieren.

Die auf dieser Seite aktivierten oder deaktivierten Einstellungen steuern den allgemeinen Compliance Status der Cluster und Storage VMs in Unified Manager. Je nach Auswahl sind die entsprechenden Spalten in der Ansicht **Security: All Clusters** auf der Cluster-Inventarseite und in der Ansicht **Security: All Storage VMs** auf der Storage VMs-Inventarseite sichtbar.

Nur Benutzer mit Administratorrolle können diese Einstellungen bearbeiten.

Die Sicherheitskriterien für Ihre ONTAP Cluster, Storage-VMs und Volumes werden anhand der in der "Leitfaden zur Sicherheitshärtung für NetApp ONTAP 9" definierten Empfehlungen bewertet. Im Sicherheitsbereich des Dashboard und auf der Seite Sicherheit wird der standardmäßige Sicherheits-Compliance-Status Ihrer Cluster, Storage-VMs und Volumes angezeigt. Für Cluster und Storage-VMs mit Sicherheitsverstößen werden außerdem Sicherheitsereignisse generiert und Managementaktionen aktiviert.

Sicherheitseinstellungen anpassen

Zur Anpassung der Einstellungen für die Compliance-Überwachung an Ihre ONTAP Umgebung sind die folgenden Schritte relevant:

Schritte

1. Die Auswahl erfolgt über **Allgemein > Funktionseinstellungen > Sicherheits-Dashboard > Anpassen**. Das Popup **Einstellungen für das Sicherheits-Dashboard anpassen** wird angezeigt.

   Die von Ihnen aktivierten oder deaktivierten Sicherheits-Compliance-Parameter können sich direkt auf die standardmäßigen Sicherheitsansichten, Berichte und geplanten Berichte in den Bildschirmen „Clusters“ und „Storage VMs“ auswirken. Wenn Sie vor der Änderung der Sicherheitsparameter einen Excel-Bericht aus diesen Bildschirmen hochgeladen hatten, könnten die heruntergeladenen Excel-Berichte fehlerhaft sein.

2. Das Aktivieren oder Deaktivieren der benutzerdefinierten Einstellungen für Ihre ONTAP Cluster erfolgt durch Auswahl der gewünschten allgemeinen Einstellung unter **Cluster**. Informationen zu den Optionen für die Anpassung der Cluster Compliance finden Sie unter "Compliance-Kategorien für Cluster".
3. Zum Aktivieren oder Deaktivieren der benutzerdefinierten Einstellungen für Ihre Storage VMs können Sie unter **Storage VM** die gewünschte allgemeine Einstellung auswählen. Informationen zu den Optionen zum Anpassen der Storage VM Compliance finden Sie unter "Compliance-Kategorien für Storage-VMs".

Anpassen von AutoSupport und Authentifizierungseinstellungen

Im Abschnitt **AutoSupport Settings** können Sie festlegen, ob HTTPS für das Senden von AutoSupport Nachrichten von ONTAP verwendet werden soll.

Im Abschnitt **Authentifizierungseinstellungen** können Sie aktivieren, dass Unified Manager Warnungen für den standardmäßigen ONTAP Administratorbenutzer ausgegeben werden.

Aktivieren und Deaktivieren des Skript-Uploads in Active IQ Unified Manager

Das Hochladen und Ausführen von Skripten in Unified Manager ist standardmäßig aktiviert. Wenn Ihr Unternehmen diese Aktivität aus Sicherheitsgründen nicht zulassen möchte, können Sie diese Funktion deaktivieren.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Funktionseinstellungen**.
2. Auf der Seite **Funktionseinstellungen** können Sie die Skriptausführung deaktivieren oder aktivieren, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Skripte deaktivieren	Im Bereich **Script Upload** lässt sich der Schieberegler nach links bewegen.
Aktivierung von Skripten	Im Bereich **Script Upload** den Schieberegler nach rechts stellen.

Hinzufügen eines Anmeldebanners in Active IQ Unified Manager

Durch das Hinzufügen eines Anmeldebanners kann Ihr Unternehmen beliebige Informationen anzeigen, z. B. wer Zugriff auf das System hat und welche Nutzungsbedingungen gelten, sowohl beim An- als auch beim Abmelden.

Jeder Benutzer, z. B. Storage Operatoren oder Administratoren, kann dieses Anmeldebanner-Popup bei der Anmeldung, Abmeldung und bei Zeitüberschreitung der Sitzung anzeigen.

Verwendung der Managementplattform

Informationen zur Wartungskonsole in Active IQ Unified Manager

Mit der Unified Manager Managementplattform für Wartung können Sie die Einstellungen auf Ihrem Unified Manager System managen und alle erforderlichen Änderungen vornehmen, um Probleme zu vermeiden.

Je nach dem Betriebssystem, auf dem Sie Unified Manager installiert haben, bietet die Managementplattform folgende Wartungsfunktionen:

- Fehlerbehebung bei Problemen mit Ihrer virtuellen Appliance, insbesondere wenn die Weboberfläche von Unified Manager nicht verfügbar ist
- Aktualisierung auf neuere Versionen von Unified Manager

- Support-Bundles für den Versand an den technischen Support generieren
- Netzwerkeinstellungen konfigurieren
- Passwort des Wartungsbenutzers ändern
- Verbindung zu einem externen Datenanbieter zum Senden von Performance Statistiken herstellen
- Änderung der internen Erfassung von Performance-Daten
- Wiederherstellung der Unified Manager Datenbank und der Konfigurationseinstellungen aus einer zuvor gesicherten Version.

Informationen zum Wartungsbenutzer in Active IQ Unified Manager

Der Wartungsbenutzer wird bei der Installation von Unified Manager auf einem Red Hat Enterprise Linux-System angelegt. Der Name des Wartungsbenutzers ist der Benutzer “umadmin”. Der Wartungsbenutzer hat in der web UI die Rolle Application Administrator und kann weitere Benutzer anlegen und ihnen Rollen zuweisen.

Der Wartungsbenutzer oder der umadmin Benutzer kann auch auf die Unified Manager Managementplattform zugreifen.

Diagnosefunktionen für Benutzer in Active IQ Unified Manager

Der Diagnosezugriff dient dazu, dass der technische Support Sie bei der Fehlersuche unterstützen kann, und Sie sollten ihn nur auf Anweisung des technischen Supports verwenden.

Der Diagnosebenutzer kann auf Anweisung des technischen Supports Befehle auf Betriebssystemebene zur Fehlerbehebung ausführen.

Zugriff auf die Wartungskonsole in Active IQ Unified Manager

Wenn die Unified Manager Benutzeroberfläche nicht in Betrieb ist oder wenn Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Wartungs-Managementplattform zugreifen, um Ihr Unified Manager System zu managen.

Bevor Sie beginnen

Sie müssen Unified Manager installiert und konfiguriert haben.

Nach 15 Minuten Inaktivität meldet die Wartungs-Managementplattform Sie ab.



Bei der Installation auf VMware ist eine gleichzeitige Anmeldung über Secure Shell nicht möglich, wenn Sie sich bereits als Wartungsbenutzer über die VMware Managementplattform angemeldet haben.

Schritt

1. Der Zugriff auf die Managementplattform erfolgt in den folgenden Schritten:

Auf diesem Betriebssystem…	Folgen Sie diesen Schritten…
VMware	a. Die Verbindung zur IP-Adresse oder zur vollqualifizierten Domain der virtuellen Unified Manager Appliance erfolgt mithilfe von Secure Shell. b. Zur Anmeldung bei der Managementplattform dienen Ihr Wartungsbenutzername und Ihr Passwort.
Linux	a. Die Verbindung mit der IP-Adresse oder dem vollqualifizierten Domainnamen des Unified Manager Systems erfolgt mithilfe von Secure Shell. b. Die Anmeldung am System erfolgt mit dem Benutzernamen und Passwort des Wartungsbenutzers (umadmin). c. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.
Windows	a. Für die Anmeldung am Unified Manager System werden Administratoranmeldedaten verwendet. b. Starten von PowerShell als Windows-Administrator. c. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.

Das Menü der Unified Manager Wartungs-Managementplattform wird angezeigt.

Zugriff auf die Wartungskonsole über die vSphere VM-Konsole in Active IQ Unified Manager

Falls die Unified Manager Benutzeroberfläche nicht funktioniert oder falls Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Managementplattform zugreifen, um Ihre virtuelle Appliance neu zu konfigurieren.

Bevor Sie beginnen

- Sie müssen der Wartungsbenutzer sein.
- Die virtuelle Appliance muss eingeschaltet sein, um auf die Wartungs Managementplattform zuzugreifen.

Schritte

1. Die virtuelle Appliance Unified Manager befindet sich im vSphere Client.
2. Sie wählen die Registerkarte **Console** aus.
3. Zum Anmelden ist ein Klick in das Fenster der Managementplattform erforderlich.
4. Die Anmeldung bei der Managementplattform für die Wartung erfolgt mit Ihrem Benutzernamen und Passwort.

   Nach 15 Minuten Inaktivität meldet die Wartungs-Managementplattform Sie ab.

Menüs der Managementplattform für die Wartung

Informationen zu den Wartungskonsolenmenüs in Active IQ Unified Manager

Die Managementplattform besteht aus verschiedenen Menüs, die die Wartung und Verwaltung spezieller Funktionen und Konfigurationseinstellungen des Unified Manager Servers ermöglichen.

Je nach Betriebssystem, auf dem Sie Unified Manager installiert haben, besteht die Wartungs-Managementplattform aus den folgenden Menüs:

- Upgrade von Unified Manager (nur VMware)
- Netzwerkkonfiguration (nur VMware)
- Systemkonfiguration (nur VMware)
  a. Support/Diagnostik
  b. Serverzertifikat zurücksetzen
  c. Client Zertifikat neu generieren
  d. Backup-Wiederherstellung
  e. Externer Datenanbieter
  f. Konfiguration des Abfrageintervalls für die Performance
  g. SAML-Authentifizierung deaktivieren
  h. Applikationsports anzeigen/ändern
  i. Konfiguration des Debug-Protokolls
  j. Zugriff auf MySQL Port 3306 steuern
  k. Beenden

Sie wählen die Nummer aus der Liste aus, um auf die entsprechende Menüoption zuzugreifen. Beispielsweise wählen Sie für Backup und Wiederherstellung die Nummer 4.

Menü „Netzwerkkonfiguration“ in Active IQ Unified Manager

Über das Menü „Netzwerkkonfiguration“ können Sie die Netzwerkeinstellungen managen. Dieses Menü sollte verwendet werden, wenn die Benutzeroberfläche von Unified Manager nicht verfügbar ist.

Dieses Menü ist nicht verfügbar, wenn Unified Manager auf Red Hat Enterprise Linux oder auf Microsoft Windows installiert ist.

Folgende Menüoptionen stehen zur Verfügung.

- **Einstellungen für die Anzeige der IP-Adresse**

  Zeigt die aktuellen Netzwerkeinstellungen für die virtuelle Appliance an, einschließlich IP-Adresse, Netzwerk, Broadcast-Adresse, Netzmaske, Gateway und DNS-Server.

- **Ändern der IP-Adresseneinstellungen**

Damit können Sie alle Netzwerkeinstellungen der virtuellen Appliance ändern, einschließlich der IP-Adresse, der Netzmaske, des Gateways oder der DNS-Server. Wenn Sie Ihre Netzwerkeinstellungen über die Wartungs-Managementplattform von DHCP auf statische Netzwerkkonfiguration umstellen, können Sie den Hostnamen nicht bearbeiten. Damit die Änderungen wirksam werden, muss **Commit Changes** ausgewählt werden.

- **Einstellungen für die Domainnamensuche anzeigen**

  Zeigt die für die Auflösung von Hostnamen verwendete Suchliste für Domainnamen an.

- **Einstellungen für die Domainnamensuche ändern**

  Hiermit können Sie die Domänennamen ändern, nach denen bei der Auflösung von Hostnamen gesucht werden soll. Sie müssen **Commit Changes** auswählen, damit die Änderungen wirksam werden.

- **Anzeige statischer Routen**

  Zeigt die aktuellen statischen Netzwerkrouten an.

- **Statische Routen ändern**

  Ermöglicht das Hinzufügen oder Löschen statischer Netzwerkrouten. **Änderungen übernehmen** muss ausgewählt werden, damit die Änderungen wirksam werden.

  - **Route hinzufügen**

    Ermöglicht das Hinzufügen einer statischen Route.

  - **Route löschen**

    Ermöglicht das Löschen einer statischen Route.

  - **Zurück**

    Sie gelangen zurück zum **Main Menu**.

  - **Beenden**

    Beendet die Wartungs-Console.

- **Netzwerkschnittstelle deaktivieren**

  Deaktiviert alle verfügbaren Netzwerkschnittstellen. Wenn nur eine Netzwerkschnittstelle verfügbar ist, kann sie nicht deaktiviert werden. Damit die Änderungen wirksam werden, muss **Commit Changes** ausgewählt werden.

- **Netzwerkschnittstelle aktivieren**

  Aktiviert die verfügbaren Netzwerkschnittstellen. Sie müssen **Commit Changes** auswählen, damit die Änderungen wirksam werden.

- **Änderungen übernehmen**

  Wendet alle an den Netzwerkeinstellungen der virtuellen Appliance vorgenommenen Änderungen an. Diese Option muss ausgewählt werden, damit vorgenommene Änderungen wirksam werden, andernfalls treten die Änderungen nicht in Kraft.

- **Host anpingen**

  Dient zum Anpingen eines Zielhosts, um IP-Adressänderungen oder DNS-Konfigurationen zu bestätigen.

- **Auf Standardeinstellungen zurücksetzen**

  Setzt alle Einstellungen auf die Werkseinstellungen zurück. Sie müssen **Änderungen übernehmen** auswählen, damit die Änderungen wirksam werden.

- **Zurück**

  Sie gelangen zurück zum **Main Menu**.

- **Beenden**

  Beendet die Wartungs-Console.

Im Active IQ Unified Manager steht das Menü „Systemkonfiguration“ zur Verfügung

Das Menü „Systemkonfiguration“ ermöglicht Ihnen das Managen Ihrer virtuellen Appliance mithilfe verschiedener Optionen, wie z. B. der Anzeige des Serverstatus sowie dem Neustarten und Herunterfahren der virtuellen Maschine.

Wenn Unified Manager auf einem Linux- oder Microsoft Windows-System installiert ist, steht in diesem Menü nur die Option „`Restore from a Unified Manager Backup`“ zur Verfügung.

Folgende Menüoptionen stehen zur Verfügung:

- **Serverstatus anzeigen**

  Zeigt den aktuellen Serverstatus an. Zu den Statusoptionen gehören „Läuft“ und „Läuft nicht“.

  Falls der Server nicht läuft, müssen Sie sich möglicherweise an den technischen Support wenden.

- **Virtuelle Maschine neu starten**

  Die virtuelle Maschine wird neu gestartet, dabei werden alle Services beendet. Nach dem Neustart starten die virtuelle Maschine und die Services erneut.

- **Virtuelle Maschine herunterfahren**

  Fährt die virtuelle Maschine herunter und beendet alle Services.

  Diese Option steht nur in der Managementplattform der virtuellen Maschine zur Auswahl.

- **Änderung des <logged in user> Benutzerpassworts**

  Ändert das Passwort des aktuell angemeldeten Benutzers, bei dem es sich nur um den Wartungsbenutzer handeln kann.

- **Größe der Datenfestplatte erhöhen**

  Erhöht die Größe der Datenfestplatte (Festplatte 3) in der virtuellen Maschine.

- **Swap-Datenträgergröße erhöhen**

  Erhöht die Größe der Auslagerungsfestplatte (Festplatte 2) in der virtuellen Maschine.

- **Änderung der Zeitzone**

  Ändert die Zeitzone entsprechend Ihrem Standort.

- **NTP-Server ändern**

  Ändert die NTP-Servereinstellungen, wie z. B. die IP-Adresse oder die vollqualifizierte Domain (FQDN).

- **NTP-Service ändern**

  Wechselt zwischen den `ntp` und `systemd-timesyncd` Services.

- **Wiederherstellung aus einer Unified Manager Sicherung**

  Stellt die Unified Manager Datenbank und die Konfigurationseinstellungen aus einer zuvor gesicherten Version wieder her.

- **Serverzertifikat zurücksetzen**

  Setzt das Server-Sicherheitszertifikat zurück.

- **Hostname ändern**

  Ändert den Namen des Hosts, auf dem die virtuelle Appliance installiert ist.

- **Zurück**

  Verlassen des Menüs „Systemkonfiguration“ und Rückkehr zum Hauptmenü.

- **Beenden**

  Verlässt das Menü der Wartungs-Managementplattform.

Das Menü „Support und Diagnose“ in Active IQ Unified Manager kann verwendet werden

Über das Menü „Support und Diagnose“ können Sie ein Supportpaket erstellen, das Sie zur Fehlerbehebung an den technischen Support senden können.

Folgende Menüoptionen stehen zur Verfügung:

- **Light Support Bundle generieren**

  Ermöglicht die Erstellung eines schlanken Support-Bundles, das nur 30 Tage Protokolle und Konfigurationsdatenbankeinträge enthält; Performance-Daten, Erfassungsaufzeichnungsdateien und Server-Heap-Dump sind ausgeschlossen.

- **Support Bundle generieren**

  Ermöglicht das Erstellen eines vollständigen Support-Pakets (7-Zip-Datei) mit Diagnoseinformationen im Home-Verzeichnis des Diagnosebenutzers. Wenn Ihr System mit dem Internet verbunden ist, kann das Support-Paket auch auf NetApp hochgeladen werden.

Die Datei enthält Informationen, die durch eine AutoSupport Nachricht generiert werden, den Inhalt der Unified Manager Datenbank, detaillierte Daten über die Interna des Unified Manager Servers sowie ausführliche Protokolle, die normalerweise nicht in AutoSupport Nachrichten oder im Lightweight Support Bundle enthalten sind.

Zusätzliche Menüoptionen der Wartungskonsole in Active IQ Unified Manager

Die folgenden Menüoptionen ermöglichen Ihnen die Durchführung verschiedener administrativer Aufgaben auf dem Unified Manager Server.

Folgende Menüoptionen stehen zur Verfügung:

- **Serverzertifikat zurücksetzen**

  Generiert das HTTPS-Serverzertifikat erneut.

  Sie können das Serverzertifikat in der Unified Manager GUI durch Klicken auf **General** > **HTTPS Certificates** > **Regenerate HTTPS Certificate** neu generieren.

- **SAML Authentifizierung deaktivieren**

  Deaktiviert die SAML Authentifizierung, sodass der Identitätsanbieter (IdP) keine Anmeldeauthentifizierung mehr für Benutzer bereitstellt, die auf die Unified Manager GUI zugreifen. Diese Managementplattform Option wird typischerweise verwendet, wenn ein Problem mit dem IdP-Server oder der SAML-Konfiguration den Zugriff von Benutzern auf die Unified Manager GUI verhindert.

- **Externer Datenanbieter**

  Bietet Optionen zum Verbinden von Unified Manager mit einem externen Datenanbieter. Nach dem Herstellen der Verbindung werden Performance-Daten an einen externen Server gesendet, sodass Storage-Performance-Experten die Performance-Kennzahlen mithilfe von Drittanbietersoftware grafisch darstellen können. Folgende Optionen werden angezeigt:

  - **Anzeigen der Serverkonfiguration**--Zeigt die aktuelle Verbindung und die Konfigurationseinstellungen für einen externen Datenanbieter an.
  - **Serververbindung hinzufügen / ändern** - ermöglicht die Eingabe neuer Verbindungseinstellungen für einen externen Datenanbieter oder die Änderung bestehender Einstellungen.
  - **Serverkonfiguration ändern** - Ermöglicht die Eingabe neuer Konfigurationseinstellungen für einen externen Datenanbieter oder die Änderung bestehender Einstellungen.
  - **Serververbindung löschen**--Löscht die Verbindung zu einem externen Datenanbieter.

    Nach dem Löschen der Verbindung verliert Unified Manager die Verbindung zum externen Server.

- **Backup-Wiederherstellung**

  Weitere Informationen finden Sie in den Themen unter "Verwaltung von Sicherungs- und Wiederherstellungsvorgängen".

- **Konfiguration des Performance-Abfrageintervalls**

  Stellt eine Option zum Konfigurieren der Häufigkeit bereit, mit der Unified Manager Performance-Statistikdaten von Clustern erfasst. Das Standarderfassungsintervall beträgt 5 Minuten.

  Sie können dieses Intervall auf 10 oder 15 Minuten ändern, wenn Sie feststellen, dass Datenerfassungen

großer Cluster nicht rechtzeitig abgeschlossen sind.

- **Anwendungsports anzeigen/ändern**

  Es besteht die Möglichkeit, die Standardports zu ändern, die Unified Manager für die HTTP- und HTTPS-Protokolle verwendet, falls dies aus Sicherheitsgründen erforderlich ist. Die Standardports sind 80 für HTTP und 443 für HTTPS.

- **Zugriff auf MySQL Port 3306 kontrollieren**

  Steuert den Hostzugriff auf den Standard-MySQL-Port 3306. Aus Sicherheitsgründen ist der Zugriff über diesen Port bei einer Neuinstallation von Unified Manager auf Linux-, Windows- und VMware vSphere-Systemen nur auf localhost beschränkt. Mit dieser Option können Sie die Transparenz dieses Ports zwischen localhost und Remote-Hosts umschalten, das heißt, wenn er in Ihrer Umgebung nur für localhost aktiviert ist, können Sie diesen Port auch für Remote-Hosts verfügbar machen. Alternativ können Sie den Zugriff über diesen Port nur auf localhost beschränken, wenn er für alle Hosts aktiviert ist. Wenn der Zugriff zuvor auf Remote-Hosts aktiviert war, bleibt die Konfiguration bei einem Upgrade erhalten. Nach dem Umschalten der Port-Transparenz sollten die Firewall-Einstellungen auf Windows-Systemen überprüft und die Firewall-Einstellungen deaktiviert werden, wenn sie so konfiguriert sind, dass sie den Zugriff auf den MySQL-Port 3306 einschränken.

- **Beenden**

  Verlässt das Menü der Wartungs-Managementplattform.

Das Kennwort des Wartungsbenutzers unter Windows in Active IQ Unified Manager ändern

Sie können das Wartungsbenutzerkennwort von Unified Manager bei Bedarf ändern.

Schritte

1. Auf der Anmeldeseite der Unified Manager Web UI können Sie **Forgot Password** auswählen.

   Es wird eine Seite angezeigt, auf der Sie den Namen des Benutzers eingeben, dessen Passwort Sie zurücksetzen möchten.

2. Den Benutzernamen eingeben und auf **Submit** klicken.

   An die für diesen Benutzernamen definierte E-Mail-Adresse wird eine E-Mail mit einem Link zum Zurücksetzen des Passworts gesendet.

3. Das neue Passwort wird über den **Link zum Zurücksetzen des Passworts** in der E-Mail definiert.
4. Anschließend erfolgt die Anmeldung bei Unified Manager über die Web-Benutzeroberfläche mit dem neuen Passwort.

Ändern des Active IQ Unified Manager umadmin Passworts auf Linux Systemen

Aus Sicherheitsgründen müssen Sie das Standardpasswort für den Unified Manager-Benutzer „umadmin“ unmittelbar nach Abschluss der Installation ändern. Bei Bedarf können Sie das Passwort später jederzeit erneut ändern.

Bevor Sie beginnen

- Unified Manager muss auf einem Red Hat Enterprise Linux Linux System installiert sein.
- Sie benötigen die Root-Benutzer-Anmeldedaten für das Linux-System, auf dem Unified Manager installiert ist.

Schritte

1. Die Anmeldung als Root-Benutzer erfolgt auf dem Linux-System, auf dem Unified Manager ausgeführt wird.
2. Das Passwort des Benutzers umadmin ändern:

   ```
   passwd umadmin
   ```

   Das System fordert Sie auf, ein neues Passwort für den Benutzer umadmin einzugeben.

Die von Active IQ Unified Manager für die HTTP- und HTTPS-Protokolle verwendeten Ports können geändert werden.

Die von Unified Manager standardmäßig für HTTP- und HTTPS-Protokolle verwendeten Ports können nach der Installation bei Bedarf aus Sicherheitsgründen geändert werden. Die Standardports sind 80 für HTTP und 443 für HTTPS.

Bevor Sie beginnen

Sie müssen über eine Benutzerkennung und ein Passwort verfügen, die für die Anmeldung an der Managementplattform für die Wartung des Unified Manager Servers autorisiert sind.

> Bei der Verwendung von Mozilla Firefox oder Google Chrome gelten einige Ports als unsicher. Vor der Zuweisung einer neuen Portnummer für HTTP- und HTTPS-Datenverkehr ist eine Prüfung im Browser erforderlich. Die Auswahl eines unsicheren Ports kann dazu führen, dass das System nicht mehr erreichbar ist; in diesem Fall ist zur Behebung des Problems eine Kontaktaufnahme mit dem Kundensupport erforderlich.

Die Instanz von Unified Manager wird nach dem Ändern des Ports automatisch neu gestartet. Daher sollte dies ein geeigneter Zeitpunkt sein, um das System für kurze Zeit herunterzufahren.

1. Sie melden sich per SSH als Wartungsbenutzer am Unified Manager Host an.

   Die Eingabeaufforderungen der Unified Manager Wartungs-Managementplattform werden angezeigt.

2. Sie geben die Nummer der Menüoption mit der Bezeichnung **Anwendungsports anzeigen/ändern** ein und drücken anschließend die Eingabetaste.
3. Falls Sie dazu aufgefordert werden, geben Sie das Passwort des Wartungsbenutzers erneut ein.
4. Die neuen Portnummern für die HTTP- und HTTPS-Ports eingeben und anschließend die Eingabetaste drücken.

   Bleibt die Portnummer leer, wird der Standardport für das Protokoll verwendet.

   Die Abfrage lautet, ob Sie die Ports ändern und Unified Manager jetzt neu starten möchten.

5. Zum Ändern der Ports und zum Neustart von Unified Manager **y** eingeben.
6. Verlassen der Wartungskonsole.

Nach dieser Änderung müssen Benutzer die neue Portnummer in die URL einfügen, um auf die Unified

Manager Web-UI zuzugreifen, zum Beispiel https://host.company.com:1234, https://12.13.14.15:1122 oder https://[2001:db8:0:1]:2123.

Netzwerkschnittstellen zu Active IQ Unified Manager hinzufügen

Neue Netzwerkschnittstellen lassen sich hinzufügen, wenn eine Trennung des Netzwerkverkehrs erforderlich ist.

Bevor Sie beginnen

Sie müssen die Netzwerkschnittstelle mithilfe von vSphere zur virtuellen Appliance hinzugefügt haben.

Die virtuelle Appliance muss eingeschaltet sein.

Sie können diesen Vorgang nicht ausführen, wenn Unified Manager auf Red Hat Enterprise Linux oder Microsoft Windows installiert ist.

Schritte

1. Im Hauptmenü der vSphere Managementplattform **System Configuration** > **Reboot Operating System** auswählen.

   Nach dem Neustart kann die Wartungskonsole die neu hinzugefügte Netzwerkschnittstelle erkennen.

2. Auf die Wartungskonsole zugreifen.
3. Die Auswahl erfolgt über **Netzwerkkonfiguration** > **Netzwerkschnittstelle aktivieren**.
4. Anschließend die neue Netzwerkschnittstelle auswählen und die **Eingabetaste** drücken.

   eth1 wird ausgewählt und mit **Enter** bestätigt.

5. Zur Aktivierung der Netzwerkschnittstelle ist die Eingabe von **y** erforderlich.
6. Nun erfolgt die Eingabe der Netzwerkeinstellungen.

   Die Eingabe der Netzwerkeinstellungen ist erforderlich, wenn eine statische Schnittstelle verwendet wird oder DHCP nicht erkannt wird.

   Nach Eingabe der Netzwerkeinstellungen kehren Sie automatisch zum Menü **Netzwerkkonfiguration** zurück.

7. **Änderungen übernehmen** auswählen.

   Sie müssen die Änderungen übernehmen, um die Netzwerkschnittstelle hinzuzufügen.

Das Clientzertifikat in Active IQ Unified Manager neu generieren

Sie können die Managementplattform verwenden, um Ihr Unified Manager Client-Zertifikat neu zu generieren. Ihr Zertifikat hat eine verlängerte Gültigkeitsdauer von fünf Jahren.

Schritte

1. Melden Sie sich als Wartungsbenutzer an.
2. Wählen Sie **Regenerate Client Certificate** aus und drücken Sie **Enter**.

3. Falls das System eine Authentifizierung anfordert, müssen die erforderlichen Anmeldeinformationen eingegeben werden.
4. **Confirm Regeneration** wird ausgewählt und **Enter** wird gedrückt.
5. Nach der Neugenerierung des Zertifikats muss der Unified Manager Dienst neu gestartet werden, um die Änderungen anzuwenden.
6. Zur Überprüfung des aktualisierten Zertifikats ist eine Anmeldung bei ONTAP erforderlich. Der Status des Clientzertifikats und der Gültigkeitsstatus sind zu sehen.

Verwandte Informationen "ONTAP Zertifikate mit System Manager verwalten"

Festplattenspeicher hinzufügen

Dem Active IQ Unified Manager Datenbankverzeichnis Speicherplatz hinzufügen

Das Unified Manager Datenbankverzeichnis enthält alle von ONTAP Systemen erfassten Systemstatus- und Performance-Daten. Unter bestimmten Umständen kann es erforderlich sein, die Größe des Datenbankverzeichnisses zu erhöhen.

Das Datenbankverzeichnis kann beispielsweise voll werden, wenn Unified Manager Daten von einer großen Anzahl von Clustern erfasst, von denen jedes viele Knoten hat. Sie erhalten ein Warnereignis, wenn das Datenbankverzeichnis zu 90 % gefüllt ist, und ein kritisches Ereignis, wenn das Verzeichnis zu 95 % gefüllt ist.

Sobald das Verzeichnis zu 95% gefüllt ist, werden keine zusätzlichen Daten mehr von Clustern erfasst.

Die erforderlichen Schritte zum Hinzufügen von Kapazität zum Datenverzeichnis unterscheiden sich je nachdem, ob Unified Manager auf einem VMware ESXi-Server, einem Red Hat-Server oder einem Microsoft Windows-Server ausgeführt wird.

Hinzufügen von Speicherplatz zum Datenverzeichnis auf einem Linux-Host in Active IQ Unified Manager

Falls Sie bei der ursprünglichen Einrichtung des Linux-Hosts dem `/opt/netapp/data` Verzeichnis nicht genügend Speicherplatz zur Unterstützung von Unified Manager zugewiesen und anschließend Unified Manager installiert haben, können Sie nach der Installation zusätzlichen Speicherplatz hinzufügen, indem Sie den Speicherplatz im `/opt/netapp/data` Verzeichnis erhöhen.

Bevor Sie beginnen

Sie benötigen Zugriff als Root-Benutzer auf den Red Hat Enterprise Linux Rechner, auf dem Unified Manager installiert ist.

Wir empfehlen Ihnen, die Unified Manager Datenbank zu sichern, bevor Sie die Größe des Datenverzeichnisses erhöhen.

Schritte

1. Die Anmeldung als Root-Benutzer erfolgt auf dem Linux-Rechner, auf dem zusätzlicher Festplattenspeicher hinzugefügt werden soll.
2. Die Beendigung des Unified Manager Service und der zugehörigen MySQL Software erfolgt in der

angegebenen Reihenfolge:

```
systemctl stop ocieau ocie mysqld
```

3. Es wird ein temporärer Sicherungsordner (zum Beispiel `/backup-data`) mit ausreichendem Speicherplatz für die Daten im aktuellen `/opt/netapp/data` Verzeichnis benötigt.
4. Der Inhalt und die Berechtigungskonfiguration des vorhandenen `/opt/netapp/data`Verzeichnisses sind in das Sicherungsdatenverzeichnis zu kopieren:

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

5. Wenn SE Linux aktiviert ist:

   a. SE Linux-Typ für Ordner in einem vorhandenen `/opt/netapp/data` Ordner:

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      Das System gibt eine Bestätigung zurück, die in etwa wie folgt aussieht:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Der Befehl chcon legt den SE Linux Typ für das Backup-Verzeichnis fest:

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. Entfernen des Inhalts des `/opt/netapp/data` Verzeichnisses:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Die Größe des `/opt/netapp/data` Verzeichnisses ist mithilfe von LVM-Befehlen oder durch Hinzufügen zusätzlicher Festplatten auf mindestens 150 GB zu erweitern.

   > Wenn Sie `/opt/netapp/data` von einer Festplatte erstellt haben, sollten Sie nicht versuchen, `/opt/netapp/data` sie als NFS- oder CIFS-Freigabe einzubinden. Denn in diesem Fall funktionieren einige LVM-Befehle, wie beispielsweise `resize` und `extend`, möglicherweise nicht wie erwartet, wenn Sie versuchen, den Speicherplatz zu erweitern.

8. Stellen Sie sicher, dass Eigentümer (mysql) und Gruppe (root) des `/opt/netapp/data`Verzeichnisses unverändert sind:

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

   Das System gibt eine Bestätigung zurück, die in etwa wie folgt aussieht:

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

9. Bei aktiviertem SE Linux muss der Kontext für das `/opt/netapp/data`Verzeichnis weiterhin auf mysqld_db_t gesetzt sein:

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

      Das System gibt eine Bestätigung zurück, die in etwa wie folgt aussieht:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Zum Vermeiden künftiger Datenbankfehler ist die überflüssige Datei abc zu löschen.
11. Kopieren des Inhalts von backup-data zurück in das erweiterte `/opt/netapp/data` Verzeichnis:

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

12. Wenn SE Linux aktiviert ist, ist der folgende Befehl auszuführen:

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

13. Start des MySQL-Dienstes:

```
systemctl start mysqld
```

14. Nach dem Start des MySQL-Service erfolgt der Start der Services ocie und ocieau in der angegebenen Reihenfolge:

```
systemctl start ocie ocieau
```

15. Nachdem alle Services gestartet sind, kann der Sicherungsordner `/backup-data` gelöscht werden:

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

Hinzufügen von Speicherplatz zur Datenfestplatte auf einer VMware Virtual Machine in Active IQ Unified Manager

Wenn Sie den Speicherplatz auf der Datenfestplatte für die Unified Manager Datenbank erhöhen müssen, können Sie nach der Installation Kapazität hinzufügen, indem Sie den Festplattenspeicher über die Unified Manager Wartungs-Managementplattform vergrößern.

Bevor Sie beginnen

- Sie müssen Zugriff auf den vSphere Client haben.
- Die virtuelle Maschine darf keine lokal gespeicherten Snapshots enthalten.
- Sie benötigen die Zugangsdaten für den Wartungsbenutzer.

Wir empfehlen Ihnen, Ihre virtuelle Maschine zu sichern, bevor Sie die Größe der virtuellen Festplatten erhöhen.

Schritte

1. Im vSphere Client können Sie die virtuelle Maschine Unified Manager auswählen und dann die Festplattenkapazität für Daten `disk 3` erweitern. Einzelheiten sind der VMware Dokumentation zu entnehmen.

   In seltenen Fällen verwendet das Unified Manager Deployment „Festplatte 2“ statt „Festplatte 3“ als Datenfestplatte. Falls dies in Ihrem Deployment auftritt, empfiehlt sich eine Vergrößerung des Speicherplatzes der größeren Festplatte. Die Datenfestplatte verfügt stets über mehr Speicherplatz als die andere Festplatte.

2. Im vSphere Client werden die virtuelle Maschine Unified Manager und anschließend die Registerkarte **Console** ausgewählt.
3. Im Fenster der Managementplattform erfolgt anschließend die Anmeldung an der Wartungskonsole mit Ihrem Benutzernamen und Passwort.
4. Im Hauptmenü erfolgt die Eingabe der Nummer für die Option **Systemkonfiguration**.
5. Im Menü „Systemkonfiguration“ wird die Zahl für die Option **Datenträgergröße erhöhen** eingegeben.

Hinzufügen von Speicherplatz zum logischen Laufwerk auf einem Windows-Server in Active IQ Unified Manager

Wenn eine Vergrößerung des Speicherplatzes für die Unified Manager Datenbank erforderlich ist, kann die Kapazität des logischen Laufwerks erweitert werden, auf dem Unified Manager installiert ist.

Bevor Sie beginnen

Sie benötigen Windows-Administratorrechte.

Wir empfehlen Ihnen, die Unified Manager Datenbank zu sichern, bevor Sie Speicherplatz hinzufügen.

Schritte

1. Die Anmeldung als Administrator auf dem Windows-Server, dem zusätzlicher Festplattenspeicher hinzugefügt werden soll, ist erforderlich.
2. Im Folgenden ist der Schritt für die Methode zum Hinzufügen von mehr Platz aufgeführt:

Option	Beschreibung
Auf einem physischen Server sollte die Kapazität des logischen Laufwerks erhöht werden, auf dem der Unified Manager server installiert ist.	Die Schritte sind im Microsoft-Thema beschrieben: "Erweitern eines Basisvolumens"
Auf einem physischen Server wird eine Festplatte hinzugefügt.	Die Schritte sind im Microsoft-Thema beschrieben: "Hinzufügen von Festplatten"
Auf einer virtuellen Maschine die Größe einer Festplattenpartition erhöhen.	Die Schritte im VMware-Thema: "Vergrößern einer Festplattenpartition"

Benutzerzugriff verwalten

Benutzer hinzufügen

Hinzufügen von Benutzern in Active IQ Unified Manager

Sie können lokale Benutzer oder Datenbankbenutzer über die Seite „Benutzer“ hinzufügen. Außerdem können Sie Remote-Benutzer oder Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Diesen Benutzern können Sie Rollen zuweisen, und auf Grundlage der Berechtigungen dieser Rollen können Benutzer mit Unified Manager die Storage Objekte und Daten managen oder die Daten in einer Datenbank anzeigen.

Bevor Sie beginnen

- Sie benötigen die Rolle des Anwendungsadministrators.
- Um einen Remote-Benutzer oder eine Remote-Gruppe hinzuzufügen, müssen Sie die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsserver konfiguriert haben.
- Wenn Sie die SAML-Authentifizierung so konfigurieren möchten, dass ein Identitätsanbieter (IdP) die Benutzer authentifiziert, die auf die grafische Benutzeroberfläche zugreifen, sollten Sie darauf achten, dass diese Benutzer als “remote” Benutzer definiert sind.

  Der Zugriff auf die Benutzeroberfläche ist für Benutzer vom Typ “local” oder “maintenance” nicht gestattet, wenn die SAML-Authentifizierung aktiviert ist.

Wenn Sie eine Gruppe aus Windows Active Directory hinzufügen, können sich alle direkten Mitglieder und verschachtelten Untergruppen bei Unified Manager authentifizieren, sofern verschachtelte Untergruppen nicht deaktiviert sind. Wenn Sie eine Gruppe aus OpenLDAP oder anderen Authentifizierungs-Services hinzufügen, können sich nur die direkten Mitglieder dieser Gruppe bei Unified Manager authentifizieren.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ erfolgt ein Klick auf **Hinzufügen**.
3. Im Dialogfeld „Benutzer hinzufügen“ erfolgt die Auswahl des Benutzertyps, den Sie hinzufügen möchten, sowie die Eingabe der erforderlichen Informationen.

   Bei der Eingabe der erforderlichen Benutzerinformationen müssen Sie eine E-Mail-Adresse angeben, die für diesen Benutzer eindeutig ist. E-Mail-Adressen, die von mehreren Benutzern gemeinsam genutzt werden, dürfen nicht angegeben werden.

4. Klicken Sie auf **Add**.

Erstellen eines Datenbankbenutzers in Active IQ Unified Manager

Um eine Verbindung zwischen Workflow Automation und Unified Manager zu unterstützen oder auf Datenbankansichten zuzugreifen, müssen Sie zunächst in der Unified Manager web UI einen Datenbankbenutzer mit der Rolle Integration Schema oder Report Schema erstellen.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Datenbankbenutzer ermöglichen die Integration mit Workflow Automation und den Zugriff auf

berichtsspezifische Datenbankansichten. Datenbankbenutzer haben keinen Zugriff auf die Web-UI von Unified Manager oder die Wartungs-Managementplattform und können keine API-Aufrufe ausführen.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ wählen Sie **Hinzufügen** aus.
3. Im Dialogfeld „Benutzer hinzufügen“ ist in der Dropdown-Liste „Typ“ die Option „Datenbankbenutzer“ auszuwählen.
4. Für den Datenbankbenutzer werden ein Name und ein Passwort eingegeben.
5. In der Dropdown-Liste **Rolle** wird die passende Rolle gewählt.

Wenn Sie…	Diese Rolle auswählen
Verbinden von Unified Manager mit Workflow Automation	Integrationsschema
Zugriff auf Berichte und andere Datenbankansichten	Berichtsschema

6. Klicken Sie auf **Add**.

Benutzereinstellungen in Active IQ Unified Manager bearbeiten

Sie können die Benutzereinstellungen, wie E-Mail-Adresse und Rolle, bearbeiten, die für jeden Benutzer festgelegt sind. Beispielsweise können Sie die Rolle eines Benutzers ändern, der ein Storage-Operator ist, und dem Benutzer Storage-Administratorrechte zuweisen.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Wenn Sie die einem Benutzer zugewiesene Rolle ändern, werden die Änderungen übernommen, sobald eine der folgenden Aktionen eintritt:

- Der Benutzer meldet sich ab und wieder bei Unified Manager an.
- Die Sitzungszeitüberschreitung von 24 Stunden ist erreicht.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ den Benutzer auswählen, dessen Einstellungen bearbeitet werden sollen, und auf **Edit** klicken.
3. Im Dialogfeld „Benutzer bearbeiten“ können Sie die für den Benutzer festgelegten Einstellungen bearbeiten.
4. Auf **Speichern** klicken.

Benutzer in Active IQ Unified Manager anzeigen

Auf der Seite „Benutzer“ kann die Liste der Benutzer angezeigt werden, die Storage Objekte und Daten mit Unified Manager managen. Dort können Details zu den Benutzern

angezeigt werden, z. B. Benutzername, Benutzertyp, E-Mail-Adresse und die den Benutzern zugewiesene Rolle.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritt

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.

Löschen von Benutzern oder Gruppen in Active IQ Unified Manager

Sie können einen oder mehrere Benutzer aus der Datenbank des Managementservers löschen, um bestimmten Benutzern den Zugriff auf Unified Manager zu verweigern. Sie können auch Gruppen löschen, sodass alle Benutzer dieser Gruppe keinen Zugriff mehr auf den Managementserver haben.

Bevor Sie beginnen

- Wenn Sie Remote-Gruppen löschen, müssen Sie die den Benutzern der Remote-Gruppen zugewiesenen Ereignisse zuvor neu zugewiesen haben.

  Wenn Sie lokale Benutzer oder Remote-Benutzer löschen, wird die Zuweisung der diesen Benutzern zugewiesenen Ereignisse automatisch aufgehoben.

- Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ erfolgt die Auswahl der Benutzer oder Gruppen, die gelöscht werden sollen; anschließend erfolgt ein Klick auf **Löschen**.
3. Zum Bestätigen der Löschung auf **Ja** klicken.

Informationen zur rollenbasierten Zugriffssteuerung in Active IQ Unified Manager

RBAC (rollenbasierte Zugriffssteuerung) bietet die Möglichkeit, zu steuern, wer Zugriff auf verschiedene Funktionen und Ressourcen auf dem Active IQ Unified Manager Server hat. RBAC ermöglicht Administratoren die Verwaltung von Benutzergruppen durch die Definition von Rollen. Wenn der Zugriff auf bestimmte Funktionen auf ausgewählte Administratoren beschränkt werden muss, müssen für diese Administratorkonten eingerichtet werden. Wenn die Informationen, die Administratoren anzeigen können, und die Vorgänge, die sie ausführen können, eingeschränkt werden sollen, müssen den erstellten Administratorkonten Rollen zugewiesen werden.

Der Verwaltungsserver verwendet rollenbasierte Zugriffskontrolle (RBAC) für die Benutzeranmeldung und Rollenberechtigungen. Wenn Sie die Standardeinstellungen des Verwaltungsservers für den administrativen Benutzerzugriff nicht geändert haben, müssen Sie sich nicht anmelden, um diese anzuzeigen.

Wenn Sie einen Vorgang initiieren, der bestimmte Berechtigungen erfordert, fordert der Managementserver Sie zur Anmeldung auf. Um beispielsweise Administratorkonten zu erstellen, müssen Sie sich mit einem Konto mit Zugriff als Application Administrator anmelden.

Informationen zu Benutzertypen in Active IQ Unified Manager

Ein Benutzertyp legt die Art des Benutzerkontos fest und umfasst Remote-Benutzer, Remote-Gruppen, lokale Benutzer, Datenbankbenutzer und Wartungsbenutzer. Jeder dieser Typen hat eine eigene Rolle, die ein Benutzer mit der Rolle „Administrator“ zuweist.

Die Unified Manager Benutzertypen sind wie folgt:

- **Wartungsbenutzer**

  Wird bei der Erstkonfiguration von Unified Manager erstellt. Der Wartungsbenutzer erstellt anschließend weitere Benutzer und weist ihnen Rollen zu. Der Wartungsbenutzer ist außerdem der einzige Benutzer mit Zugriff auf die Managementplattform. Wenn Unified Manager auf einem Red Hat Enterprise Linux-System installiert wird, erhält der Wartungsbenutzer den Benutzernamen “umadmin.”

- **Lokaler Benutzer**

  Greift auf die Unified Manager-Benutzeroberfläche zu und führt je nach der vom Wartungsbenutzer oder von einem Benutzer mit der Rolle "Application Administrator" zugewiesenen Rolle Funktionen aus.

- **Remote-Gruppe**

  Eine Gruppe von Benutzern, die mit den auf dem Authentifizierungsserver gespeicherten Anmeldedaten auf die Unified Manager UI zugreifen. Der Name dieses Kontos sollte mit dem Namen einer auf dem Authentifizierungsserver gespeicherten Gruppe übereinstimmen. Alle Benutzer innerhalb der Remote-Gruppe erhalten mit ihren individuellen Benutzeranmeldeinformationen Zugriff auf die Unified Manager UI. Remote-Gruppen können entsprechend ihren zugewiesenen Rollen Funktionen ausführen.

- **Remote-Benutzer**

  Der Zugriff auf die Unified Manager UI erfolgt mithilfe der Anmeldedaten, die auf dem Authentifizierungsserver gespeichert sind. Ein Remote-Benutzer führt Funktionen basierend auf der Rolle aus, die ihm vom Wartungsbenutzer oder von einem Benutzer mit der Rolle „Application Administrator“ zugewiesen wurde.

- **Datenbankbenutzer**

  Verfügt über Lesezugriff auf Daten in der Unified Manager Datenbank, hat keinen Zugriff auf die Unified Manager Weboberfläche oder die Wartungsmanagementplattform und kann keine API-Aufrufe ausführen.

Informationen zu Benutzerrollen in Active IQ Unified Manager

Der Wartungsbenutzer oder Anwendungsadministrator weist jedem Benutzer eine Rolle zu. Jede Rolle beinhaltet bestimmte Berechtigungen. Der Umfang der Aktivitäten, die Sie im Unified Manager ausführen können, hängt von Ihrer zugewiesenen Rolle und den damit verbundenen Berechtigungen ab.

Unified Manager umfasst die folgenden vordefinierten Benutzerrollen:

- **Operator**

  Zeigt Storage-Systeminformationen und andere von Unified Manager erfasste Daten an, einschließlich

Verlaufsdaten und Kapazitätstrends. Diese Rolle ermöglicht dem Storage-Operator, Ereignisse anzuzeigen, zuzuweisen, zu bestätigen, zu beheben und mit Notizen zu versehen.

- **Storage-Administrator**

  Konfiguriert Storage-Managementvorgänge in Unified Manager. Diese Rolle ermöglicht dem Storage-Administrator die Konfiguration von Schwellenwerten sowie die Erstellung von Warnungen und anderen spezifischen Optionen und Richtlinien für das Storage-Management.

- **Anwendungsadministrator**

  Konfiguriert Einstellungen, die nicht mit dem Storage-Management zusammenhängen. Diese Rolle ermöglicht die Verwaltung von Benutzern, Sicherheitszertifikaten, Datenbankzugriff und administrativen Optionen, einschließlich Authentifizierung, SMTP, Netzwerk und AutoSupport.

  ⓘ Bei der Installation von Unified Manager auf Linux-Systemen erhält der erste Benutzer mit der Rolle des Anwendungsadministrators automatisch den Namen “umadmin”.

- **Integrationsschema**

  Diese Rolle ermöglicht schreibgeschützten Zugriff auf Unified Manager Datenbankansichten zur Integration von Unified Manager mit OnCommand Workflow Automation (WFA).

- **Berichtsschema**

  Diese Rolle ermöglicht schreibgeschützten Zugriff auf Berichte und andere Datenbankansichten direkt aus der Unified Manager Datenbank. Zu den einsehbaren Datenbanken gehören:

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

Informationen zu Benutzerrollen und Berechtigungen in Active IQ Unified Manager

Anhand Ihrer zugewiesenen Benutzerrolle können Sie ermitteln, welche Operationen Sie im Unified Manager durchführen können.

Die folgende Tabelle zeigt die Funktionen, die jede Benutzerrolle ausführen kann:

Funktion	Operator	Storage-Administrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Anzeigen von Informationen zum Storage-System	•	•	•	•	•

Funktion	Operator	Storage-Administrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Andere Daten wie z. B. Verläufe und Kapazitätstrends lassen sich anzeigen.	•	•	•	•	•
Ereignisse anzeigen, zuweisen und beheben	•	•	•		
Storage-Service-Objekte wie SVM-Zuordnungen und Ressourcenpools anzeigen	•	•	•		
Anzeige von Schwellenwertrichtlinien	•	•	•		
Management von Storage-Serviceobjekten wie SVM-Zuordnungen und Ressourcenpools		•	•		
Warnmeldungen definieren		•	•		
Storage-Managementoptionen managen		•	•		
Storage-Managementrichtlinien managen		•	•		
Benutzer verwalten			•		
Administrative Optionen managen			•		
Definition von Schwellenwertrichtlinien			•		
Datenbankzugriff managen			•		

Funktion	Operator	Storage-Administrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Integration mit WFA managen und Zugriff auf die Datenbankansichten gewähren				•	
Berichte planen und speichern		•	•		
Ausführung von “Fix It”-Vorgängen über Management Actions		•	•		
Bereitstellung von schreibgeschütztem Zugriff auf Datenbankansichten					•

Verwalten der SAML-Authentifizierungseinstellungen

SAML Authentifizierung in Active IQ Unified Manager ist aktiviert

Nachdem Sie die Einstellungen für die Remote-Authentifizierung konfiguriert haben, können Sie die Authentifizierung mit Security Assertion Markup Language (SAML) aktivieren, sodass Remote-Benutzer von einem sicheren Identitätsanbieter (IdP) authentifiziert werden, bevor sie auf die Web-Benutzeroberfläche von Unified Manager zugreifen können.

Nach der Aktivierung der SAML-Authentifizierung haben nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager. Lokale Benutzer und Wartungsbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Managementplattform für die Wartung zugreifen.

Verwendung eines Identitätsanbieters in Active IQ Unified Manager

Wenn Unified Manager so konfiguriert wird, dass ein Identitätsanbieter (IdP) die SAML-Authentifizierung für alle Remote-Benutzer durchführt, müssen einige erforderliche Konfigurationseinstellungen beachtet werden, damit die Verbindung zu Unified Manager erfolgreich hergestellt werden kann.

Sie müssen die Unified Manager URI und die Metadaten in den IdP-Server eingeben. Diese Informationen können Sie auf der Unified Manager SAML-Authentifizierungsseite kopieren. Unified Manager gilt im Standard Security Assertion Markup Language (SAML) als Serviceprovider (SP).

Unterstützte Verschlüsselungsstandards

- Advanced Encryption Standard (AES): AES-128 und AES-256
- Sicherer Hash-Algorithmus (SHA): SHA-1 und SHA-256

Validierte Identitätsanbieter

- Shibboleth
- Active Directory Federation Services (ADFS)

ADFS Konfigurationsanforderungen

- Sie müssen drei Anspruchsregeln in der folgenden Reihenfolge definieren, die erforderlich sind, damit Unified Manager ADFS SAML-Antworten für diesen Vertrauensstellungseintrag der vertrauenden Seite analysieren kann.

Claim-Regel	Wert
SAM-Kontoname	Name-ID
SAM-Kontoname	urn:oid:0.9.2342.19200300.100.1.1
Tokengruppen — Unqualifizierter Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Sie müssen das Authentifizierungsverfahren auf “Forms Authentication” festlegen, da Benutzer sonst beim Abmelden von Unified Manager eine Fehlermeldung erhalten können. Die folgenden Schritte sind erforderlich:
  a. Die ADFS Management Console wird geöffnet.
  b. In der linken Baumansicht den Ordner „Authentifizierungsrichtlinien“ auswählen.
  c. Rechts unter „Aktionen“ befindet sich die Option „Globale primäre Authentifizierungsrichtlinie bearbeiten“.
  d. Als Authentifizierungsverfahren für das Intranet wird statt der Standardeinstellung “Windows Authentication” die Option “Forms Authentication” verwendet.
- In einigen Fällen wird die Anmeldung über den IdP abgelehnt, wenn das Sicherheitszertifikat des Unified Manager CA-signiert ist. Es gibt zwei Lösungsansätze für dieses Problem:
  - Im Link finden Sie Anweisungen zum Deaktivieren der Widerrufsprüfung auf dem ADFS-Server für verkettete CA-Zertifikate der zugeordneten Relying Party:

    "Widerrufsprüfung pro Relying Party Trust deaktivieren"

  - Der CA-Server muss sich innerhalb des ADFS-Servers befinden, um die Zertifikatsanforderung des Unified Manager Servers zu signieren.

Weitere Konfigurationsanforderungen

- Die Taktabweichung von Unified Manager ist auf 5 Minuten eingestellt, daher darf die Zeitdifferenz zwischen dem IdP-Server und dem Unified Manager-Server nicht mehr als 5 Minuten betragen, da die Authentifizierung sonst fehlschlägt.

SAML Authentifizierung in Active IQ Unified Manager ist aktiviert

Sie können die Security Assertion Markup Language (SAML) Authentifizierung aktivieren, sodass Remote-Benutzer von einem sicheren Identitätsanbieter (IdP) authentifiziert werden, bevor sie auf die Unified Manager Weboberfläche zugreifen können.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung konfiguriert und überprüft haben, dass sie erfolgreich ist.
- Sie müssen mindestens einen Remote User oder eine Remote Group mit der Rolle Application Administrator erstellt haben.
- Der Identitätsanbieter (IdP) muss von Unified Manager unterstützt werden und konfiguriert sein.
- Sie benötigen die IdP-URL und die Metadaten.
- Sie benötigen Zugriff auf den IdP-Server.

Nachdem Sie die SAML-Authentifizierung in Unified Manager aktiviert haben, können Benutzer erst dann auf die grafische Benutzeroberfläche zugreifen, wenn der IdP mit den Hostinformationen des Unified Manager Servers konfiguriert wurde. Daher ist es erforderlich, beide Teile der Verbindung abzuschließen, bevor der Konfigurationsprozess gestartet wird. Der IdP kann vor oder nach der Konfiguration von Unified Manager eingerichtet werden.

Nach der Aktivierung der SAML-Authentifizierung haben nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche des Unified Manager. Lokale Benutzer und Wartungsbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Managementplattform, die Unified Manager-Befehle oder die ZAPIs zugreifen.

Unified Manager wird automatisch neu gestartet, nachdem Sie die SAML-Konfiguration auf dieser Seite abgeschlossen haben.

Schritte

1. Im linken Navigationsbereich wählen Sie **General** > **SAML Authentication** aus.
2. Das Kontrollkästchen **SAML-Authentifizierung aktivieren** ist auszuwählen.

   Die für die Konfiguration der IdP-Verbindung erforderlichen Felder werden angezeigt.

3. Einzugeben sind die IdP URI und die IdP Metadaten, die für die Verbindung des Unified Manager Servers mit dem IdP Server erforderlich sind.

   Wenn der IdP-Server direkt vom Unified Manager Server aus erreichbar ist, können Sie nach Eingabe der IdP URI auf die Schaltfläche **Fetch IdP Metadata** klicken, um das Feld „IdP Metadata“ automatisch zu füllen.

4. Die Host-Metadaten-URI von Unified Manager kann kopiert oder die Host-Metadaten können in einer XML-Textdatei gespeichert werden.

   Sie können den IdP-Server jetzt mit diesen Informationen konfigurieren.

5. Auf **Speichern** klicken.

   Ein Meldungsfeld erscheint zur Bestätigung, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

6. Nach einem Klick auf **Confirm and Logout** wird Unified Manager neu gestartet.

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche des Unified Manager zuzugreifen, müssen sie ihre Anmeldeinformationen auf der IdP-Anmeldeseite anstatt auf der Unified Manager-Anmeldeseite eingeben.

Falls dies noch nicht geschehen ist, sind für den Abschluss der Konfiguration der Zugriff auf Ihren IdP sowie die Eingabe der URI und der Metadaten des Unified Manager Servers erforderlich.



Wenn Sie ADFS als Identitätsanbieter verwenden, beachtet die Unified Manager GUI die ADFS-Zeitüberschreitung nicht und funktioniert weiter, bis die Unified Manager Sitzungs-Zeitüberschreitung erreicht ist. Die Zeitüberschreitung der GUI-Sitzung kann durch Klicken auf **General** > **Feature Settings** > **Inactivity Timeout** geändert werden.

Änderung des SAML Authentifizierungs-Identitätsanbieters in Active IQ Unified Manager

Sie können den Identitätsanbieter (IdP) ändern, den Unified Manager zur Authentifizierung von Remote-Benutzern verwendet.

Bevor Sie beginnen

- Sie benötigen die IdP-URL und die Metadaten.
- Sie benötigen Zugriff auf den Identitätsanbieter (IdP).

Der neue IdP lässt sich vor oder nach der Konfiguration von Unified Manager konfigurieren.

Schritte

1. Im linken Navigationsbereich wählen Sie **General** > **SAML Authentication** aus.
2. Einzugeben sind die neue IdP URI sowie die IdP-Metadaten, die für die Verbindung des Unified Manager server mit dem IdP erforderlich sind.

   Wenn der IdP direkt vom Unified Manager Server aus erreichbar ist, können Sie nach Eingabe der IdP URL auf die Schaltfläche **Fetch IdP Metadata** klicken, um das Feld „IdP Metadata“ automatisch auszufüllen.

3. Sie können den Unified Manager Metadaten-URI kopieren oder die Metadaten in einer XML-Textdatei speichern.
4. Im nächsten Schritt erfolgt die Auswahl von **Konfiguration speichern**.

   Ein Meldungsfeld wird angezeigt, um zu bestätigen, dass Sie die Konfiguration ändern möchten.

5. Klicken Sie auf **OK**.

Zum Abschließen der Konfiguration auf den neuen IdP zugreifen und die Unified Manager Server-URI sowie die Metadaten eingeben.

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche des Unified Manager zuzugreifen, müssen sie ihre Anmeldeinformationen auf der neuen IdP-Anmeldeseite anstatt auf der alten IdP-Anmeldeseite eingeben.

Aktualisierung der SAML-Authentifizierungseinstellungen nach einer Änderung des Active IQ Unified Manager Sicherheitszertifikats

Jede Änderung des auf dem Unified Manager Server installierten HTTPS-Sicherheitszertifikats erfordert eine Aktualisierung der SAML Authentifizierungskonfigurationseinstellungen. Das Zertifikat wird aktualisiert, wenn Sie das Hostsystem umbenennen, ihm eine neue IP-Adresse zuweisen oder das Sicherheitszertifikat für das System manuell ändern.

Nach der Änderung des Sicherheitszertifikats und dem Neustart des Unified Manager Servers funktioniert die SAML Authentifizierung nicht mehr, und Benutzer können nicht auf die grafische Benutzeroberfläche des Unified Manager zugreifen. Um den Zugriff auf die Benutzeroberfläche wiederherzustellen, müssen Sie die SAML Authentifizierungseinstellungen sowohl auf dem IdP Server als auch auf dem Unified Manager Server aktualisieren.

Schritte

1. Bei der Wartungs-Managementplattform erfolgt die Anmeldung.
2. Im **Hauptmenü** erfolgt die Eingabe der Nummer für die Option **SAML-Authentifizierung deaktivieren**.

   Es erscheint eine Meldung zur Bestätigung, dass Sie die SAML-Authentifizierung deaktivieren und Unified Manager neu starten möchten.

3. Die Unified Manager Benutzeroberfläche kann über den aktualisierten FQDN oder die IP-Adresse aufgerufen werden. Dabei wird das aktualisierte Serverzertifikat im Browser akzeptiert, und die Anmeldung erfolgt mit den Anmeldedaten des Wartungsbenutzers.
4. Die Konfiguration der IdP-Verbindung erfolgt auf der Seite **Setup/Authentifizierung** über die Registerkarte **SAML-Authentifizierung**.
5. Die Host-Metadaten-URI von Unified Manager kann kopiert oder die Host-Metadaten können in einer XML-Textdatei gespeichert werden.
6. Auf **Speichern** klicken.

   Ein Meldungsfeld erscheint zur Bestätigung, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

7. Nach einem Klick auf **Confirm and Logout** wird Unified Manager neu gestartet.
8. Zum Abschluss der Konfiguration erfolgt auf dem IdP-Server die Eingabe der URI des Unified Manager-Servers und der Metadaten.

Identitätsanbieter	Konfigurationsschritte
ADFS	a. In der ADFS-Management-GUI erfolgt das Löschen des vorhandenen Eintrags für die Vertrauensstellung der vertrauenden Seite. b. Das Hinzufügen eines neuen Eintrags für die Vertrauensstellung der vertrauenden Seite erfolgt mithilfe des `saml_sp_metadata.xml` aktualisierten Unified Manager Servers. c. Definition der drei Anspruchsregeln, die Unified Manager benötigt, um ADFS SAML-Antworten für diesen Eintrag der Vertrauensstellung der vertrauenden Seite zu analysieren. d. Ein Neustart des ADFS Windows Service ist erforderlich.
Shibboleth	a. Der neue FQDN des Unified Manager Servers ist in den `attribute-filter.xml` und `relying-party.xml` Dateien zu aktualisieren. b. Nach dem Neustart des Apache Tomcat Webservers ist zu warten, bis Port 8005 online ist.

9. Nach der Anmeldung bei Unified Manager sollte überprüft werden, ob die SAML-Authentifizierung über Ihren IdP wie erwartet funktioniert.

SAML Authentifizierung in Active IQ Unified Manager deaktivieren

Sie können die SAML Authentifizierung deaktivieren, wenn die Authentifizierung von Remote-Benutzern über einen sicheren Identitätsanbieter (IdP) beendet werden soll, bevor sie sich bei der Unified Manager Weboberfläche anmelden können. Wenn die SAML Authentifizierung deaktiviert ist, übernehmen die konfigurierten Verzeichnisdienstanbieter, wie z. B. Active Directory oder LDAP, die Anmeldeauthentifizierung.

Nach der Deaktivierung der SAML-Authentifizierung können neben den konfigurierten Remote-Benutzern auch lokale Benutzer und Wartungsbenutzer auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch über die Unified Manager Managementplattform deaktivieren, wenn Sie keinen Zugriff auf die grafische Benutzeroberfläche haben.

Unified Manager wird nach der Deaktivierung der SAML-Authentifizierung automatisch neu gestartet.

Schritte

1. Im linken Navigationsbereich wählen Sie **General** > **SAML Authentication** aus.
2. Das Häkchen im Kontrollkästchen **SAML-Authentifizierung aktivieren** wird entfernt.
3. Auf **Speichern** klicken.

Ein Meldungsfeld erscheint zur Bestätigung, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

4. Nach einem Klick auf **Confirm and Logout** wird Unified Manager neu gestartet.

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche des Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der Unified Manager Anmeldeseite statt auf der IdP Anmeldeseite ein.

Sie greifen auf Ihren IdP zu und löschen die Unified Manager Server URI und die Metadaten.

Die SAML Authentifizierung wird über die Active IQ Unified Manager Wartungskonsole deaktiviert.

Möglicherweise ist es erforderlich, die SAML Authentifizierung über die Managementplattform zu deaktivieren, wenn kein Zugriff auf die Unified Manager GUI besteht. Dies kann bei Fehlkonfigurationen oder wenn der Identitätsanbieter (IdP) nicht erreichbar ist, der Fall sein.

Bevor Sie beginnen

Sie müssen als Wartungsbenutzer Zugriff auf die Managementplattform haben.

Wenn die SAML-Authentifizierung deaktiviert ist, übernehmen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP die Anmeldeauthentifizierung. Lokale Benutzer und Wartungsbenutzer können dann zusätzlich zu den konfigurierten Remote-Benutzern auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML Authentifizierung auch auf der Seite „Setup/Authentication“ in der UI deaktivieren.

Unified Manager wird nach der Deaktivierung der SAML-Authentifizierung automatisch neu gestartet.

Schritte

1. Bei der Wartungs-Managementplattform erfolgt die Anmeldung.
2. Im **Hauptmenü** erfolgt die Eingabe der Nummer für die Option **SAML-Authentifizierung deaktivieren**.

   Es erscheint eine Meldung zur Bestätigung, dass Sie die SAML-Authentifizierung deaktivieren und Unified Manager neu starten möchten.

3. Nach Eingabe von **y** und Drücken der Eingabetaste wird Unified Manager neu gestartet.

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche des Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der Unified Manager Anmeldeseite statt auf der IdP Anmeldeseite ein.

Falls erforderlich, können Sie auf Ihren IdP zugreifen und die Unified Manager Server-URL sowie die Metadaten löschen.

Die SAML Authentifizierungsseite in Active IQ Unified Manager kann verwendet werden

Auf der Seite „SAML-Authentifizierung“ können Sie Unified Manager so konfigurieren, dass Remote-Benutzer mithilfe von SAML über einen sicheren Identitätsanbieter (IdP)

authentifiziert werden, bevor sie sich bei der Unified Manager Weboberfläche anmelden können.

- Sie müssen über die Rolle „Application Administrator“ verfügen, um die SAML-Konfiguration zu erstellen oder zu ändern.
- Sie müssen die Remote-Authentifizierung konfiguriert haben.
- Mindestens ein Remote-Benutzer oder eine Remote-Gruppe muss konfiguriert sein.

Nachdem die Remote-Authentifizierung und die Remote-Benutzer konfiguriert wurden, können Sie durch Aktivieren des Kontrollkästchens „SAML-Authentifizierung aktivieren“ die Authentifizierung mithilfe eines sicheren Identitätsanbieters aktivieren.

- **IdP-URI**

  Die URI für den Zugriff auf den IdP vom Unified Manager Server. Beispiel-URIs sind unten aufgeführt.

  ADFS Beispiel-URI:

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

  Shibboleth Beispiel-URI:

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

- **IdP-Metadaten**

  Die IdP-Metadaten im XML-Format.

  Wenn die IdP-URL vom Unified Manager Server aus erreichbar ist, können Sie auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um dieses Feld auszufüllen.

- **Hostsystem (FQDN)**

  Der FQDN des Unified Manager Hostsystems, wie er während der Installation definiert wurde. Sie können diesen Wert bei Bedarf ändern.

- **Host-URI**

  Die URI für den Zugriff auf das Unified Manager Hostsystem vom IdP aus.

- **Host-Metadaten**

  Die Metadaten des Hostsystems im XML-Format.

Authentifizierung verwalten

Bearbeiten von Authentifizierungsservern in Active IQ Unified Manager

Sie können den Port ändern, den der Unified Manager Server für die Kommunikation mit Ihrem Authentifizierungsserver verwendet.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Das Kontrollkästchen **Verschachtelte Gruppensuche deaktivieren** muss aktiviert sein.
3. Im Bereich **Authentifizierungsserver** den Authentifizierungsserver auswählen, der bearbeitet werden soll, und anschließend auf **Bearbeiten** klicken.
4. Im Dialogfeld **Authentifizierungsserver bearbeiten** können Sie die Portdetails bearbeiten.
5. Auf **Speichern** klicken.

Authentifizierungsserver in Active IQ Unified Manager löschen

Sie können einen Authentifizierungsserver löschen, wenn Sie verhindern möchten, dass der Unified Manager Server mit dem Authentifizierungsserver kommuniziert. Wenn Sie beispielsweise einen Authentifizierungsserver ändern möchten, mit dem der Verwaltungsserver kommuniziert, können Sie den Authentifizierungsserver löschen und einen neuen Authentifizierungsserver hinzufügen.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Wenn Sie einen Authentifizierungsserver löschen, können Remote-Benutzer oder -Gruppen des Authentifizierungsservers nicht mehr auf Unified Manager zugreifen.

Schritte

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Einen oder mehrere Authentifizierungsserver, die gelöscht werden sollen, auswählen und anschließend auf **Löschen** klicken.
3. Mit **Ja** wird die Löschanfrage bestätigt.

   Wenn die Option **Sichere Verbindung verwenden** aktiviert ist, werden die mit dem Authentifizierungsserver verknüpften Zertifikate zusammen mit dem Authentifizierungsserver gelöscht.

Authentifizierung mit Active Directory oder OpenLDAP in Active IQ Unified Manager

Sie können die Remote Authentifizierung auf dem Management-Server aktivieren und den Management-Server so konfigurieren, dass er mit Ihren Authentifizierungsservern kommuniziert, sodass Benutzer innerhalb der Authentifizierungsserver auf Unified Manager zugreifen können.

Sie können einen der folgenden vordefinierten Authentifizierungsservices verwenden oder Ihren eigenen Authentifizierungsservice angeben:

- Microsoft Active Directory

  Sie können Microsoft Lightweight Directory Services nicht verwenden.

- OpenLDAP

Sie können den erforderlichen Authentifizierungsservice auswählen und die entsprechenden Authentifizierungsserver hinzufügen, um den Remote-Benutzern im Authentifizierungsserver den Zugriff auf Unified Manager zu ermöglichen. Die Anmeldeinformationen für Remote-Benutzer oder -Gruppen werden vom Authentifizierungsserver verwaltet. Der Managementserver verwendet das Lightweight Directory Access Protocol (LDAP), um Remote-Benutzer innerhalb des konfigurierten Authentifizierungsservers zu authentifizieren.

Für lokale Benutzer, die im Unified Manager angelegt werden, verwaltet der Verwaltungsserver eine eigene Datenbank mit Benutzernamen und Passwörtern. Der Verwaltungsserver führt die Authentifizierung durch und verwendet weder Active Directory noch OpenLDAP für die Authentifizierung.

Audit-Logging

Informationen zu Audit-Protokollen in Active IQ Unified Manager

Mithilfe von Revisionsprotokollen lässt sich feststellen, ob die Revisionsprotokolle manipuliert wurden. Alle von einem Benutzer durchgeführten Aktivitäten werden überwacht und in den Revisionsprotokollen protokolliert. Die Audits werden für alle Funktionen der Benutzeroberfläche und der öffentlich zugänglichen APIs von Active IQ Unified Manager durchgeführt.

Mit der **Audit Log: File View** können Sie alle in Ihrem Active IQ Unified Manager verfügbaren Revisionsprotokolldateien anzeigen und darauf zugreifen. Die Dateien in der **Audit Log: File View** sind nach ihrem Erstellungsdatum aufgelistet. Diese Ansicht zeigt Informationen zu allen Revisionsprotokollen an, die seit der Installation oder dem Upgrade bis zum aktuellen Zeitpunkt im System erfasst wurden. Wenn Sie im Unified Manager eine Aktion ausführen, werden die Informationen aktualisiert und sind in den Protokollen verfügbar. Der Status jeder Protokolldatei wird mithilfe des Attributs “File Integrity Status” erfasst, das aktiv überwacht wird, um Manipulationen oder das Löschen der Protokolldatei zu erkennen. Die Revisionsprotokolle können einen der folgenden Status aufweisen, wenn sie im System verfügbar sind:

Status	Beschreibung
AKTIV	Datei, in der Protokolle derzeit protokolliert werden.
NORMAL	Eine inaktive, komprimierte und im System gespeicherte Datei.
MANIPULIERT	Datei, die von einem Benutzer kompromittiert wurde, der die Datei manuell bearbeitet hat.
MANUAL_DELETE	Datei, die ein autorisierter Benutzer gelöscht hat.
ROLLOVER_DELETE	Datei, die aufgrund des auf der Rolling Configuration Policy basierenden Entfernens gelöscht wurde.
UNEXPECTED_DELETE	Datei, die aus unbekannten Gründen gelöscht wurde.

Die Seite „Revisionsprotokoll“ enthält die folgenden Befehlsschaltflächen:

- Konfigurieren
- Löschen
- Download

Mit der Schaltfläche **DELETE** können Sie alle in der Ansicht „Audit Logs“ aufgeführten Revisionsprotokolle löschen. Sie können ein Revisionsprotokoll löschen und optional einen Grund für das Löschen der Datei angeben, was künftig dabei hilft, eine gültige Löschung nachzuvollziehen. In der Spalte REASON werden der Grund zusammen mit dem Namen des Benutzers aufgeführt, der den Löschvorgang durchgeführt hat.

Das Löschen einer Protokolldatei führt dazu, dass die Datei aus dem System gelöscht wird, der Eintrag in der DB-Tabelle jedoch nicht.

Sie können die Revisionsprotokolle aus Active IQ Unified Manager über die Schaltfläche **HERUNTERLADEN** im Bereich „Audit Logs“ herunterladen und die Revisionsprotokolldateien exportieren. Die Dateien, die als „`NORMAL`“ oder „`TAMPERED`“ gekennzeichnet sind, werden in einem komprimierten `.gzip` Format heruntergeladen.

Die Revisionsprotokoll-Dateien werden regelmäßig archiviert und zur späteren Referenz in der Datenbank gespeichert. Vor der Archivierung werden die Revisionsprotokolle digital signiert, um die Sicherheit und Integrität zu wahren.

Wenn ein vollständiges AutoSupport Bundle generiert wird, enthält das Support Bundle sowohl archivierte als auch aktive Revisionsprotokolldateien. Wenn jedoch ein kompaktes Support Bundle generiert wird, enthält es nur die aktiven Revisionsprotokolle. Die archivierten Revisionsprotokolle sind nicht enthalten.

Konfiguration der Audit-Protokolle von Active IQ Unified Manager

Mit der Schaltfläche **Configure** im Abschnitt „Revisionsprotokolle“ lässt sich die Rotationsrichtlinie für Revisionsprotokolldateien konfigurieren und außerdem die Remote Protokollierung für die Revisionsprotokolle aktivieren.

Sie können die Werte in **MAX FILE SIZE** und **AUDIT LOG RETENTION DAYS** entsprechend der gewünschten Datenmenge und -häufigkeit festlegen, die Sie im System speichern möchten. Der Wert im Feld **TOTAL AUDIT LOG SIZE** ist die Größe der gesamten im System vorhandenen Revisionsprotokolldaten. Die Rotationsrichtlinie wird durch die Werte im Feld **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** und **TOTAL AUDIT LOG SIZE** bestimmt. Wenn die Größe der Revisionsprotokoll-Sicherung den in **TOTAL AUDIT LOG SIZE** konfigurierten Wert erreicht, wird die Datei gelöscht, die zuerst archiviert wurde. Das bedeutet, dass die älteste Datei gelöscht wird. Der Dateieintrag bleibt jedoch weiterhin in der Datenbank verfügbar und ist als “Rollover Delete” gekennzeichnet. Der Wert **AUDIT LOG RETENTION DAYS** steht für die Anzahl der Tage, für die die Revisionsprotokolldateien aufbewahrt werden. Jede Datei, die älter ist als der in diesem Feld festgelegte Wert, wird rotiert.

Schritte

1. **Revisionsprotokolle** > > **Konfigurieren** auswählen.
2. Werte für **MAXIMALE DATEIGRÖSSE**, **GESAMTGRÖSSE DES REVISIONSPROTOKOLLS** und **AUFBEWAHRUNGSTAGE DES REVISIONSPROTOKOLLS** werden eingegeben.

   Die Aktivierung der Remote-Protokollierung erfolgt über **Enable Remote Logging**.

Die Remote-Protokollierung von Audit-Protokollen in Active IQ Unified Manager kann aktiviert werden

Sie können im Dialogfeld „Revisionsprotokolle konfigurieren“ das Kontrollkästchen „Remote-Protokollierung aktivieren“ auswählen, um die Remote-Revisionsprotokollierung zu aktivieren. Mit dieser Funktion können Sie Revisionsprotokolle an einen Remote-Syslog-Server übertragen. Dies ermöglicht Ihnen, Ihre Revisionsprotokolle auch bei begrenztem Speicherplatz zu managen.

Die Remote-Protokollierung von Revisionsprotokollen bietet eine manipulationssichere Sicherung für den Fall, dass die Revisionsprotokoll-Dateien auf dem Active IQ Unified Manager Server manipuliert werden.

Schritte

1. Im Dialogfeld **Revisionsprotokolle konfigurieren** kann das Kontrollkästchen **Remote-Protokollierung aktivieren** ausgewählt werden.

   Es werden zusätzliche Felder zum Konfigurieren der Remote-Protokollierung angezeigt.

2. Für die Verbindung mit dem gewünschten Remote-Server werden **HOSTNAME** und **PORT** eingegeben.
3. Im Feld **SERVER CA CERTIFICATE** erfolgt die Auswahl eines öffentlichen Zertifikats des Zielservers über **BROWSE**.

   Das Zertifikat sollte im `.pem` Format hochgeladen werden. Dieses Zertifikat sollte vom Ziel Syslog-Server bezogen werden und darf nicht abgelaufen sein. Das Zertifikat sollte den ausgewählten “hostname” als Teil des `SubjectAltName`(SAN)-Attributs enthalten.

4. Einzugeben sind die Werte für die folgenden Felder: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   Die Werte sollten für diese Felder in Millisekunden angegeben werden.

5. Die Auswahl des gewünschten Syslog-Formats und der TLS Protokollversion erfolgt in den Feldern **FORMAT** und **PROTOCOL**.
6. Wenn der Ziel-Syslog-Server eine zertifikatbasierte Authentifizierung erfordert, ist das Kontrollkästchen **Client-Authentifizierung aktivieren** auszuwählen.

   Sie müssen das Zertifikat für die Client-Authentifizierung herunterladen und vor dem Speichern der Konfiguration des Revisionsprotokolls auf den Syslog-Server hochladen, andernfalls schlägt die Verbindung fehl. Je nach Typ des Syslog-Servers müssen Sie möglicherweise einen Hash des Zertifikats für die Client-Authentifizierung erstellen.

   Beispiel: syslog-ng erfordert, dass ein <hash> des Zertifikats mit dem Befehl `openssl x509 -noout -hash -in cert.pem` erstellt wird. Anschließend sollten Sie das Client-Authentifizierungs-Zertifikat symbolisch mit einer Datei verknüpfen, die nach dem <hash> .0 benannt ist.

7. **Speichern** konfiguriert die Verbindung mit Ihrem Server und aktiviert die Remote-Protokollierung.

   Sie werden zur Seite „Revisionsprotokolle“ weitergeleitet.

> Der Wert für **Verbindungs-Zeitüberschreitung** kann sich auf die Konfiguration auswirken. Wenn die Konfiguration länger für eine Antwort benötigt als der definierte Wert, kann dies aufgrund eines Verbindungsfehlers zu einem Konfigurationsfehler führen. Für den Aufbau einer erfolgreichen Verbindung sollte der Wert für **Verbindungs-Zeitüberschreitung** erhöht und die Konfiguration erneut versucht werden.

Die Seite „Remote-Authentifizierung“ in Active IQ Unified Manager

Auf der Seite „Remote-Authentifizierung“ kann Unified Manager so konfiguriert werden, dass es mit Ihrem Authentifizierungsserver kommuniziert, um Remote-Benutzer zu authentifizieren, die versuchen, sich bei der Unified Manager Web-Benutzeroberfläche anzumelden.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Nachdem Sie das Kontrollkästchen „Enable remote authentication“ aktiviert haben, können Sie die Remote-Authentifizierung mithilfe eines Authentifizierungsservers aktivieren.

- **Authentifizierungsdienst**

  Ermöglicht die Konfiguration des Verwaltungsservers zur Authentifizierung von Benutzern bei Verzeichnisdienstanbietern wie Active Directory oder OpenLDAP oder zur Angabe eines eigenen Authentifizierungsverfahrens. Die Angabe eines Authentifizierungsdienstes ist nur möglich, wenn die Remote-Authentifizierung aktiviert wurde.

  - **Active Directory**
    - Administratorname

      Gibt den Administratornamen des Authentifizierungsservers an.

    - Passwort

      Gibt das Passwort für den Zugriff auf den Authentifizierungsserver an.

    - Basis-individueller Name

      Gibt den Speicherort der Remote-Benutzer auf dem Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, ist der individuelle Name der Basisname **cn=ou,dc=domain,dc=com**.

    - Verschachtelte Gruppensuche deaktivieren

      Legt fest, ob die Option für die Suche nach verschachtelten Gruppen aktiviert oder deaktiviert werden soll. Standardmäßig ist diese Option deaktiviert. Bei Verwendung von Active Directory können Sie die Authentifizierung beschleunigen, indem Sie die Unterstützung für verschachtelte Gruppen deaktivieren.

    - Sichere Verbindung verwenden

      Gibt den Authentifizierungsdienst an, der für die Kommunikation mit Authentifizierungsservern verwendet wird.

  - **OpenLDAP**
    - Bind individueller Name

      Gibt den Bind-individuellen Namen an, der zusammen mit dem Basis-individuellen Namen verwendet wird, um Remote-Benutzer auf dem Authentifizierungsserver zu finden.

    - Bind Passwort

      Gibt das Passwort für den Zugriff auf den Authentifizierungsserver an.

    - Basis-individueller Name

      Gibt den Speicherort der Remote-Benutzer auf dem Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, ist der individuelle Name der Basisname **cn=ou,dc=domain,dc=com**.

- Sichere Verbindung verwenden

  Gibt an, dass Secure LDAP für die Kommunikation mit LDAP-Authentifizierungsservern verwendet wird.

◦ **Andere**

- Bind individueller Name

  Gibt den Bind individueller Name an, der zusammen mit dem Basis individueller Name verwendet wird, um Remote-Benutzer auf dem von Ihnen konfigurierten Authentifizierungsserver zu finden.

- Bind Passwort

  Gibt das Passwort für den Zugriff auf den Authentifizierungsserver an.

- Basis-individueller Name

  Gibt den Speicherort der Remote-Benutzer auf dem Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, ist der individuelle Name der Basisname **cn=ou,dc=domain,dc=com**.

- Protokollversion

  Gibt die vom Authentifizierungsserver unterstützte Version des Lightweight Directory Access Protocol (LDAP) an. Sie können festlegen, ob die Protokollversion automatisch erkannt werden soll oder ob die Version auf 2 oder 3 gesetzt werden soll.

- Attribut für den Benutzernamen

  Gibt den Namen des Attributs auf dem Authentifizierungsserver an, das die Benutzeranmeldenamen enthält, die der Verwaltungsserver authentifiziert.

- Attribut der Gruppenzugehörigkeit

  Gibt einen Wert an, der Remote-Benutzern die Mitgliedschaft in der Management Servergruppe basierend auf einem Attribut und einem Wert zuweist, die im Authentifizierungsserver des Benutzers angegeben sind.

- UGID

  Wenn die Remote-Benutzer als Mitglieder eines GroupOfUniqueNames-Objekts im Authentifizierungsserver enthalten sind, können Sie mit dieser Option den Remote-Benutzern die Mitgliedschaft in der Managementservergruppe basierend auf einem bestimmten Attribut in diesem GroupOfUniqueNames-Objekt zuweisen.

- Verschachtelte Gruppensuche deaktivieren

  Legt fest, ob die Option für die Suche nach verschachtelten Gruppen aktiviert oder deaktiviert werden soll. Standardmäßig ist diese Option deaktiviert. Bei Verwendung von Active Directory können Sie die Authentifizierung beschleunigen, indem Sie die Unterstützung für verschachtelte Gruppen deaktivieren.

- Mitglied

  Gibt den Attributnamen an, den Ihr Authentifizierungsserver verwendet, um Informationen über die

einzelnen Mitglieder einer Gruppe zu speichern.

- Benutzerobjektklasse

  Gibt die Objektklasse eines Benutzers auf dem Remote-Authentifizierungsserver an.

- Gruppenobjektklasse

  Gibt die Objektklasse aller Gruppen auf dem Remote-Authentifizierungsserver an.

> Die Werte, die Sie für die Attribute „Member“, „User Object Class“ und „Group Object Class“ eingeben, müssen mit den Werten übereinstimmen, die in Ihren Active Directory-, OpenLDAP- und LDAP-Konfigurationen hinzugefügt wurden. Andernfalls kann die Authentifizierung fehlschlagen.

- Sichere Verbindung verwenden

  Gibt den Authentifizierungsdienst an, der für die Kommunikation mit Authentifizierungsservern verwendet wird.

> Wenn Sie den Authentifizierungsservice ändern möchten, ist es erforderlich, alle vorhandenen Authentifizierungsserver zu löschen und neue Authentifizierungsserver hinzuzufügen.

Bereich der Authentifizierungsserver

Im Bereich „Authentifizierungsserver“ sind die Authentifizierungsserver aufgeführt, mit denen der Verwaltungsserver kommuniziert, um Remote-Benutzer zu finden und zu authentifizieren. Die Anmeldeinformationen für Remote-Benutzer oder -Gruppen werden vom Authentifizierungsserver verwaltet.

- **Befehlsschaltflächen**

  Ermöglicht das Hinzufügen, Bearbeiten oder Löschen von Authentifizierungsservern.

  - Hinzufügen

    Ermöglicht das Hinzufügen eines Authentifizierungsservers.

  Wenn der Authentifizierungsserver, den Sie hinzufügen, Teil eines Hochverfügbarkeitspaars ist (das dieselbe Datenbank verwendet), können Sie auch den Partner-Authentifizierungsserver hinzufügen. Dadurch kann der Managementserver mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

  - Bearbeiten

    Hier können Sie die Einstellungen für einen ausgewählten Authentifizierungsserver bearbeiten.

  - Löschen

    Löscht die ausgewählten Authentifizierungsserver.

- **Name oder IP-Adresse**

  Zeigt den Hostnamen oder die IP-Adresse des Authentifizierungsservers an, der zur Authentifizierung des Benutzers auf dem Managementserver verwendet wird.

- **Port**

  Zeigt die Portnummer des Authentifizierungsservers an.

- **Authentifizierungstest**

  Mit dieser Schaltfläche können Sie die Konfiguration Ihres Authentifizierungsservers überprüfen, indem Sie einen Remote-Benutzer oder eine Remote-Gruppe authentifizieren.

  Wenn Sie beim Testen nur den Benutzernamen angeben, sucht der Verwaltungsserver den Remote-Benutzer auf dem Authentifizierungsserver, authentifiziert ihn aber nicht. Wenn Sie sowohl den Benutzernamen als auch das Passwort angeben, sucht der Verwaltungsserver den Remote-Benutzer und authentifiziert ihn.

  Sie können die Authentifizierung nicht testen, wenn die Remote-Authentifizierung deaktiviert ist.

Sicherheitszertifikate verwalten

Das HTTPS-Sicherheitszertifikat in Active IQ Unified Manager anzeigen

Sie können die Details des HTTPS-Zertifikats mit dem abgerufenen Zertifikat in Ihrem Browser vergleichen, um sicherzustellen, dass die verschlüsselte Verbindung Ihres Browsers zu Unified Manager nicht abgefangen wird.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Die Anzeige des Zertifikats ermöglicht die Überprüfung des Inhalts eines neu generierten Zertifikats oder die Anzeige von Subject Alt Names (SAN), über die auf Unified Manager zugegriffen werden kann.

Schritt

1. Im linken Navigationsbereich auf **General** > **HTTPS Certificate** klicken.

   Das HTTPS-Zertifikat wird oben auf der Seite angezeigt

Falls Sie detailliertere Informationen zum Sicherheitszertifikat benötigen, als auf der Seite HTTPS Certificate angezeigt werden, können Sie das Verbindungszertifikat in Ihrem Browser anzeigen.

Herunterladen einer HTTPS-Zertifikatsignierungsanforderung in Active IQ Unified Manager

Sie können eine Zertifikatssignierungsanforderung für das aktuelle HTTPS-Sicherheitszertifikat herunterladen, um die Datei einer Zertifizierungsstelle zur Signierung vorzulegen. Ein von einer Zertifizierungsstelle signiertes Zertifikat hilft, Man-in-the-Middle-Angriffe zu verhindern, und bietet besseren Schutz als ein selbstsigniertes Zertifikat.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich auf **General** > **HTTPS Certificate** klicken.

2. Sie können auf **Download HTTPS Certificate Signing Request** klicken.
3. Die `<hostname>.csr` Datei speichern.

Sie können die Datei einer Zertifizierungsstelle zum Signieren vorlegen und anschließend das signierte Zertifikat installieren.

Installation eines von einer Zertifizierungsstelle signierten HTTPS-Zertifikats in Active IQ Unified Manager

Sie können ein Sicherheitszertifikat hochladen und installieren, nachdem es von einer Certificate Authority signiert und zurückgegeben wurde. Die Datei, die Sie hochladen und installieren, muss eine signierte Version des vorhandenen selbstsignierten Zertifikats sein. Ein CA-signiertes Zertifikat hilft, Man-in-the-Middle-Angriffe zu verhindern, und bietet besseren Schutz als ein selbstsigniertes Zertifikat.

*Was Sie vor Beginn beachten sollten

Sie müssen die folgenden Aktionen abgeschlossen haben:

- Die Datei mit der Zertifikatsignierungsanforderung wurde heruntergeladen und durch eine Zertifizierungsstelle signiert.
- Zertifikatskette im PEM-Format gespeichert
- Die Kette umfasste alle Zertifikate, vom Unified Manager Serverzertifikat bis zum Stamm-Signaturzertifikat, einschließlich aller vorhandenen Zwischenzertifikate.

Sie benötigen die Rolle des Anwendungsadministrators.

Beträgt die Gültigkeitsdauer des Zertifikats, für das ein CSR erstellt wurde, mehr als 397 Tage, wird sie von der CA vor der Unterzeichnung und Rücksendung des Zertifikats auf 397 Tage verkürzt.

Schritte

1. Im linken Navigationsbereich auf **General** > **HTTPS Certificate** klicken.
2. Anschließend wählen Sie **HTTPS-Zertifikat installieren** aus.
3. In dem angezeigten Dialogfeld kann über **Datei auswählen…** die hochzuladende Datei gesucht werden.
4. Nach dem Auswählen der Datei installiert ein Klick auf **Install** die Datei.

   Informationen finden sich unter "Installation eines mit externen Tools generierten HTTPS-Zertifikats".

Beispiel einer Zertifikatskette

Das folgende Beispiel zeigt, wie die Zertifikatskettendatei aussehen könnte:

```
-----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-----
```

Informationen zu HTTPS-Zertifikaten, die mit externen Tools in Active IQ Unified Manager Unified Manager generiert wurden

Sie können selbstsignierte oder CA-signierte Zertifikate installieren, die mit einem externen Tool wie OpenSSL, BoringSSL oder LetsEncrypt generiert wurden.

Sie sollten den privaten Schlüssel zusammen mit der Zertifikatskette hochladen, da diese Zertifikate extern generierte Paare aus öffentlichem und privatem Schlüssel sind. Die zulässigen Schlüsselpaaralgorithmen sind „`RSA`“ und „`EC`“. Die Option „Install HTTPS Certificate“ ist auf der Seite „HTTPS Certificates“ im Abschnitt „General“ verfügbar. Die hochgeladene Datei sollte das folgende Eingabeformat aufweisen.

1. Privater Schlüssel des Servers, der zum Active IQ Unified Manager Host gehört
2. Zertifikat des Servers, das zum privaten Schlüssel passt
3. Zertifikate der Zertifizierungsstellen in umgekehrter Reihenfolge bis zur Root-CA, die zum Signieren des obigen Zertifikats verwendet werden

Format zum Laden eines Zertifikats mit einem EC Schlüsselpaar

Zulässige Kurven sind „`prime256v1`“ und „`secp384r1`“. Beispiel eines Zertifikats mit einem extern generierten EC-Paar:

```
 -----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-----
```

Format zum Laden eines Zertifikats mit einem RSA-Schlüsselpaar

Die zulässigen Schlüssellängen für das zum Host-Zertifikat gehörende RSA-Schlüsselpaar sind 2048, 3072 und 4096. Zertifikat mit einem extern generierten **RSA-Schlüsselpaar**:

```
-----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-----
```

Nach dem Hochladen des Zertifikats sollte die Active IQ Unified Manager Instanz neu gestartet werden, damit die Änderungen wirksam werden.

Prüfungen beim Hochladen extern generierter Zertifikate

Das System führt beim Hochladen eines mit externen Tools erstellten Zertifikats Prüfungen durch. Wenn eine dieser Prüfungen fehlschlägt, lehnt das System das Zertifikat ab. Die Validierung umfasst auch Zertifikate, die innerhalb des Produkts aus dem CSR generiert werden, sowie Zertifikate, die mit externen Tools erstellt werden.

- Der private Schlüssel in den Eingabedaten wird mit dem Host-Zertifikat in den Eingabedaten validiert.
- Der Common Name (CN) im Hostzertifikat wird mit dem FQDN des Hosts verglichen.
- Der Common Name (CN) des Hostzertifikats darf nicht leer sein oder nur Leerzeichen enthalten und darf nicht auf localhost gesetzt sein.
- Das Gültigkeitsbeginndatum sollte nicht in der Zukunft liegen, und das Gültigkeitsablaufdatum des Zertifikats sollte nicht in der Vergangenheit liegen.
- Falls Intermediate CA oder CA vorhanden ist, sollte das Gültigkeitsbeginn-Datum des Zertifikats nicht in der Zukunft liegen und das Gültigkeitsablaufdatum nicht in der Vergangenheit liegen.



Der private Schlüssel in den Eingabedaten darf nicht verschlüsselt sein. Falls private Schlüssel verschlüsselt sind, lehnt das System sie ab.

Beispiel 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
```

```
-----END ENCRYPTED PRIVATE KEY-----
```

Beispiel 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Beispiel 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Falls die Zertifikatsinstallation fehlschlägt, finden Sie weitere Informationen im Wissensdatenbank-Artikel (KB): "ActiveIQ Unified Manager kann ein extern generiertes Zertifikat nicht installieren"

Seitenbeschreibungen für die Zertifikatsverwaltung

Informationen zur HTTPS-Zertifikatsseite in Active IQ Unified Manager

Die Seite „HTTPS-Zertifikat“ ermöglicht das Anzeigen des aktuellen Sicherheitszertifikats, das Herunterladen einer Anforderung zur Zertifikatsignierung, das Generieren eines neuen selbstsignierten HTTPS-Zertifikats oder das Installieren eines neuen HTTPS-Zertifikats.

Wenn Sie kein neues selbstsigniertes HTTPS-Zertifikat erstellt haben, wird auf dieser Seite das Zertifikat angezeigt, das während der Installation generiert wurde.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie die folgenden Vorgänge durchführen:

- **HTTPS-Zertifikatsignierungsanforderung herunterladen**

  Lädt eine Zertifikatanforderung für das derzeit installierte HTTPS-Zertifikat herunter. Ihr Browser fordert Sie auf, die <hostname>.csr-Datei zu speichern, damit Sie die Datei einer Zertifizierungsstelle zum Signieren bereitstellen können.

- **Installation des HTTPS-Zertifikats**

  Ermöglicht das Hochladen und Installieren eines Sicherheitszertifikats, nachdem dieses von einer Zertifizierungsstelle signiert und zurückgesendet wurde. Das neue Zertifikat ist nach einem Neustart des Verwaltungsservers wirksam.

- **HTTPS-Zertifikat neu generieren**

Ermöglicht die Generierung eines neuen selbstsignierten HTTPS-Zertifikats, das das aktuelle Sicherheitszertifikat ersetzt. Das neue Zertifikat ist nach einem Neustart des Unified Manager gültig.

Dialogfeld „HTTPS-Zertifikat in Active IQ Unified Manager neu generieren“

Im Dialogfeld „HTTPS-Zertifikat neu generieren“ können Sie die Sicherheitsinformationen anpassen und anschließend ein neues HTTPS-Zertifikat mit diesen Informationen generieren.

Auf dieser Seite erscheinen die aktuellen Zertifikatsinformationen.

Die Auswahlmöglichkeiten “Regenerate Using Current Certificate Attributes” und “Update the Current Certificate Attributes” ermöglichen es Ihnen, das Zertifikat mit den aktuellen Informationen neu zu generieren oder ein Zertifikat mit neuen Informationen zu erstellen.

- **Allgemeiner Name**

  Erforderlich. Der vollqualifizierte Domain-Name (FQDN), den Sie sichern möchten.

  In Hochverfügbarkeitskonfigurationen von Unified Manager kommt die virtuelle IP-Adresse zum Einsatz.

- **E-Mail**

  Optional. Eine E-Mail-Adresse zur Kontaktaufnahme mit Ihrem Unternehmen; in der Regel die E-Mail-Adresse des Zertifikatsadministrators oder der IT-Abteilung.

- **Unternehmen**

  Optional. In der Regel der eingetragene Name Ihres Unternehmens.

- **Abteilung**

  Optional. Der Name der Abteilung in Ihrem Unternehmen.

- **Stadt**

  Optional. Der Ort Ihres Unternehmens.

- **Zustand**

  Optional. Das Bundesland oder die Provinz Ihres Unternehmens, nicht abgekürzt.

- **Land**

  Optional. Der Länderstandort Ihres Unternehmens. Dies ist normalerweise ein zweistelliger ISO-Code des Landes.

- **Alternative Bezeichnungen**

  Erforderlich. Zusätzliche, nicht primäre Domänennamen, die zusätzlich zu localhost oder anderen Netzwerkadressen für den Zugriff auf diesen Server verwendet werden können. Als Trennzeichen zwischen den einzelnen alternativen Namen dienen Kommas.

  Das Kontrollkästchen „`Lokale Identifikationsinformationen ausschließen (z. B. localhost)`“ wird ausgewählt, wenn die lokalen Identifikationsinformationen aus dem Feld „Alternative

Namen“ im Zertifikat entfernt werden sollen. Wenn dieses Kontrollkästchen aktiviert ist, werden im Feld „Alternative Namen“ nur die Daten verwendet, die in das Feld eingegeben werden. Wenn das Feld leer bleibt, enthält das resultierende Zertifikat überhaupt kein Feld „Alternative Namen“.

- **SCHLÜSSELLÄNGE (SCHLÜSSELALGORITHMUS: RSA)**

  Der Schlüsselalgorithmus ist auf RSA eingestellt. Sie können zwischen den Schlüssellängen 2048, 3072 oder 4096 Bit wählen. Die Standardschlüssellänge beträgt 2048 Bit.

- **GÜLTIGKEITSDAUER**

  Die Standardgültigkeitsdauer beträgt 397 Tage. Wenn Sie ein Upgrade von einer früheren Version durchgeführt haben, bleibt die Gültigkeit des vorherigen Zertifikats möglicherweise unverändert.

Weitere Informationen sind unter "Generierung von HTTPS-Zertifikaten" verfügbar.

Storage überwachen und managen

Einführung in Active IQ Unified Manager

Informationen zu Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) ermöglicht es Ihnen, den Systemstatus und die Performance Ihrer ONTAP Storage Systeme über eine einzige Schnittstelle zu überwachen und zu managen.

Unified Manager bietet folgende Funktionen:

- Erkennung, Überwachung und Benachrichtigungen für Systeme, auf denen ONTAP-Software installiert ist.
- Dashboard zur Anzeige des Kapazitäts-, Sicherheits- und Performance-Systemstatus der Umgebung.
- Erweiterte Warnungs-, Ereignis- und Schwellenwertinfrastruktur.
- Zeigt detaillierte Diagramme, die die Workload-Aktivität im Zeitverlauf darstellen, einschließlich IOPS (Operationen), MBps (Durchsatz), Latenz (Antwortzeit), Auslastung, Performance Kapazität und Cache-Verhältnis.
- Identifiziert Workloads, die Clusterkomponenten übermäßig beanspruchen, und Workloads, deren Performance durch die erhöhte Aktivität beeinträchtigt wird.
- Bietet Vorschläge für Korrekturmaßnahmen zur Behebung bestimmter Vorfälle und Ereignisse sowie für einige Ereignisse eine Schaltfläche „Fix It“, damit Sie das Problem sofort beheben können.
- Lässt sich in OnCommand Workflow Automation integrieren, um automatisierte Schutz-Workflows auszuführen.
- Möglichkeit, neue Workloads, wie z. B. eine LUN oder eine Dateifreigabe, direkt aus Unified Manager zu erstellen und ein Performance Service Level zuzuweisen, um die Performance- und Storage-Ziele für die Benutzer zu definieren, die über diesen Workload auf die Applikation zugreifen.

Informationen zur Zustandsüberwachung in Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) ermöglicht die Überwachung einer großen Anzahl von Systemen mit ONTAP-Software über eine zentrale Benutzeroberfläche. Die Unified Manager Serverinfrastruktur bietet Skalierbarkeit, Supportfähigkeit sowie erweiterte Überwachungs- und Benachrichtigungsfunktionen.

Zu den wichtigsten Funktionen des Unified Manager gehören Überwachung, Alarmierung, das Managen der Verfügbarkeit und Kapazität von Clustern, das Managen der Schutzfunktionen sowie die Bündelung von Diagnosedaten und deren Weiterleitung an den technischen Support.

Mit Unified Manager können Sie Ihre Cluster überwachen. Wenn Probleme im Cluster auftreten, benachrichtigt Sie Unified Manager über Ereignisse mit detaillierten Informationen zu diesen Problemen. Einige Ereignisse bieten Ihnen auch Abhilfemaßnahmen, mit denen Sie die Probleme beheben können. Sie können Warnmeldungen für Ereignisse konfigurieren, sodass Sie bei Problemen per E-Mail und SNMP-Traps benachrichtigt werden.

Mit Unified Manager können Sie Storage Objekte in Ihrer Umgebung managen, indem Sie sie mit Annotationen verknüpfen. Sie können benutzerdefinierte Annotationen erstellen und Cluster, Storage Virtual Machines

(SVMs) und Volumes dynamisch über Regeln mit den Annotationen verknüpfen.

Sie können auch die Storage-Anforderungen Ihrer Clusterobjekte anhand der Informationen in den Kapazitäts- und Systemstatusdiagrammen für das jeweilige Clusterobjekt planen.

Physische und logische Kapazität

Unified Manager verwendet für ONTAP Storage Objekte die Konzepte des physischen und logischen Speicherplatzes.

- Physische Kapazität: Der physische Speicherplatz bezieht sich auf die physischen Blöcke des Storage, die im Volume verwendet werden. „Genutzte physische Kapazität“ ist typischerweise kleiner als die genutzte logische Kapazität, da Daten durch Storage-Effizienzfunktionen (wie Deduplizierung und Komprimierung) reduziert werden.
- Logische Kapazität: Logischer Speicherplatz bezeichnet den nutzbaren Speicherplatz (die logischen Blöcke) in einem Volume. Logischer Speicherplatz bezieht sich darauf, wie theoretischer Speicherplatz genutzt werden kann, ohne die Ergebnisse von Deduplizierung oder Komprimierung zu berücksichtigen. „Genutzter logischer Speicherplatz“ ist der genutzte physische Speicherplatz zuzüglich der Einsparungen durch konfigurierte Storage-Effizienzfunktionen (wie Deduplizierung und Komprimierung). Dieser Wert erscheint oft höher als die genutzte physische Kapazität, da er die Datenkomprimierung und andere Verringerungen des physischen Speicherplatzes nicht widerspiegelt. Daher könnte die gesamte logische Kapazität höher sein als der bereitgestellte Speicherplatz.

Kapazitätsmaßeinheiten

Unified Manager berechnet die Storage-Kapazität auf der Grundlage binärer Einheiten von 1024 (2^{10}) Byte. In ONTAP 9.10.0 und früheren Versionen wurden diese Einheiten als KB, MB, GB, TB und PB angezeigt. Ab ONTAP 9.10.1 werden sie in Unified Manager als KiB, MiB, GiB, TiB und PiB angezeigt.

Die für den Datendurchsatz verwendeten Einheiten sind weiterhin Kilobyte pro Sekunde (Kbps), Megabyte pro Sekunde (Mbps), Gigabyte pro Sekunde (Gbit/s), Terabyte pro Sekunde (Tbps) usw. für alle Releases von ONTAP.

Im Unified Manager für ONTAP 9.10.0 und frühere Versionen angezeigte Kapazitätseinheit	In Unified Manager für ONTAP 9.10.1 angezeigte Kapazitätseinheit	Berechnung	Wert in Bytes
KB	KiB	1024	1024 Bytes
MB	MiB	1024 * 1024	1.048.576 Bytes
GB	GiB	1024 * 1024 * 1024	1.073.741.824 Bytes
TB	TiB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 Bytes

Informationen zur Leistungsüberwachung in Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) bietet Funktionen zur Performance-Überwachung und zur Ursachenanalyse von Ereignissen für Systeme, auf denen NetApp ONTAP-Software ausgeführt wird.

Unified Manager hilft Ihnen, Workloads zu identifizieren, die Clusterkomponenten übermäßig beanspruchen und die Performance anderer Workloads im Cluster beeinträchtigen. Durch das Definieren von Performance-Schwellenwertrichtlinien können Sie auch Maximalwerte für bestimmte Performance-Zähler festlegen, sodass Ereignisse generiert werden, wenn der Schwellenwert überschritten wird. Unified Manager benachrichtigt Sie über diese Performance-Ereignisse, damit Sie eine Korrekturmaßnahme ergreifen und die Performance wieder auf ein normales Betriebsniveau bringen können. Sie können Ereignisse in der Unified Manager UI anzeigen und analysieren.

Unified Manager überwacht die Performance von zwei Arten von Arbeitslasten:

- Benutzerdefinierte Arbeitslasten

  Diese Workloads bestehen aus FlexVol Volumes und FlexGroup Volumes, die Sie in Ihrem Cluster erstellt haben.

- Systemdefinierte Workloads

  Diese Arbeitslasten bestehen aus internen Systemaktivitäten.

Active IQ Unified Manager REST APIs verwenden

Active IQ Unified Manager bietet Ihnen REST-APIs zur Anzeige von Informationen über die Überwachung und Verwaltung Ihrer Storage-Umgebung. APIs ermöglichen außerdem die Provisionierung und Verwaltung von Storage Objekten auf Basis von Richtlinien.

Sie können ONTAP-APIs auch auf allen von ONTAP verwalteten Clustern ausführen, indem Sie das vom Unified Manager unterstützte API-Gateway verwenden.

Informationen zu Unified Manager REST APIs sind unter "Erste Schritte mit Active IQ Unified Manager REST APIs" verfügbar.

Was der Unified Manager Server leistet

Informationen zum Active IQ Unified Manager Server

Die Unified Manager Serverinfrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Applikationsserver. Sie bietet Infrastruktur Services wie Erkennung, Überwachung, rollenbasierte Zugriffssteuerung (RBAC), Auditierung und Protokollierung.

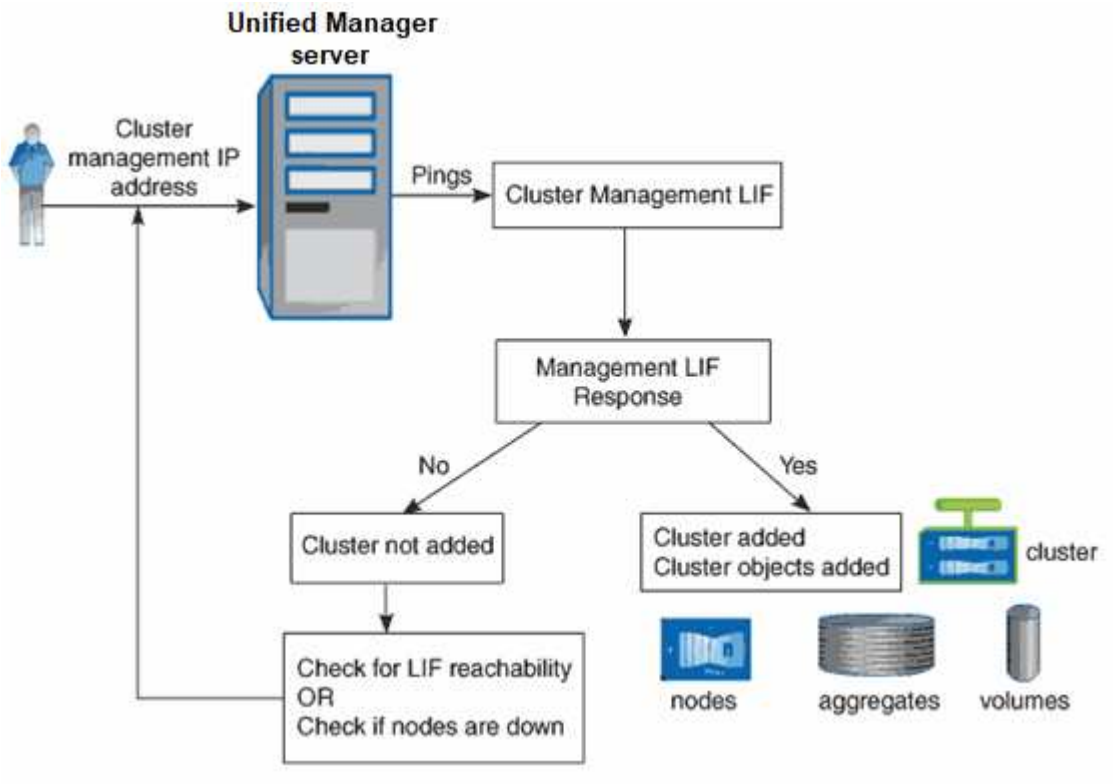
Unified Manager sammelt Clusterinformationen, speichert die Daten in der Datenbank und analysiert die Daten, um festzustellen, ob Clusterprobleme vorliegen.

Informationen zur Funktionsweise des Cluster-Erkennungsprozesses in Active IQ Unified Manager

Nachdem Sie den Cluster zu Unified Manager hinzugefügt haben, erkennt der Server die Clusterobjekte und fügt sie seiner Datenbank hinzu. Wenn Sie verstehen, wie dieser Erkennungsprozess funktioniert, können Sie die Cluster Ihres Unternehmens und deren Objekte besser managen.

Das Standardüberwachungsintervall beträgt 15 Minuten: Wenn Sie einen Cluster zum Unified Manager Server hinzugefügt haben, dauert es 15 Minuten, bis die Clusterdetails in der Unified Manager UI angezeigt werden.

Die folgende Abbildung veranschaulicht den Erkennungsprozess in Active IQ Unified Manager:



Die Benutzeroberfläche verstehen

Informationen zur Active IQ Unified Manager Benutzeroberfläche

Die Benutzeroberfläche von Unified Manager besteht hauptsächlich aus einem Dashboard, das einen schnellen Überblick über die überwachten Objekte bietet. Die Benutzeroberfläche bietet außerdem Zugriff auf die Ansicht aller Clusterobjekte.

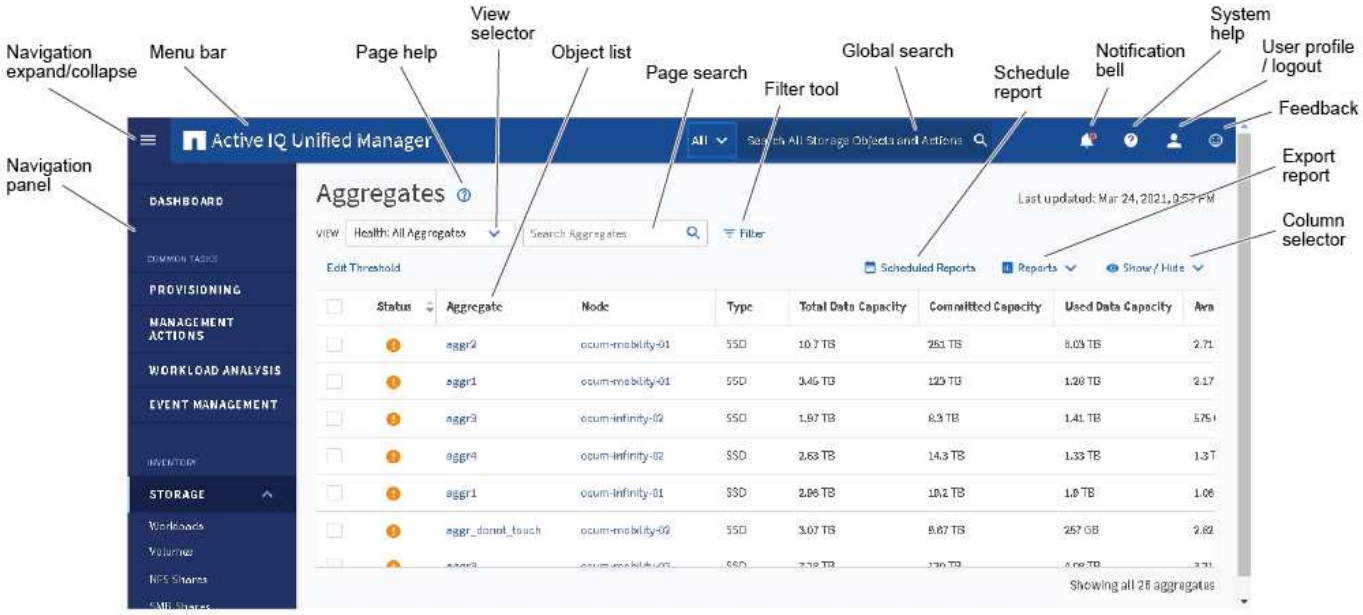
Sie können eine bevorzugte Ansicht auswählen und die Aktionsschaltflächen nach Bedarf verwenden. Ihre Bildschirmkonfiguration wird in einem Arbeitsbereich gespeichert, sodass alle benötigten Funktionen beim Start von Unified Manager verfügbar sind. Wenn Sie jedoch zwischen verschiedenen Ansichten wechseln und anschließend wieder zurückkehren, kann die Ansicht abweichen.

Typische Fensterlayouts in Active IQ Unified Manager

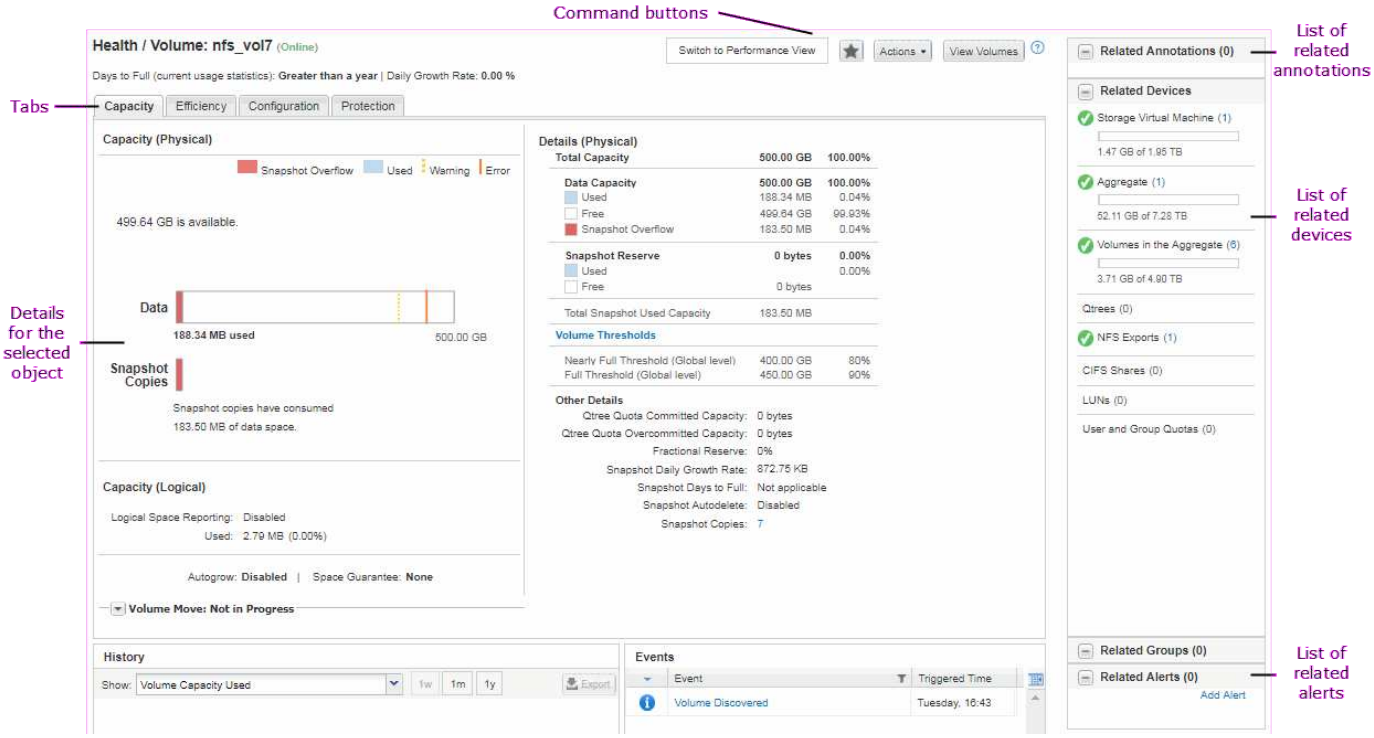
Das Verständnis der typischen Fensterlayouts hilft Ihnen, Active IQ Unified Manager effektiv zu nutzen. Die meisten Unified Manager Fenster ähneln einem von zwei allgemeinen Layouts: Objektliste oder Details. Die empfohlene Anzeigeeinstellung beträgt mindestens 1280 x 1024 Pixel.

Nicht jedes Fenster enthält jedes Element in den folgenden Diagrammen.

Layout des Objektlistenfensters



Layout des Fensters „Objektdetails“



Anpassen des Fensterlayouts in Active IQ Unified Manager

Mit Active IQ Unified Manager können Sie das Layout der Informationen auf den Storage- und Netzwerkobjektseiten anpassen. Durch die Anpassung der Fenster können Sie steuern, welche Daten angezeigt werden und wie diese dargestellt werden.

- **Sortierung**

  Sie können auf die Spaltenüberschrift klicken, um die Sortierreihenfolge der Spalteneinträge zu ändern.

Wenn Sie auf die Spaltenüberschrift klicken, erscheinen die Sortierpfeile (und) für diese Spalte.

- **Filtern**

  Durch Klicken auf das Filtersymbol () lassen sich Filter anwenden, um die Anzeige von Informationen auf den Seiten für Storage- und Netzwerkobjekte so anzupassen, dass nur die Einträge angezeigt werden, die den angegebenen Bedingungen entsprechen. Die Filter werden im Bereich „Filter“ angewendet.

  Im Filterbereich lassen sich die meisten Spalten anhand der ausgewählten Optionen filtern. Beispielsweise lassen sich in der Ansicht „Zustand: Alle Volumes“ im Filterbereich alle Volumes anzeigen, die offline sind, wenn die entsprechende Filteroption unter „Status“ ausgewählt wird.

  Kapazitätsbezogene Spalten in jeder Liste zeigen Kapazitätsdaten immer in den entsprechenden Einheiten an, gerundet auf zwei Dezimalstellen. Dies gilt auch beim Filtern von Kapazitätsspalten. Wenn beispielsweise in der Ansicht „Health: All Aggregates“ in der Spalte „Total Data Capacity“ der Filter verwendet wird, um Daten größer als 20,45 GB zu filtern, wird die tatsächliche Kapazität von 20,454 GB als 20,45 GB angezeigt. Entsprechend wird beim Filtern von Daten kleiner als 20,45 GB die tatsächliche Kapazität von 20,449 GB als 20,45 GB angezeigt.

  Wenn Sie in der Ansicht „Integrität: Alle Aggregate“ den Filter in der Spalte „Verfügbare Daten %“ verwenden, um Daten über 20,45 % zu filtern, wird die tatsächliche Kapazität von 20,454 % als 20,45 % angezeigt. Wenn Daten unter 20,45 % gefiltert werden, wird die tatsächliche Kapazität von 20,449 % als 20,45 % angezeigt.

- **Spalten ein- oder ausblenden**

  Über das Symbol für die Spaltenanzeige (**Ein-/Ausblenden**) lässt sich auswählen, welche Spalten angezeigt werden sollen. Nachdem die gewünschten Spalten ausgewählt wurden, lässt sich ihre Reihenfolge durch Ziehen mit der Maus ändern.

- **Suche**

  Mithilfe des Suchfelds können Sie nach bestimmten Objektattributen suchen, um die Liste der Elemente auf der Inventarseite weiter einzugrenzen. Beispielsweise kann „cloud“ eingegeben werden, um die Liste der Volumes auf der Volumes-Inventarseite zu verfeinern, sodass alle Volumes angezeigt werden, die das Wort „cloud“ enthalten.

- **Datenexport**

  Sie können auf die Schaltfläche **Reports** klicken (oder auf die Schaltfläche **Export**, um Daten in eine CSV `(.csv)`-Datei, `(.pdf)`ein Dokument oder eine Microsoft Excel `(.xlsx)` Datei zu exportieren) und die exportierten Daten zum Erstellen von Berichten verwenden.

Verwendung der Active IQ Unified Manager Hilfe

Die Hilfe enthält Informationen zu allen Funktionen von Active IQ Unified Manager. Mithilfe des Inhaltsverzeichnisses, des Index oder der Suchfunktion finden Sie Informationen zu den Funktionen und deren Verwendung.

Hilfe ist über die einzelnen Registerkarten und die Menüleiste der Benutzeroberfläche von Unified Manager verfügbar.

Die Suchfunktion in der Hilfe funktioniert nicht für Wortteile.

- Informationen zu bestimmten Feldern oder Parametern finden Sie unter .
- Zum Anzeigen des gesamten Hilfseinhalts wählen Sie in der Menüleiste > **Hilfe/Dokumentation** aus.

  Detailliertere Informationen finden Sie, wenn Sie einen beliebigen Abschnitt des Inhaltsverzeichnisses im Navigationsbereich erweitern.

- Zum Durchsuchen der Hilfethemen können Sie im Navigationsbereich die Registerkarte **Search** auswählen, das gewünschte Wort oder die gewünschte Wortfolge eingeben und auf **Go!** klicken.
- Hilfethemen lassen sich über das Druckersymbol drucken.

Lesezeichen für bevorzugte Hilfethemen in Active IQ Unified Manager

Im Tab „Hilfefavoriten“ können Sie häufig genutzte Hilfethemen als Lesezeichen speichern. Hilfe-Lesezeichen bieten schnellen Zugriff auf Ihre bevorzugten Themen.

Schritte

1. Zum Hilfethema navigieren, das als Favorit hinzugefügt werden soll.
2. Auf **Favoriten** und anschließend auf **Hinzufügen** klicken.

Suche nach Speicherobjekten in Active IQ Unified Manager

Um schnell auf ein bestimmtes Objekt zuzugreifen, können Sie das Feld **Alle Speicherobjekte durchsuchen** oben in der Menüleiste verwenden. Diese globale Suche in allen Objekten ermöglicht es Ihnen, bestimmte Objekte schnell nach Typ zu finden. Die Suchergebnisse sind nach Speicherobjekttyp sortiert, und Sie können sie über das Dropdown-Menü weiter nach Objekt filtern.

Bevor Sie beginnen

- Zum Ausführen dieser Aufgabe müssen Sie über eine der folgenden Rollen verfügen: Operator, Application Administrator oder Storage Administrator.
- Eine gültige Suchanfrage muss mindestens drei Zeichen enthalten.

Bei Verwendung des Werts „Alle“ im Dropdown-Menü zeigt die globale Suche die Gesamtzahl der in allen Objektkategorien gefundenen Ergebnisse an, mit maximal 25 Suchergebnissen für jede Objektkategorie. Aus dem Dropdown-Menü lässt sich ein bestimmter Objekttyp auswählen, um die Suche innerhalb eines bestimmten Objekttyps zu verfeinern. In diesem Fall ist die zurückgegebene Liste nicht auf die ersten 25 Objekte beschränkt.

Zu den Objekttypen, nach denen Sie suchen können, gehören:

- Cluster
- Nodes
- Storage VMs
- Aggregate
- Volumes
- Qtrees
- SMB Freigaben

- NFS-Freigaben
- Benutzer- oder Gruppenkontingente
- LUNs
- NVMe-Namespaces
- Initiatorgruppen
- Initiatoren
- Konsistenzgruppe

Die Eingabe eines Workload-Namens liefert die Liste der Workloads unter der entsprechenden Volumes- oder LUNs-Kategorie.

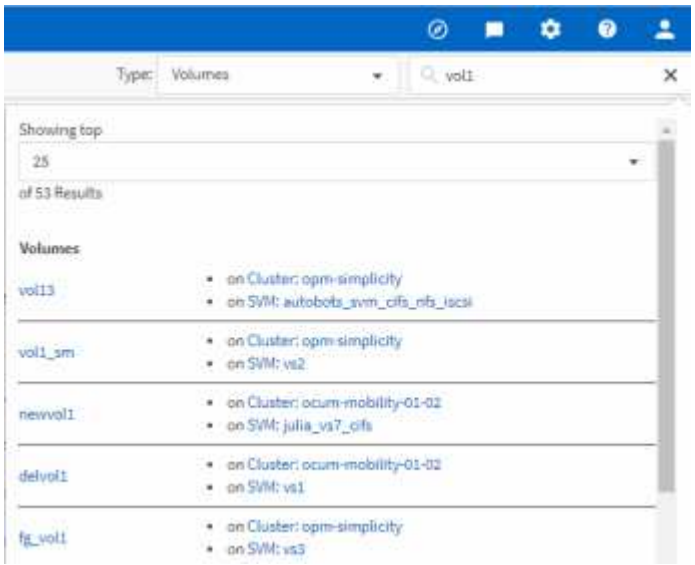
Sie können in den Suchergebnissen auf jedes Objekt klicken, um zur Systemstatus-Detailseite für dieses Objekt zu gelangen. Falls für ein Objekt keine direkte Systemstatusseite vorhanden ist, wird die Systemstatusseite des übergeordneten Objekts angezeigt. Wenn Sie beispielsweise nach einer bestimmten LUN suchen, wird die SVM-Detailseite angezeigt, auf der sich die LUN befindet.

Ports und LIFs sind in der globalen Suchleiste nicht auffindbar.

Schritte

1. Im Menü kann ein Objekttyp ausgewählt werden, um die Suchergebnisse auf einen einzelnen Objekttyp einzugrenzen.
2. Im Feld **Alle Storage Objekte durchsuchen** sind mindestens drei Zeichen des Objektnamens erforderlich.

   In diesem Beispiel ist im Dropdown-Menü der Objekttyp „Volumes“ ausgewählt. Die Eingabe von „vol1“ in das Feld „Alle Storage-Objekte durchsuchen“ zeigt eine Liste aller Volumes an, deren Namen diese Zeichen enthalten.



Speicherdaten können in Active IQ Unified Manager als Berichte exportiert werden

Sie können Storage-Daten in verschiedenen Ausgabeformaten exportieren und die exportierten Daten dann zum Erstellen von Berichten verwenden. Wenn beispielsweise 10 kritische Ereignisse noch nicht behoben wurden, können Sie die Daten von der

Inventarseite der Ereignisverwaltung exportieren, um einen Bericht zu erstellen und diesen dann an Administratoren zu senden, die die Probleme beheben können.

Daten können von den Inventarseiten **Storage** und **Network** in eine `.csv`Datei, `.xlsx`Datei oder ein `.pdf`Dokument exportiert und zum Erstellen von Berichten verwendet werden. Es gibt weitere Bereiche im Produkt, in denen nur `.csv`- oder `.pdf`Dateien generiert werden können.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie exportieren möchten…	Folgendes ist zu tun…
Inventardetails der Storage Objekte	Im linken Navigationsmenü wird **Storage** oder **Network** ausgewählt; anschließend folgt die Auswahl eines Storage-Objekts. Zur Auswahl stehen eine der vom System bereitgestellten Ansichten oder eine von Ihnen erstellte benutzerdefinierte Ansicht.
Details zur QoS-Richtliniengruppe	Die Auswahl erfolgt im linken Navigationsmenü über **Storage** > **QoS Policy Groups**.
Details zur Speicherkapazität und zum Schutzverlauf	Die Auswahl eines einzelnen Aggregats oder Volumes erfolgt unter **Storage** > **Aggregates** oder **Storage** > **Volumes**.
Ereignisdetails	Die Auswahl von **Event Management** erfolgt im linken Navigationsmenü.
Top-10-Performancedetails von Storage Objekten	Über **Storage** > **Clusters** > **Performance:All Clusters** lässt sich dann ein Cluster auswählen und die Registerkarte **Top Performers** öffnen. Anschließend können Sie ein Storage Objekt und einen Performance Zähler auswählen.

2. Die Schaltfläche **Reports** auswählen (oder auf einigen UI-Seiten die Schaltfläche **Export**).
3. Zum Bestätigen der Exportanfrage **CSV herunterladen**, **PDF herunterladen** oder **Excel herunterladen** auswählen.

   Auf der Registerkarte „Top Performers“ können Sie auswählen, einen Bericht mit den Statistiken für den einzelnen angezeigten Cluster oder für alle Cluster im Datacenter herunterzuladen.

   Die Datei wurde heruntergeladen.

4. Die Datei lässt sich in der entsprechenden Applikation öffnen.

Verwandte Informationen

"Systemstatus/Cluster-Inventarseite"

"Planen eines Berichts"

Inhalte der Inventarseite in Active IQ Unified Manager filtern

Sie können die Daten auf den Inventarseiten im Unified Manager filtern, um schnell Daten anhand bestimmter Kriterien zu finden. Mithilfe der Filterfunktion können Sie die Inhalte der Unified Manager Seiten so einschränken, dass nur die für Sie relevanten Ergebnisse angezeigt werden. Dies ist eine sehr effiziente Methode, um nur die Daten anzuzeigen, die für Sie relevant sind.

Mit **Filterung** lässt sich die Rasteransicht an Ihre Präferenzen anpassen. Die verfügbaren Filteroptionen hängen vom Objekttyp ab, der in der Rasteransicht angezeigt wird. Wenn derzeit Filter angewendet werden, erscheint rechts neben der Schaltfläche „Filter“ deren Anzahl.

Drei Arten von Filterparametern stehen zur Verfügung.

Parameter	Validierung
Zeichenkette (Text)	Die Operatoren sind **enthält**, **beginnt mit**, **endet mit** und **enthält nicht**.
Anzahl	Die Operatoren sind **größer als**, **kleiner als**, **im letzten** und **zwischen**.
Enum (Text)	Die Operatoren sind **is** und **is not**.

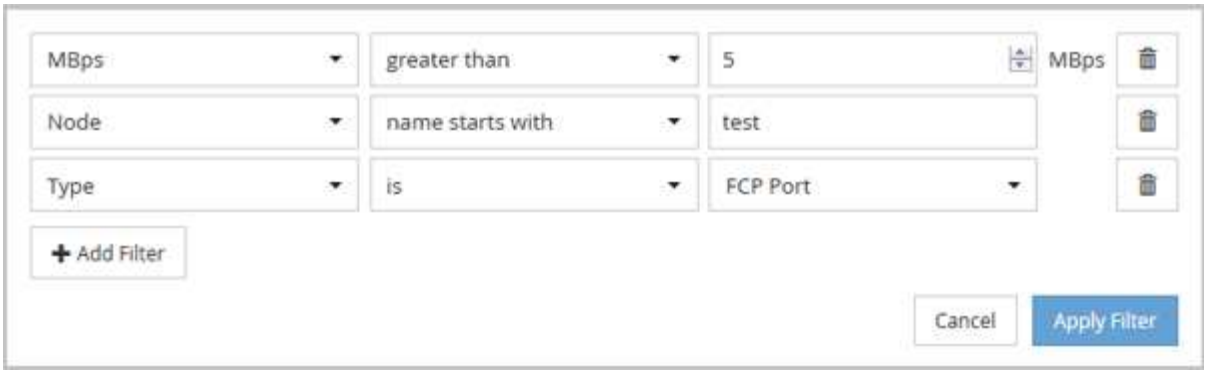
Die Felder „Spalte“, „Operator“ und „Wert“ sind für jeden Filter erforderlich; die verfügbaren Filter entsprechen den filterbaren Spalten auf der aktuellen Seite. Es können maximal vier Filter angewendet werden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten Ihrer gefilterten Suche, nicht nur für die aktuell angezeigte Seite.

Sie können Filter über den Bereich „Filtering“ hinzufügen.

1. Oben auf der Seite wählen Sie die Schaltfläche **Filter** aus. Der Filterbereich wird angezeigt.
2. Über die linke Dropdown-Liste lässt sich ein Objekt auswählen, z. B. *Cluster* oder ein Performance-Zähler.
3. In der mittleren Dropdown-Liste wählen Sie den Operator aus, den Sie verwenden möchten.
4. In der letzten Liste erfolgt die Auswahl oder Eingabe eines Werts, um den Filter für dieses Objekt zu vervollständigen.
5. Zum Hinzufügen eines weiteren Filters klicken Sie auf **+Add Filter**. Ein zusätzliches Filterfeld wird angezeigt. Dieses Filterfeld wird mithilfe des in den vorherigen Schritten beschriebenen Verfahrens ausgefüllt. Es ist zu beachten, dass die Schaltfläche **+Add Filter** nach dem Hinzufügen des vierten Filters nicht mehr angezeigt wird.
6. Zum Anwenden des Filters **Filter anwenden** auswählen. Die Filteroptionen werden auf das Raster angewendet, und die Anzahl der Filter wird rechts neben der Schaltfläche „Filter“ angezeigt.
7. Im Filterbereich können einzelne Filter entfernt werden, indem auf das Papierkorbsymbol rechts neben dem zu entfernenden Filter geklickt wird.
8. Zum Entfernen aller Filter steht unten im Filterbereich **Zurücksetzen** zur Verfügung.

Filterbeispiel

Die Abbildung zeigt das Filterfeld mit drei Filtern. Die Schaltfläche **+Filter hinzufügen** erscheint, wenn weniger als die maximale Anzahl von vier Filtern vorhanden ist.



Nach einem Klick auf **Filter anwenden** schließt sich der Filterbereich, übernimmt Ihre Filter und zeigt die Anzahl der angewendeten Filter an (3).

Aktive Ereignisse können über die Benachrichtigungsglocke in Active IQ Unified Manager angezeigt werden

Die Benachrichtigungsglocke ( ) in der Menüleiste bietet eine schnelle Möglichkeit, die wichtigsten aktiven Ereignisse anzuzeigen, die Unified Manager überwacht.

Die Liste der aktiven Ereignisse zeigt die Gesamtzahl der kritischen Ereignisse, Fehler, Warnungen und Upgrade-Ereignisse auf allen Clustern an. Diese Liste enthält Ereignisse der letzten 7 Tage, jedoch keine Informationsereignisse. Über einen Link kann die Liste der Ereignisse angezeigt werden, die für Sie am relevantesten sind.

Wenn ein Cluster nicht erreichbar ist, zeigt Unified Manager diese Informationen auf dieser Seite an. Detaillierte Informationen zu einem nicht erreichbaren Cluster können durch Klicken auf die Schaltfläche „Details“ angezeigt werden. Dadurch wird die Seite mit den Ereignisdetails geöffnet. Probleme bei der Scale-Überwachung, wie z. B. geringer Speicherplatz oder RAM auf der Managementstation, werden ebenfalls auf dieser Seite angezeigt.

Schritte

1. In der Menüleiste wird ausgewählt.
2. Details zu allen aktiven Ereignissen lassen sich über den Ereignistext-Link anzeigen, z. B. „2 Capacity“ oder „4 Performance“.

Überwachung und Management von Clustern über das Dashboard

Cluster lassen sich über das Dashboard in Active IQ Unified Manager überwachen und verwalten

Das Dashboard bietet einen kumulativen Überblick über den aktuellen Systemstatus Ihrer überwachten ONTAP Systeme. Das Dashboard bietet “Bereiche”, mit denen Sie die Gesamtkapazität sowie den Performance- und Sicherheitsstatus der von Ihnen überwachten Cluster beurteilen können.

Darüber hinaus gibt es bestimmte ONTAP Probleme, die Sie direkt über die Benutzeroberfläche des Unified Manager beheben können, anstatt ONTAP System Manager oder die ONTAP CLI verwenden zu müssen.

Im oberen Bereich des Dashboard können Sie auswählen, ob die Panels Informationen für alle überwachten Cluster oder für einen einzelnen Cluster anzeigen. Sie können zunächst den Status aller Cluster anzeigen und dann zu einzelnen Clustern wechseln, wenn Sie detaillierte Informationen anzeigen möchten.

Je nach Ihrer Konfiguration erscheinen einige der unten aufgeführten Bedienfelder möglicherweise nicht auf der Seite.

Panels	Beschreibung
Managementaktionen	Wenn Unified Manager ein Problem diagnostizieren und eine einzige Lösung dafür ermitteln kann, werden diese Lösungen in diesem Bereich mit einer Schaltfläche **Beheben** angezeigt.
Kapazität	Zeigt die Gesamtkapazität und die genutzte Kapazität der lokalen Ebene und der Cloud-Ebene sowie die Anzahl der Tage an, bis die lokale Kapazität die Obergrenze erreicht.
Performance-Kapazität	Zeigt für jeden Cluster den Wert der Performance-Kapazität und die Anzahl der Tage an, bis die Performance-Kapazität die Obergrenze erreicht.
Workload-IOPS	Zeigt die Gesamtzahl der Workloads an, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden.
Workload-Performance	Zeigt die Gesamtzahl der konformen und nicht konformen Workloads an, die jedem definierten Performance Service Level zugeordnet sind.
Sicherheit	Zeigt die Anzahl der konformen bzw. nicht konformen Cluster, die Anzahl der konformen bzw. nicht konformen SVMs und die Anzahl der verschlüsselten bzw. unverschlüsselten Volumes an.
Schutz	Zeigt die Anzahl der Storage VMs an, die durch eine SVM-DR-Beziehung geschützt sind, die Anzahl der Volumes, die durch eine SnapMirror Beziehung geschützt sind, die Anzahl der durch Snapshot geschützten Volumes und die Anzahl der Cluster, die durch MetroCluster geschützt sind.
Nutzungsübersicht	Zeigt Cluster an, sortiert nach höchster IOPS, höchstem Durchsatz (MBps) oder höchster genutzter physischer Kapazität.

Informationen zur Dashboard-Seite von Active IQ Unified Manager

Die Dashboard-Seite enthält „Bereiche“, die die allgemeine Kapazität, Performance und den Sicherheitsstatus der Cluster anzeigen, die Sie überwachen. Diese Seite enthält außerdem den Bereich Management Actions, in dem Korrekturen aufgeführt sind, die Unified Manager zur Behebung bestimmter Ereignisse durchführen kann.

Die meisten Bereiche zeigen außerdem die Anzahl der aktiven Ereignisse in der jeweiligen Kategorie sowie die Anzahl der in den letzten 24 Stunden neu hinzugekommenen Ereignisse an. Diese Informationen helfen Ihnen bei der Entscheidung, welche Cluster Sie möglicherweise genauer analysieren müssen, um Ereignisse zu

beheben. Beim Klicken auf die Ereignisse werden die wichtigsten Ereignisse angezeigt, und es wird ein Link zur Event Management-Inventarseite bereitgestellt, die so gefiltert ist, dass die aktiven Ereignisse in dieser Kategorie angezeigt werden.

Am oberen Rand des Dashboard lässt sich auswählen, ob die Panels Informationen für alle überwachten Cluster („Alle Cluster“) oder für einen einzelnen Cluster anzeigen. Zunächst lässt sich der Status aller Cluster anzeigen, und anschließend kann zu einzelnen Clustern gewechselt werden, wenn detaillierte Informationen angezeigt werden sollen.

Einige der unten aufgeführten Bereiche werden je nach Ihrer Konfiguration im Dashboard angezeigt.

Bereich „Managementaktionen“

Es gibt bestimmte Probleme, die Unified Manager umfassend diagnostizieren und mit einer einzigen Lösung beheben kann. Falls verfügbar, werden diese Lösungen in diesem Bereich mit einer Schaltfläche **Fix It** oder **Fix All** angezeigt. Diese Probleme können direkt in Unified Manager behoben werden, ohne dass ONTAP System Manager oder die ONTAP CLI verwendet werden muss. Zum Anzeigen aller Probleme steht "Direktes Beheben von ONTAP Problemen in Unified Manager" Weitere Informationen zur Verfügung.

Kapazitätsbereich

Bei der Anzeige aller Cluster zeigt dieses Panel für jeden Cluster die physisch genutzte Kapazität (nach Anwendung von Storage-Effizienzeinsparungen) und die physisch verfügbare Kapazität (ohne potenzielle Storage-Effizienzeinsparungen), die Anzahl der Tage bis zur voraussichtlichen vollständigen Auslastung der Festplatten sowie das Datenreduktionsverhältnis (ohne Snapshot Kopien) auf Grundlage der konfigurierten ONTAP Storage-Effizienzeinstellungen an. Außerdem wird die genutzte Kapazität für alle konfigurierten Cloud-Tiers aufgeführt. Durch Klicken auf das Balkendiagramm wird die Seite „Aggregates Inventory“ für diesen Cluster geöffnet. Durch Klicken auf den Text „Days To Full“ wird eine Meldung angezeigt, die das Aggregat mit der geringsten Anzahl verbleibender Kapazitätstage angibt; durch Klicken auf den Aggregatnamen werden weitere Details angezeigt.

Bei der Anzeige eines einzelnen Clusters zeigt dieses Fenster die physisch belegte Kapazität und die physisch verfügbare Kapazität für die Datenaggregate an, sortiert nach jedem einzelnen Festplattentyp auf dem lokalen Tier sowie für den Cloud Tier. Durch Klicken auf das Balkendiagramm für einen Festplattentyp gelangen Sie zur Inventarseite „Volumes“ für die Volumes, die diesen Festplattentyp verwenden.

Panel „Performance Capacity“

Bei der Anzeige aller Cluster zeigt dieses Panel für jeden Cluster den Wert der Performance-Kapazität an, gemittelt über die vorherige 1 Stunde, sowie die Anzahl der Tage, bis die Performance-Kapazität die Obergrenze erreicht, basierend auf der täglichen Wachstumsrate. Durch Klicken auf das Balkendiagramm wird die Nodes-Inventarseite für diesen Cluster geöffnet. Zu beachten ist, dass auf der Nodes-Inventarseite die Performance-Kapazität angezeigt wird, gemittelt über die vorherigen 72 Stunden. Durch Klicken auf den Text „Days To Full“ wird eine Meldung angezeigt, die den Node mit der geringsten Anzahl verbleibender Tage der Performance-Kapazität identifiziert; durch Klicken auf den Node-Name werden weitere Details angezeigt.

Beim Anzeigen eines einzelnen Clusters werden in diesem Panel der Prozentsatz der genutzten Cluster-Performancekapazität, die Gesamt-IOPS und der Gesamtdurchsatz (MB/s) sowie die Anzahl der Tage angezeigt, bis voraussichtlich jede dieser drei Kennzahlen ihren oberen Grenzwert erreicht.

Workload IOPS Panel

Bei der Ansicht eines einzelnen Clusters zeigt dieses Panel die Gesamtzahl der Workloads an, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden, und die Anzahl für jeden Datenträgertyp, wenn sich der Mauszeiger über dem Diagramm befindet.

Bereich Workload-Performance

Dieses Panel zeigt die Gesamtzahl der konformen und nicht konformen Workloads an, die jeder Richtlinie für Performance Service Level (PSL) zugewiesen sind. Außerdem wird die Anzahl der Workloads angezeigt, denen kein PSL zugewiesen ist. Ein Klick auf ein Balkendiagramm führt auf der Seite „Workloads“ zu den konformen Workloads, die dieser Richtlinie zugewiesen sind. Ein Klick auf die Zahl, die auf das Balkendiagramm folgt, führt zu den konformen und nicht konformen Workloads, die dieser Richtlinie zugewiesen sind.

Sicherheitsbereich

Das Sicherheitspanel zeigt den allgemeinen Sicherheitsstatus für alle Cluster oder einen einzelnen Cluster an, je nach Ihrer aktuellen Ansicht. Dieses Panel zeigt Folgendes an:

- eine Liste der Sicherheitsereignisse, die in den letzten 24 Stunden eingegangen sind. Durch Klicken auf ein Ereignis werden die Details auf der Seite „Ereignisdetails“ angezeigt.
- Sicherheitsstatus des Clusters (Anzahl der konformen und nicht konformen Cluster)
- der Sicherheitsstatus der Storage VMs (Anzahl der konformen und nicht konformen Storage VMs)
- der Verschlüsselungsstatus des Volumes (Anzahl der verschlüsselten bzw. unverschlüsselten Volumes)
- der Anti-Ransomware-Status der Volumes (Anzahl der Volumes, für die Anti-Ransomware aktiviert oder deaktiviert ist)

Sie können auf die Balkendiagramme der konformen und nicht konformen Cluster, Storage-VMs, verschlüsselten und unverschlüsselten Volumes sowie des Anti-Ransomware-Status der Volumes klicken, um zu den jeweiligen Seiten zu gelangen und die Sicherheitsdetails der gefilterten Cluster, Storage-VMs und Volumes anzuzeigen.

Die Einhaltung der Vorschriften basiert auf den "NetApp Security Hardening Guide für ONTAP 9". Mit dem Pfeil nach rechts oben im Fenster lassen sich auf der Seite „Sicherheit“ die Sicherheitsdetails für alle Cluster anzeigen. Informationen dazu finden Sie unter "Anzeigen des detaillierten Sicherheitsstatus für Cluster und Storage VMs".

Bereich „Data Protection“

Dieses Panel zeigt die Zusammenfassung des Datenschutzes für einen oder alle Cluster in einem Datacenter an. Es zeigt die Gesamtzahl der Datenschutzereignisse, MetroCluster Ereignisse und die Anzahl der aktiven Ereignisse an, die in den letzten 24 Stunden in ONTAP ausgelöst wurden. Über den Link in jedem dieser Ereignisse gelangen Sie zur Seite Event details. Über den Link **View All** können alle aktiven Schutzereignisse auf der Bestandsseite Event Management angezeigt werden. Das Panel zeigt Folgendes an:

- Die Volume-Anzahl in einem Cluster oder in allen Clustern eines durch Snapshot copies geschützten Datacenters.
- Die Volume-Anzahl in einem Cluster oder in allen Clustern eines Datacenter, die durch SnapMirror Beziehungen geschützt sind. Bei SnapMirror Beziehungen wird die Volume-Anzahl im Quell-Cluster berücksichtigt.
- Die Anzahl der Cluster oder aller Cluster in einem Datacenter, die durch eine MetroCluster Konfiguration

über IP oder FC geschützt sind.

- Die Anzahl der Volume-Beziehungen mit einer auf dem Verzögerungsstatus basierenden SnapMirror Recovery Point Objective (RPO)-Verzögerung.

Beim Bewegen des Mauszeigers lassen sich die jeweiligen Anzahlen und Legenden anzeigen. Über den Pfeil nach rechts oben im Bereich lassen sich die Details für einen einzelnen oder für alle Cluster auf der Seite „Data Protection“ anzeigen. Außerdem sind folgende Elemente anklickbar:

- Die Balkendiagramme für ungeschützte Volumes und durch Snapshot Kopien geschützte Volumes führen zur Seite „Volumes“, auf der die Details angezeigt werden.
- Die Balkendiagramme für die Cluster, die durch die MetroCluster Konfiguration geschützt sind oder nicht geschützt sind, führen zur Seite „Cluster“, auf der die Details angezeigt werden.
- Die Balkendiagramme für alle Beziehungen führen zur Seite „Beziehungen“, auf der die Details anhand des Quell-Clusters gefiltert werden.

Weitere Informationen sind unter "Anzeigen des Volume-Schutzstatus" verfügbar.

Bereich „Nutzungsübersicht“

Bei der Anzeige aller Cluster können Sie die Cluster nach höchster IOPS-Zahl, höchstem Durchsatz (MB/s) oder höchster genutzter physischer Kapazität sortieren.

Bei der Anzeige eines einzelnen Clusters können Sie die Workloads sortiert nach den höchsten IOPS, dem höchsten Durchsatz (MB/s) oder der höchsten genutzten logischen Kapazität anzeigen.

Verwandte Informationen

"Beheben von Problemen mithilfe automatischer Korrekturmaßnahmen von Unified Manager"

"Anzeigen von Informationen zu Performance-Ereignissen"

"Managen der Performance mithilfe von Informationen zur Performance-Kapazität und zu verfügbaren IOPS"

"Seite mit Details zu Volume/Systemstatus"

"Performance Ereignisanalyse und Benachrichtigung"

"Beschreibung der Schweregrade von Ereignissen"

"Quellen von Performance-Ereignissen"

"Cluster-Sicherheitsziele managen"

"Sie können die Cluster-Performance auf der Performance Cluster Landing page überwachen."

"Überwachung der Performance mithilfe der Seiten zur Performance-Inventur"

ONTAP Probleme direkt aus Unified Manager beheben oder managen

ONTAP Probleme oder Funktionen direkt über Active IQ Unified Manager verwalten

Sie können bestimmte ONTAP Probleme beheben oder bestimmte ONTAP Funktionen direkt über die Unified Manager Benutzeroberfläche managen, anstatt den ONTAP

System Manager oder die ONTAP CLI verwenden zu müssen. Die Option “Management Actions” bietet Korrekturen für eine Reihe von ONTAP Problemen, die Unified Manager Ereignisse ausgelöst haben.

Probleme lassen sich direkt auf der Seite „Management Actions“ beheben, wenn im linken Navigationsbereich die Option **Management Actions** ausgewählt wird. Management Actions ist außerdem über den Bereich „Management Actions“ im Dashboard, auf der Seite „Event details“ und über die Auswahl „Workload Analysis“ im linken Navigationsmenü verfügbar.

Unified Manager kann bestimmte Probleme umfassend diagnostizieren und eine einzelne Lösung bereitstellen. Für bestimmte ONTAP Funktionen, wie z. B. Anti-Ransomware Monitoring, führt Unified Manager interne Prüfungen durch und empfiehlt spezifische Maßnahmen. Sofern verfügbar, werden diese Lösungen in Management Actions mit einer Schaltfläche **Fix It** angezeigt. Über die Schaltfläche **Fix It** lässt sich das Problem beheben. Hierfür ist die Rolle Application Administrator oder Storage Administrator erforderlich.

Unified Manager sendet ONTAP Befehle an den Cluster, um die angeforderte Korrektur durchzuführen. Nach Abschluss der Korrektur gilt das Ereignis als obsolet.

Einige Verwaltungsaktionen ermöglichen es Ihnen, dasselbe Problem auf mehreren Storage Objekten mit der Schaltfläche **Fix All** zu beheben. Beispielsweise kann es 5 Volumes mit dem Ereignis "Volume Space Full" geben, das durch Klicken auf die Verwaltungsaktion **Fix All** für "Enable volume autogrow" behoben werden könnte. Mit einem Klick können Sie dieses Problem auf 5 Volumes beheben.

Informationen zu den ONTAP Problemen und Funktionen, die Sie durch automatische Behebung managen können, finden Sie unter "Welche Probleme kann Unified Manager beheben".

Informationen zu den Schaltflächenoptionen „Reparieren“ und „Alle reparieren“ in Active IQ Unified Manager

Auf der Seite „Verwaltungsaktionen“ steht die Schaltfläche **Fix It** oder **Fix All** zur Verfügung, um Probleme zu beheben, über die Unified Manager durch ein Ereignis benachrichtigt wurde.

Wir empfehlen, bei Bedarf auf die Schaltflächen zu klicken, um ein Problem zu beheben. Sollten Sie sich jedoch nicht sicher sein, ob Sie das Problem wie von Unified Manager empfohlen beheben möchten, können Sie die folgenden Aktionen ausführen:

Was möchten Sie tun?	Aktion
Unified Manager das Problem bei allen identifizierten Objekten beheben lassen.	Die Auswahl erfolgt über die Schaltfläche **Fix All**.
Das Problem wird derzeit für keines der identifizierten Objekte behoben, und diese Verwaltungsaktion bleibt ausgeblendet, bis das Ereignis erneut auftritt.	Über den Abwärtspfeil kann **Alle verwerfen** ausgewählt werden.
Das Problem nur bei einigen der identifizierten Objekte beheben.	Ein Klick auf den Namen der Verwaltungsmaßnahme erweitert die Liste und zeigt alle einzelnen **Fix It** -Aktionen an. Anschließend folgen die Schritte zum Beheben oder Verwerfen einzelner Verwaltungsmaßnahmen.

Was möchten Sie tun?	Aktion
Unified Manager behebt das Problem.	Auf die Schaltfläche **Fix It** klicken.

Was möchten Sie tun?	Aktion
Das Problem wird zu diesem Zeitpunkt nicht behoben, und diese Verwaltungsaktion bleibt ausgeblendet, bis das Ereignis erneut auftritt.	Auf den Abwärtspfeil und anschließend auf **Dismiss** klicken.
Die Anzeige der Details zu diesem Ereignis erleichtert das Verständnis des Problems.	• Nach Auswahl der Schaltfläche **Fix It** kann die Korrektur im daraufhin angezeigten Dialogfeld überprüft werden. • Über den Abwärtspfeil und **Ereignisdetails anzeigen** lässt sich die Seite mit den Ereignisdetails öffnen. Anschließend kann auf einer der beiden daraufhin angezeigten Seiten **Fix It** ausgewählt werden, wenn das Problem behoben werden soll.
Die Anzeige der Details dieses Storage Objekts erleichtert das Verständnis des Problems.	Wenn Sie den Namen des Storage Objekts auswählen, werden Details entweder im Performance Explorer oder auf der Seite „Health Details“ angezeigt.

In manchen Fällen wird die Korrektur in der nächsten 15-Minuten-Konfigurationsabfrage berücksichtigt. In anderen Fällen kann es viele Stunden dauern, bis die Konfigurationsänderung verifiziert und das entsprechende Ereignis als veraltet eingestuft wird.

Die Liste der abgeschlossenen oder laufenden Verwaltungsaktionen lässt sich über das Filtersymbol anzeigen, indem **Abgeschlossen** oder **In Bearbeitung** ausgewählt wird.

Alle Vorgänge von Fix All werden seriell ausgeführt, sodass beim Anzeigen des Bereichs **In Progress** einige Objekte den Status **In Progress** und andere den Status **Scheduled** haben; das bedeutet, dass sie noch auf ihre Implementierung warten.

Status der Managementaktionen zur Behebung von Problemen in Active IQ Unified Manager anzeigen

Auf der Seite „Management Actions“ können Sie den Status aller Management-Aktionen anzeigen, die Sie zur Behebung ausgewählt haben. Die meisten Aktionen werden relativ schnell als **Completed** angezeigt, nachdem Unified Manager den ONTAP-Befehl an den Cluster gesendet hat. Einige Aktionen, etwa das Verschieben eines Volumes, können jedoch länger dauern.

Auf der Seite „Verwaltungsaktionen“ stehen drei Filter zur Verfügung:

- **Abgeschlossen** zeigt sowohl Managementaktionen an, die erfolgreich abgeschlossen wurden, als auch solche, die fehlgeschlagen sind. **Fehlgeschlagen** Aktionen geben einen Grund für den Fehler an, sodass Sie das Problem manuell beheben können.
- **In Bearbeitung** zeigt sowohl die Managementmaßnahmen an, die gerade umgesetzt werden, als auch diejenigen, deren Umsetzung geplant ist.
- **Empfohlen** zeigt alle Verwaltungsaktionen an, die aktuell für alle überwachten Cluster aktiv sind.

Schritte

1. Im linken Navigationsbereich ist **Management Actions** auszuwählen. Alternativ kann oben im Bereich **Management Actions** auf dem **Dashboard** ⋮ ausgewählt und die gewünschte Ansicht gewählt werden.

Die Seite „Verwaltungsaktionen“ wird angezeigt.

2. Sie können auf das Pfeilsymbol neben der Verwaltungsaktion im Feld **Beschreibung** klicken, um Details zum Problem und den Befehl anzuzeigen, mit dem das Problem behoben wird.
3. Aktionen, die **fehlgeschlagen** sind, lassen sich anzeigen, indem in der Ansicht **Abgeschlossen** nach der Spalte **Status** sortiert wird. Für denselben Zweck kann auch das **Filter**-Tool verwendet werden.
4. Wenn weitere Informationen zu einer fehlgeschlagenen Verwaltungsaktion angezeigt werden sollen oder eine empfohlene Verwaltungsaktion korrigiert werden soll, kann nach einem Klick auf das Caret-Symbol neben der Verwaltungsaktion im erweiterten Bereich auf **View Event Detail** geklickt werden. Auf dieser Seite ist die Schaltfläche **Fix It** verfügbar.

Informationen zu ONTAP Problemen, die Active IQ Unified Manager beheben kann

Durch die Nutzung der automatischen Problembehebungsfunktion von Active IQ Unified Manager können Sie bestimmte ONTAP Probleme beheben oder bestimmte ONTAP Funktionen, wie z. B. die Anti-Ransomware-Überwachung, effektiv über Unified Manager managen.

Diese Tabelle beschreibt die ONTAP Probleme oder Funktionen, die direkt über die Schaltfläche **Fix It** oder **Fix All** in der Unified Manager Weboberfläche gemanagt werden können.

Name und Beschreibung des Ereignisses	Managementaktion	"Fix It"-Vorgang
Speicherplatz des Volumes voll Das Volume ist fast voll und hat den Schwellenwert für volle Kapazität überschritten. Dieser Schwellenwert ist standardmäßig auf 90 % der Größe des Volume festgelegt.	Aktivieren des automatischen Volume-Wachstums	Unified Manager stellt fest, dass für dieses Volume kein automatisches Vergrößern konfiguriert ist, und aktiviert diese Funktion daher, damit die Kapazität des Volumes bei Bedarf zunimmt.
Inodes voll Dieses Volume hat keine Inodes mehr und kann keine neuen Dateien mehr aufnehmen.	Erhöhung der Anzahl der Inodes auf dem Volume	Erhöht die Anzahl der Inodes im Volume um 2 Prozent.
Abweichung bei der Storage-Tier-Richtlinie erkannt Das Volume enthält viele inaktive Daten, und die aktuelle Tiering-Richtlinie ist auf „snapshot-only“ oder „none“ eingestellt.	Aktivierung des automatischen Cloud-Tiering	Da sich das Volume bereits auf einem FabricPool befindet, wird die Tiering-Richtlinie in „auto“ geändert, sodass inaktive Daten in das kostengünstigere Cloud-Tier verschoben werden.
Storage-Tier-Nichtübereinstimmung erkannt Das Volume enthält viele inaktive Daten, befindet sich aber nicht auf einer Cloud-fähigen Storage-Tier (FabricPool).	Ändern des Storage-Tiers von Volumes	Verschieben des Volume auf den Cloud-fähigen Storage-Tier und Festlegen der Tiering-Richtlinie auf „auto“, um inaktive Daten auf den Cloud-Tier zu verschieben.

Name und Beschreibung des Ereignisses	Managementaktion	"Fix It"-Vorgang
Revisionsprotokoll deaktiviert Das Revisionsprotokoll ist für die Storage VM nicht aktiviert	Revisionsprotokollierung für die Storage VM aktivieren	Aktiviert die Revisionsprotokollierung auf der Storage-VM. Voraussetzung ist, dass für die Storage VM bereits ein lokaler oder entfernter Speicherort für das Revisionsprotokoll konfiguriert ist.
Anmeldebanner deaktiviert Zur Erhöhung der Sicherheit sollte das Anmeldebanner für den Cluster aktiviert werden, damit die Zugriffsbeschränkungen klar erkennbar sind.	Anmeldebanner für den Cluster festlegen	Legt das Cluster-Anmeldebanner auf „`Access restricted to authorized users`“ fest.
Anmeldebanner deaktiviert Das Anmeldebanner für die Storage-VM sollte aktiviert sein, um die Sicherheit zu erhöhen, indem die Zugriffsbeschränkungen klar dargestellt werden.	Anmeldebanner für die Storage VM festlegen	Legt das Anmeldebanner der Storage VM auf „Zugriff nur für autorisierte Benutzer“ fest.
SSH verwendet unsichere Verschlüsselungsalgorithmen Chiffren mit dem Suffix "-cbc" gelten als unsicher.	Unsichere Chiffren aus dem Cluster entfernen	Entfernt die unsicheren Verschlüsselungsverfahren — wie beispielsweise aes192-cbc und aes128-cbc — aus dem Cluster.
SSH verwendet unsichere Verschlüsselungsalgorithmen Chiffren mit dem Suffix "-cbc" gelten als unsicher.	Unsichere Verschlüsselungsverfahren aus der Storage VM entfernen	Entfernt unsichere Verschlüsselungsverfahren wie aes192-cbc und aes128-cbc aus der Storage VM.
AutoSupport HTTPS-Transport deaktiviert Das Transportprotokoll, das zum Senden von AutoSupport Nachrichten an den technischen Support verwendet wird, sollte verschlüsselt sein.	HTTPS als Transportprotokoll für AutoSupport Nachrichten festlegen	Legt HTTPS als Transportprotokoll für AutoSupport Nachrichten auf dem Cluster fest.

Name und Beschreibung des Ereignisses	Managementaktion	"Fix It"-Vorgang
Schwellenwert für Cluster-Lastungleichgewicht überschritten Zeigt an, dass die Last zwischen den Knoten im Cluster unausgewogen verteilt ist. Dieses Ereignis wird ausgelöst, wenn die Varianz der genutzten Performance-Kapazität zwischen den Knoten mehr als 30 % beträgt.	Ausgleichen von Cluster-Workloads	Unified Manager ermittelt das optimale Volume, das von einem Knoten auf den anderen verschoben werden soll, um das Ungleichgewicht zu verringern, und verschiebt anschließend das Volume.
Schwellenwert für Kapazitätsungleichgewicht im Cluster überschritten Zeigt an, dass die Kapazität unter den Aggregaten im Cluster unausgewogen ist. Dieses Ereignis wird generiert, wenn die Abweichung der genutzten Kapazität zwischen den Aggregaten mehr als 70 % beträgt.	Clusterkapazität ausgleichen	Unified Manager ermittelt das optimale Volume, das von einem Aggregat zu einem anderen verschoben werden soll, um das Ungleichgewicht zu verringern, und verschiebt das Volume dann.
Schwellenwert für die genutzte Performance-Kapazität überschritten Diese Meldung weist darauf hin, dass der Knoten überlastet werden könnte, wenn die Auslastung nicht durch einen oder mehrere hochaktive Workloads reduziert wird. Dieses Ereignis wird generiert, wenn der Wert für die genutzte Node-Performance-Kapazität länger als 12 Stunden über 100 % liegt.	Hohe Last auf dem Knoten begrenzen	Unified Manager ermittelt das Volume mit den höchsten IOPS und wendet eine QoS-Richtlinie an, die auf den historischen erwarteten und maximalen IOPS-Werten basiert, um die Last auf dem Knoten zu reduzieren.
Schwellenwert für dynamische Ereigniswarnungen überschritten Zeigt an, dass der Knoten aufgrund der ungewöhnlich hohen Last einiger Workloads bereits überlastet ist.	Reduzierung der Überlastung im Node	Unified Manager ermittelt das Volume mit den höchsten IOPS und wendet eine QoS-Richtlinie an, die auf den historischen erwarteten und maximalen IOPS-Werten basiert, um die Last auf dem Knoten zu reduzieren.
Eine Übernahme ist nicht möglich Failover ist derzeit deaktiviert, daher würde der Zugriff auf die Ressourcen des Knotens während eines Ausfalls oder Neustarts verloren gehen, bis der Knoten wieder verfügbar ist.	Aktivierung des Node-Failover	Unified Manager sendet den entsprechenden Befehl, um Failover auf allen Knoten im Cluster zu aktivieren.

Name und Beschreibung des Ereignisses	Managementaktion	"Fix It"-Vorgang
Die Option Cf.takeover.on_panic ist auf OFF konfiguriert Die nodeshell Option "cf.takeover.on_panic" ist auf **off** gesetzt, was auf HA-konfigurierten Systemen zu Problemen führen könnte.	Aktivierung der Übernahme bei Panic	Unified Manager sendet den entsprechenden Befehl an den Cluster, um diese Einstellung auf **on** zu ändern.
Deaktivieren der NodeShell-Option snapmirror.enable Die alte nodeshell-Option "snapmirror.enable" ist auf **on** gesetzt, was nach dem Upgrade auf ONTAP 9.3 oder höher zu Problemen beim Bootvorgang führen kann.	Die Option snapmirror.enable auf off setzen	Unified Manager sendet den entsprechenden Befehl an den Cluster, um diese Einstellung in **off** zu ändern.
Telnet aktiviert Dies deutet auf ein potenzielles Sicherheitsproblem hin, da Telnet unsicher ist und Daten unverschlüsselt überträgt.	Deaktivieren von Telnet	Unified Manager sendet den entsprechenden Befehl an den Cluster, um Telnet zu deaktivieren.
Konfiguration des Anti-Ransomware-Lernens für Storage-VMs Prüft regelmäßig, ob Cluster über Lizenzen für die Anti-Ransomware-Überwachung verfügen. Validiert, ob eine Storage VM in einem solchen Cluster ausschließlich NFS- oder SMB-Volumes unterstützt.	Storage VMs in einen `learning`Modus zur Anti-Ransomware-Überwachung versetzen	Unified Manager setzt die Anti-Ransomware-Überwachung für die Storage-VMs über die Cluster-Management-Konsole in den `learning`Status. Bei allen neu auf der Storage-VM erstellten Volumes wechselt die Anti-Ransomware-Überwachung automatisch in einen Lernmodus. Dadurch kann ONTAP die Aktivitätsmuster auf den Volumes erlernen und Anomalien infolge potenziell bösartiger Angriffe erkennen.
Konfiguration des Lernens für den Ransomware-Schutz von Volumes Prüft regelmäßig, ob Cluster über Lizenzen für die Anti-Ransomware-Überwachung verfügen. Prüft, ob ein Volume in einem solchen Cluster nur NFS- oder SMB-Services unterstützt.	Versetzen von Volumes in den `learning` Modus der Anti-Ransomware-Überwachung	Unified Manager setzt die Anti-Ransomware-Überwachung für die Volumes über die Cluster-Management-Konsole in den `learning`Status. Durch diese Aktivierung kann ONTAP die Aktivitätsmuster auf den Volumes analysieren und Anomalien aufgrund potenzieller bösartiger Angriffe erkennen.

Name und Beschreibung des Ereignisses	Managementaktion	"Fix It"-Vorgang
Anti-Ransomware für Volumes aktivieren Prüft regelmäßig, ob Cluster über Lizenzen für die Anti-Ransomware-Überwachung verfügen. Erkennt, ob sich die Volumes länger als 45 Tage im `learning`Anti-Ransomware-Überwachungsmodus befinden, und ermittelt die Aussicht, sie in den aktiven Modus zu versetzen.	Volumes in den `active`Modus der Anti-Ransomware-Überwachung versetzen	Unified Manager setzt die Anti-Ransomware-Überwachung auf `active` den Volumes über die Cluster-Management-Konsole. Durch diese Aktivierung kann ONTAP die Aktivitätsmuster auf den Volumes analysieren, Anomalien aufgrund potenziell bösartiger Angriffe erkennen und Warnmeldungen für Datenschutzmaßnahmen erstellen.
Volume Anti-Ransomware deaktivieren Prüft regelmäßig, ob Cluster über Lizenzen für die Anti-Ransomware-Überwachung verfügen. Erkennt wiederholte Benachrichtigungen während der aktiven Anti-Ransomware-Überwachung der Volumes (z. B. mehrere Warnungen vor potenziellen Ransomware-Angriffen innerhalb von 30 Tagen).	Deaktivierung der Anti-Ransomware-Überwachung auf Volumes	Unified Manager deaktiviert die Anti-Ransomware-Überwachung der Volumes über die Cluster-Management-Konsole.

Verwaltungsaktionen in Active IQ Unified Manager mit Skripten überschreiben

Sie können benutzerdefinierte Skripte erstellen und sie Warnmeldungen zuordnen, um für bestimmte Ereignisse spezifische Aktionen auszuführen, anstatt die standardmäßigen Verwaltungsaktionen zu verwenden, die auf der Seite „Management Actions“ oder im Unified Manager Dashboard dafür verfügbar sind.

Wenn Sie für einen Ereignistyp bestimmte Aktionen ausführen und diese nicht als Teil der von Unified Manager bereitgestellten Management Actions Funktion beheben möchten, können Sie ein benutzerdefiniertes Skript für die jeweilige Aktion konfigurieren. Anschließend können Sie das Skript einer Warnung für diesen Ereignistyp zuordnen und solche Ereignisse einzeln bearbeiten. In diesem Fall werden auf der Seite Management Actions oder im Unified Manager Dashboard keine Verwaltungsaktionen für diesen spezifischen Ereignistyp generiert.

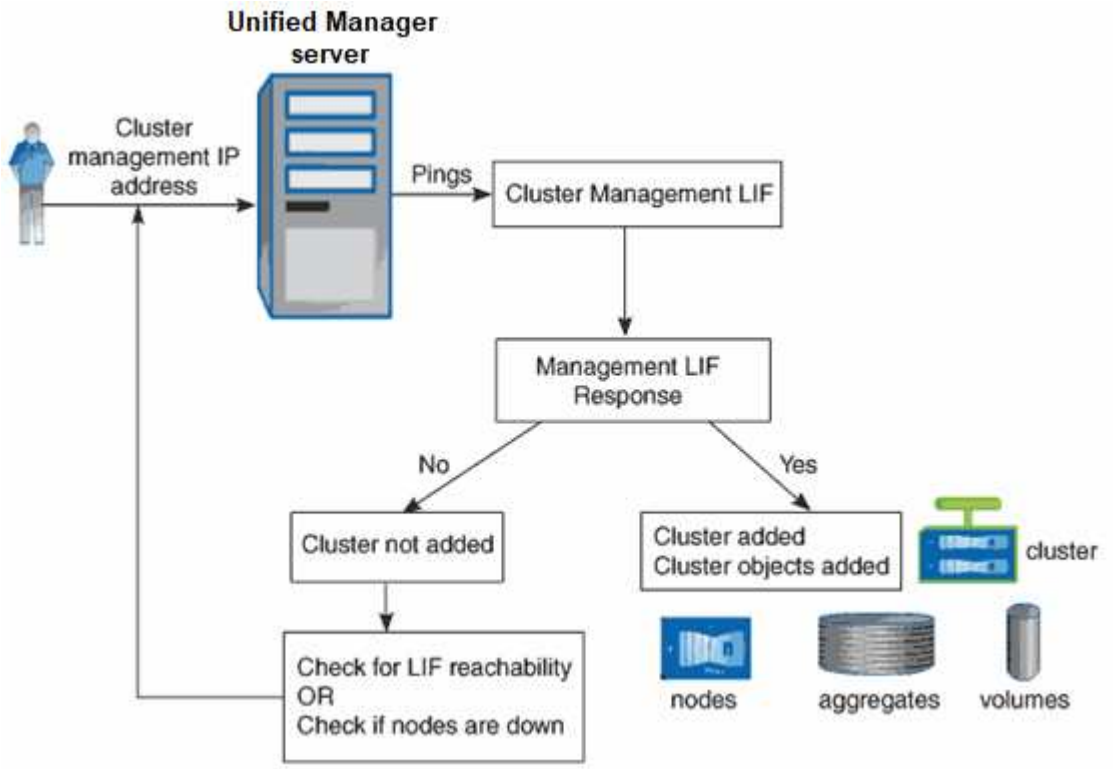
Cluster verwalten

Informationen zur Funktionsweise des Cluster-Erkennungsprozesses in Active IQ Unified Manager

Nachdem Sie einen Cluster zu Unified Manager hinzugefügt haben, erkennt der Server die Clusterobjekte und fügt sie seiner Datenbank hinzu. Das Verständnis der Funktionsweise dieses Erkennungsprozesses unterstützt Sie beim Managen der Cluster Ihres Unternehmens und ihrer Objekte.

Das Überwachungsintervall für die Erfassung von Clusterkonfigurationsinformationen beträgt 15 Minuten. Nachdem Sie beispielsweise einen Cluster hinzugefügt haben, dauert es 15 Minuten, bis die Clusterobjekte in der Unified Manager UI angezeigt werden. Dieser Zeitraum gilt auch für Änderungen an einem Cluster. Wenn Sie beispielsweise zwei neue Volumes zu einer SVM in einem Cluster hinzufügen, werden diese neuen Objekte nach dem nächsten Abfrageintervall, das bis zu 15 Minuten betragen kann, in der UI angezeigt.

Die folgende Abbildung veranschaulicht den Entdeckungsprozess:



Nachdem alle Objekte für einen neuen Cluster erkannt wurden, beginnt Unified Manager mit der Erfassung historischer Performance-Daten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Erfassung der Datenkontinuität gesammelt. Diese Funktion stellt Ihnen unmittelbar nach dem Hinzufügen eines Clusters Performance-Informationen für mehr als zwei Wochen zur Verfügung. Nach Abschluss des Erfassungszyklus für die Datenkontinuität werden standardmäßig alle fünf Minuten Echtzeit-Performance-Daten für den Cluster erfasst.

Da die Erfassung von 15 Tagen Performance-Daten CPU-intensiv ist, wird empfohlen, die Hinzufügung neuer Cluster zeitlich zu staffeln, damit die Abfragen zur Erfassung der Datenkontinuität nicht gleichzeitig auf zu vielen Clustern ausgeführt werden.

Liste der von Active IQ Unified Manager überwachten Cluster

Auf der Seite „Cluster Setup“ können Sie Ihre Clusterübersicht einsehen. Dort finden Sie Details zu den Clustern, wie z. B. deren Name, IP-Adresse und Kommunikationsstatus.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritt

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.

Alle Cluster in Ihrer vom Unified Manager gemanagten Storage-Umgebung werden angezeigt. Die Clusterliste ist nach der Spalte für den Schweregrad des Erfassungsstatus sortiert. Durch Klicken auf eine Spaltenüberschrift können die Cluster nach verschiedenen Spalten sortiert werden.

Cluster zu Active IQ Unified Manager hinzufügen

Sie können Active IQ Unified Manager einen Cluster hinzufügen, damit Sie den Cluster überwachen können. Dies umfasst die Möglichkeit, Clusterinformationen wie den Systemstatus, die Kapazität, die Performance und die Konfiguration des Clusters abzurufen, damit Sie auftretende Probleme erkennen und beheben können.

Bevor Sie beginnen

- Sie benötigen die Rolle des Anwendungsadministrators oder die Rolle des Storage-Administrators.
- Sie benötigen folgende Informationen:
  - Unified Manager unterstützt lokale ONTAP Cluster, ONTAP Select, Cloud Volumes ONTAP.
  - Sie benötigen den Hostnamen oder die Cluster-Management-IP-Adresse (IPv4 oder IPv6) für den Cluster.

    Bei Verwendung des Hostnamens muss dieser zur Clusterverwaltungs-IP-Adresse für die Clusterverwaltungs-LIF aufgelöst werden. Bei Verwendung einer Knotenverwaltungs-LIF schlägt der Vorgang fehl.
  - Sie benötigen den Benutzernamen und das Passwort, um auf den Cluster zugreifen zu können.

    Dieses Konto muss die Rolle *admin* besitzen, wobei der Anwendungszugriff auf *ontapi*, *amqp*, *console* und *http* festgelegt sein muss.
  - Sie müssen die Portnummer kennen, um sich über das HTTPS-Protokoll mit dem Cluster zu verbinden (typischerweise Port 443).
  - Auf dem Cluster muss ONTAP Softwareversion 9.9 oder höher ausgeführt werden.
  - Auf dem Unified Manager Server muss ausreichend Speicherplatz vorhanden sein. Das Hinzufügen eines Clusters zum Server ist nicht möglich, wenn bereits mehr als 90 % des Speicherplatzes belegt sind.
  - Sie verfügen über die erforderlichen Zertifikate:

    SSL-Zertifikat (HTTPS): Dieses Zertifikat gehört Unified Manager. Bei einer Neuinstallation von Unified Manager wird standardmäßig ein selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt, es für mehr Sicherheit auf ein von einer Zertifizierungsstelle signiertes Zertifikat umzustellen. Wenn das Serverzertifikat abläuft, sollten Sie es neu generieren und Unified Manager neu starten, damit die Services das neue Zertifikat übernehmen. Weitere Informationen zum Regenerieren von SSL-Zertifikaten enthält "Generieren eines HTTPS-Sicherheitszertifikats".

    EMS-Zertifikat: Dieses Zertifikat gehört dem Unified Manager. Es dient zur Authentifizierung von EMS-Benachrichtigungen, die von ONTAP empfangen werden.

    Zertifikate für die gegenseitige TLS-Kommunikation: Werden während der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatbasierte Authentifizierung ist für einen Cluster abhängig von der ONTAP Version aktiviert. Wenn auf einem Cluster eine ONTAP Version niedriger als 9.5 ausgeführt wird, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

Die zertifikatbasierte Authentifizierung ist für einen Cluster nicht automatisch aktiviert, wenn Sie eine ältere Version von Unified Manager aktualisieren. Sie können sie jedoch aktivieren, indem Sie die Clusterdetails ändern und speichern. Wenn das Zertifikat abläuft, müssen Sie es neu generieren, um das neue Zertifikat einzubinden. Weitere Informationen zum Anzeigen und Neugenerieren des Zertifikats finden Sie unter "Cluster bearbeiten".

- Über die Web-Benutzeroberfläche lässt sich ein Cluster hinzufügen, und die zertifikatbasierte Authentifizierung wird dabei automatisch aktiviert.
- Sie können einen Cluster über Unified Manager CLI hinzufügen, die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie einen Cluster mit Unified Manager CLI hinzufügen, müssen Sie den Cluster anschließend über Unified Manager UI bearbeiten. Unter "Unterstützte Unified Manager CLI-Befehle" finden Sie Informationen zum Hinzufügen eines Clusters mit Unified Manager CLI.
- Wenn die zertifikatbasierte Authentifizierung für einen Cluster aktiviert ist und Sie das Backup von Unified Manager auf einem Server erstellen und es auf einem anderen Unified Manager Server wiederherstellen, bei dem Hostname oder IP-Adresse geändert wurden, kann die Überwachung des Clusters fehlschlagen. Zur Vermeidung dieses Fehlers empfiehlt sich das Bearbeiten und Speichern der Clusterdetails. Weitere Informationen zum Bearbeiten von Clusterdetails finden Sie unter "Cluster bearbeiten".
- Auf Cluster-Level fügt die Active IQ Schnittstelle zwei neue Benutzergruppeneinträge für das Authentifizierungsverfahren „cert“ hinzu.

+
Clusterzertifikate: Dieses Zertifikat gehört ONTAP. Sie können keinen Cluster mit einem abgelaufenen Zertifikat zu Unified Manager hinzufügen. Wenn das Zertifikat bereits abgelaufen ist, müssen Sie es vor dem Hinzufügen des Clusters neu generieren. Informationen zur Zertifikatserstellung finden Sie im entsprechenden Knowledge-Base-Artikel "Erneuern eines ONTAP selbstsignierten Zertifikats in der System Manager Benutzeroberfläche".

- Eine einzelne Instanz von Unified Manager kann eine bestimmte Anzahl von Knoten unterstützen. Wenn Sie eine Umgebung überwachen müssen, die die unterstützte Knotenanzahl überschreitet, müssen Sie eine zusätzliche Instanz von Unified Manager installieren, um einige der Cluster zu überwachen. Die Liste der unterstützten Knotenanzahl finden Sie in der "Unified Manager Best Practices-Leitfaden".

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. Auf der Seite „Cluster Setup“ ist **Add** auszuwählen.
3. Im Dialogfeld „Cluster hinzufügen“ werden die erforderlichen Werte wie erforderlich angegeben; anschließend wird auf **Submit** geklickt.
4. Im Dialogfeld „Host autorisieren“ kann über **Zertifikat anzeigen** die Zertifikatsinformation zum Cluster angezeigt werden.
5. Klicken Sie auf **Ja**.

   Nach dem Speichern der Clusterdetails können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für einen Cluster einsehen.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, prüft Unified Manager das Zertifikat nur beim erstmaligen Hinzufügen des Clusters. Unified Manager prüft das Zertifikat nicht bei jedem API-Aufruf an ONTAP.

Nachdem alle Objekte für einen neuen Cluster erkannt wurden, beginnt Unified Manager mit der Erfassung

historischer Performance-Daten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Erfassung der Datenkontinuität gesammelt. Diese Funktion stellt Ihnen unmittelbar nach dem Hinzufügen eines Clusters Performance-Informationen für mehr als zwei Wochen zur Verfügung. Nach Abschluss des Erfassungszyklus für die Datenkontinuität werden standardmäßig alle fünf Minuten Echtzeit-Performance-Daten für den Cluster erfasst.

- Die Erfassung von 15 Tagen Performance-Daten ist CPU-intensiv. NetApp empfiehlt, das Hinzufügen neuer Cluster zeitlich zu staffeln, damit die Abfragen zur Erfassung der Datenkontinuität nicht gleichzeitig auf zu vielen Clustern ausgeführt werden. Wenn Sie Unified Manager während des Zeitraums der Erfassung der Datenkontinuität neu starten, wird die Erfassung angehalten, und in den Performance-Diagrammen werden Lücken für den fehlenden Zeitraum angezeigt.
- Beim Hinzufügen eines ONTAP Clusters ab Version 9.14.1 erfolgt die Kommunikation über die Cloud-Agent-Funktion. ONTAP erstellt automatisch einen internen Servicekonto-Benutzer mit schreibgeschützten Berechtigungen (z. B. clus-agent-xxxx). Unified Manager stellt die Datenerfassung von diesen Clustern ein, wenn der `clus-agent` Benutzer gelöscht wird.

Falls Sie eine Fehlermeldung erhalten, dass Sie den Cluster nicht hinzufügen können, kann eines der folgenden Probleme vorliegen:

- Wenn die Uhren auf den beiden Systemen nicht synchronisiert sind und das Startdatum des Unified Manager HTTPS-Zertifikats nach dem Datum auf dem Cluster liegt. Die Uhren müssen mithilfe von NTP oder einem ähnlichen Dienst synchronisiert sein.
- Wenn die maximale Anzahl an EMS-Benachrichtigungszielen im Cluster erreicht ist, kann die Unified Manager Adresse nicht hinzugefügt werden. Standardmäßig können im Cluster nur 20 EMS-Benachrichtigungsziele definiert werden.

Verwandte Informationen

"Hinzufügen von Benutzern"

"Anzeigen der Clusterliste und Details"

"Installation eines von einer CA signierten und zurückgegebenen HTTPS-Zertifikats"

Bearbeiten der Clustereinstellungen in Active IQ Unified Manager

Über das Dialogfeld „Cluster bearbeiten“ können Sie die Einstellungen eines bestehenden Clusters ändern, z. B. den Hostnamen oder die IP-Adresse, den Benutzernamen, das Passwort und den Port.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators oder die Rolle des Storage-Administrators.

Ab Unified Manager 9.7 können Cluster nur noch über HTTPS hinzugefügt werden.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. Auf der Seite **Cluster Setup** erfolgt die Auswahl des Clusters, den Sie bearbeiten möchten; anschließend

klicken Sie auf **Edit**.

3. Im Dialogfeld **Edit Cluster** lassen sich die Werte bei Bedarf ändern. + Wenn die Details für einen zu Unified Manager hinzugefügten Cluster geändert wurden, können die Zertifikatsdetails für die Mutual TLS-Kommunikation abhängig von der ONTAP Version angezeigt werden. Weitere Informationen zur ONTAP Version finden Sie unter "Zertifikate für die gegenseitige TLS-Kommunikation". + Die Zertifikatsdetails können über **Certificate Details** angezeigt werden. Wenn das Zertifikat abgelaufen ist, lässt sich das neue Zertifikat über die Schaltfläche **Regenerate** einbinden.
4. Anschließend **Absenden** auswählen.
5. Im Dialogfeld „Host autorisieren“ kann über **Zertifikat anzeigen** die Zertifikatsinformation zum Cluster angezeigt werden.
6. Klicken Sie auf **Ja**.

Verwandte Informationen

"Hinzufügen von Benutzern"

"Anzeigen der Clusterliste und Details"

Entfernung von Clustern aus Active IQ Unified Manager

Sie können einen Cluster aus Unified Manager über die Seite „Cluster Setup“ entfernen. Beispielsweise können Sie einen Cluster entfernen, wenn die Clustererkennung fehlschlägt oder wenn Sie ein Storage-System stilllegen möchten.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators oder die Rolle des Storage-Administrators.

Diese Aufgabe entfernt den ausgewählten Cluster aus Unified Manager. Nach dem Entfernen eines Clusters überwacht Unified Manager ihn nicht mehr. Die bei dem entfernten Cluster registrierte Instanz von Unified Manager wird ebenfalls von dem Cluster abgemeldet.

Durch das Entfernen eines Clusters werden auch alle zugehörigen Storage-Objekte, Verlaufsdaten, Storage Services und alle zugehörigen Ereignisse aus Unified Manager gelöscht. Diese Änderungen werden nach dem nächsten Datenerfassungszyklus auf den Inventar- und Detailseiten angezeigt.



Sie müssen einen Cluster aus Unified Manager entfernen, bevor Sie ihn außer Betrieb nehmen. Wenn der Cluster bereits offline oder nicht erreichbar ist, wenn Sie versuchen, ihn zu entfernen, kann Unified Manager nicht mit dem Cluster kommunizieren, um den Anwendungsdatensatz und die konfigurierten Event Management System (EMS) Abonnements zu entfernen. Dies kann dazu führen, dass der Entfernungsprozess fehlschlägt oder nicht mehr reagiert, bevor er abgeschlossen ist.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. Auf der Seite „Cluster Setup“ wählen Sie den Cluster aus, der entfernt werden soll, und klicken anschließend auf **Remove**.
3. Im Meldungsdialogfeld **Remove Data Source** wird durch Klicken auf **Remove** die Entfernungsanforderung bestätigt.

Verwandte Informationen

"Hinzufügen von Benutzern"

"Anzeigen der Clusterliste und Details"

Cluster in Active IQ Unified Manager erneut erkennen

Auf der Seite „Cluster Setup“ kann ein Cluster manuell erneut identifiziert werden, um die neuesten Informationen über den Systemstatus, den Überwachungsstatus und den Performance-Status des Clusters zu erhalten.

Sie können einen Cluster manuell erneut identifizieren, wenn Sie den Cluster aktualisieren möchten, beispielsweise durch Erhöhen der Größe eines Aggregats, wenn nicht genügend Speicherplatz vorhanden ist, und wenn Unified Manager die von Ihnen vorgenommenen Änderungen identifizieren soll.

Wenn Unified Manager mit OnCommand Workflow Automation (WFA) gekoppelt ist, löst die Kopplung die erneute Erfassung der von WFA zwischengespeicherten Daten aus.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. Auf der Seite **Cluster Setup** erfolgt die Auswahl von **Rediscover**.

   Unified Manager identifiziert den ausgewählten Cluster erneut und zeigt den aktuellen Systemstatus und Performance-Status an.

Verwandte Informationen

"Anzeigen der Clusterliste und Details"

Überwachung der VMware virtuellen Infrastruktur

Informationen dazu, wie Active IQ Unified Manager die virtuelle Infrastruktur von VMware überwacht

Active IQ Unified Manager bietet Transparenz in die virtuellen Maschinen (VMs) Ihrer virtuellen Infrastruktur und ermöglicht die Überwachung und Behebung von Storage- und Performance-Problemen in Ihrer virtuellen Umgebung. Mit dieser Funktion lassen sich Latenzprobleme in Ihrer Storage-Umgebung ermitteln oder Fälle untersuchen, in denen auf Ihrem vCenter Server ein Performance-Ereignis gemeldet wird.

Ein typisches Deployment einer virtuellen Infrastruktur auf ONTAP umfasst verschiedene Komponenten, die sich über Rechen-, Netzwerk- und Storage-Ebenen erstrecken. Performance Verzögerungen in einer VM Applikation können durch eine Kombination von Latenzen verursacht werden, mit denen die verschiedenen Komponenten auf den jeweiligen Ebenen konfrontiert sind. Diese Funktion ist für Storage- und vCenter Server-Administratoren sowie IT-Generalisten nützlich, die ein Performance Problem in einer virtuellen Umgebung analysieren und nachvollziehen müssen, in welcher Komponente das Problem aufgetreten ist.

Sie können jetzt über das Menü vCenter im VMware Bereich auf den vCenter Server zugreifen. In der Vorschau jeder aufgeführten virtuellen Maschine gibt es in der TOPOLOGY VIEW den Link **VCENTER SERVER**, der den vCenter Server in einem neuen Browserfenster öffnet. Sie können auch die Schaltfläche **Expand Topology** verwenden, um den vCenter Server zu öffnen, und auf die Schaltfläche **View in vCenter** klicken, um die Datastores im vCenter Server anzuzeigen.

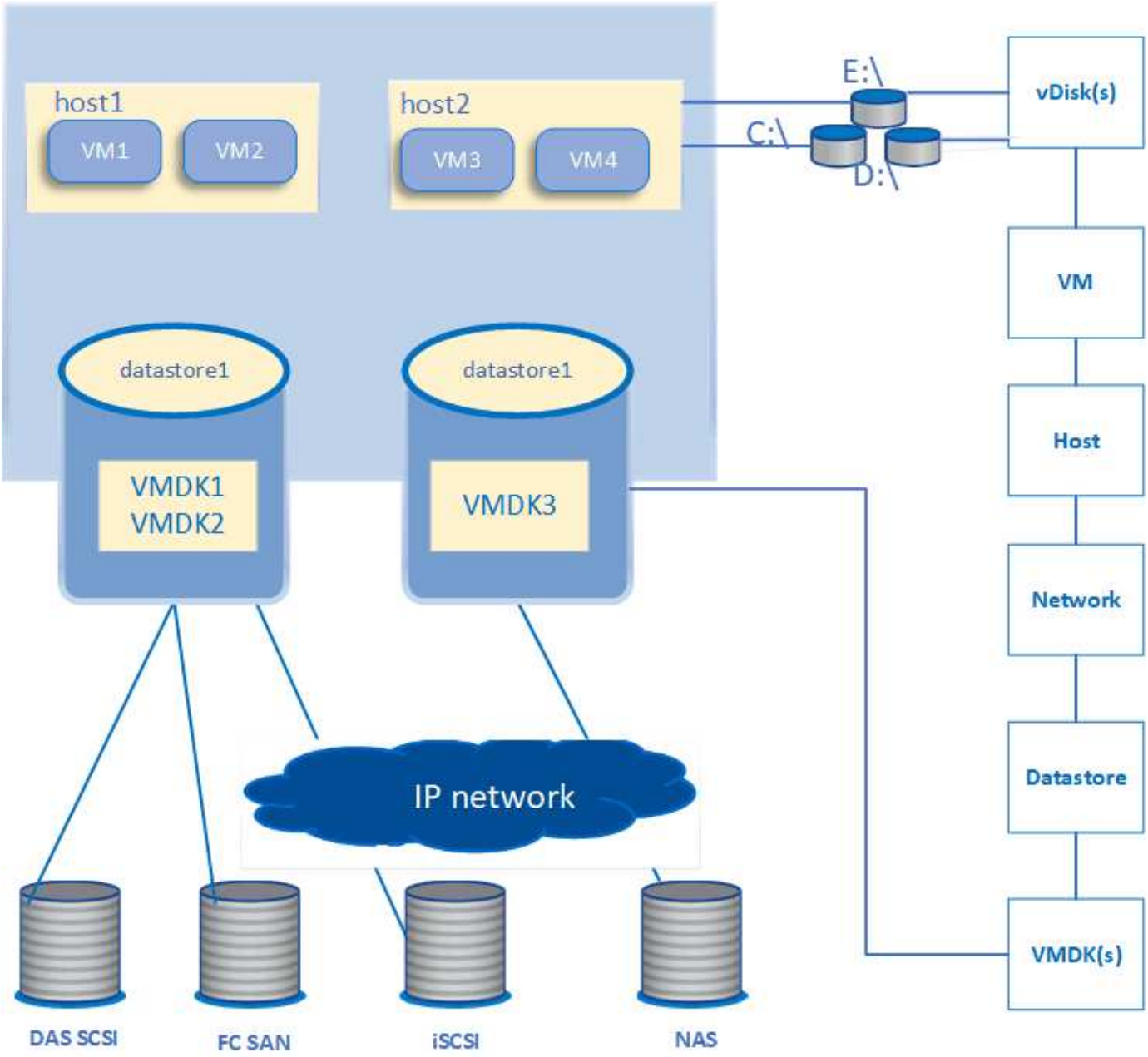
Unified Manager stellt das zugrunde liegende Subsystem einer virtuellen Umgebung in einer topologischen Ansicht dar, um festzustellen, ob ein Latenzproblem im Rechenknoten, im Netzwerk oder im Storage aufgetreten ist. Die Ansicht hebt zudem das spezifische Objekt hervor, das die Performance-Verzögerung verursacht, sodass Abhilfemaßnahmen ergriffen und das zugrunde liegende Problem behoben werden können.

Eine virtuelle Infrastruktur auf ONTAP Storage umfasst die folgenden Objekte:

- vCenter Server: Eine zentrale Kontrollebene für das Managen der VMware VMs, ESXi Hosts und aller zugehörigen Komponenten in einer virtuellen Umgebung. Weitere Informationen zu vCenter Server enthält die VMware-Dokumentation.
- Host: Ein physisches oder virtuelles System, auf dem ESXi, die Virtualisierungssoftware von VMware, ausgeführt wird und das die VM beherbergt.
- Datastore: Datastores sind virtuelle Storage Objekte, die mit den ESXi Hosts verbunden sind. Datastores sind verwaltbare Storage Einheiten von ONTAP, z. B. LUNs oder Volumes, die als Ablageort für VM-Dateien wie Protokolldateien, Skripte, Konfigurationsdateien und virtuelle Festplatten verwendet werden. Sie sind über eine SAN- oder IP-Netzwerkverbindung mit den Hosts in der Umgebung verbunden. Datastores außerhalb von ONTAP, die vCenter Server zugeordnet sind, werden in Unified Manager nicht unterstützt und nicht angezeigt.
- VM: Eine virtuelle Maschine von VMware.
- Virtuelle Festplatten: Die virtuellen Festplatten auf Datastores, die zu den VMs gehören und die Erweiterung VMDK haben. Die Daten einer virtuellen Festplatte werden in der entsprechenden VMDK gespeichert.
- VMDK: Eine virtuelle Maschinenfestplatte auf dem Datastore, die Speicherplatz für virtuelle Festplatten bereitstellt. Jeder virtuellen Festplatte ist eine entsprechende VMDK zugeordnet.

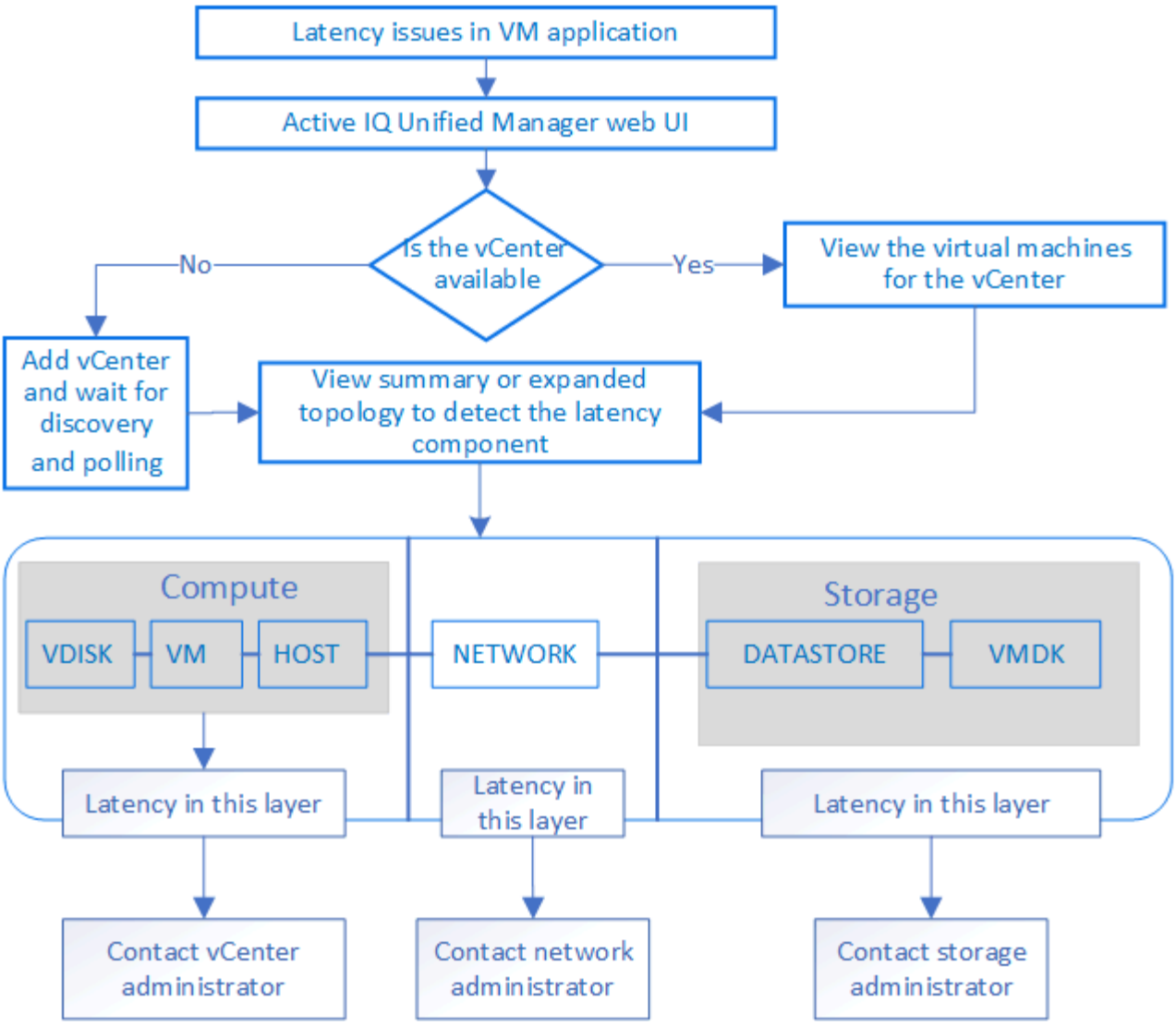
Eine VM-Topologieansicht zeigt diese Objekte.

VMware Virtualisierung auf ONTAP



Benutzer-Workflow

Das folgende Diagramm zeigt einen typischen Anwendungsfall der VM-Topologieansicht:



Was nicht unterstützt wird

- Datenspeicher außerhalb von ONTAP, die den vCenter Server Instanzen zugeordnet sind, werden von Unified Manager nicht unterstützt. VMs mit virtuellen Festplatten auf diesen Datenspeichern werden ebenfalls nicht unterstützt.
- Ein Datenspeicher über mehrere LUNs hinweg wird nicht unterstützt.
- Datastores, die Network address translation (NAT) für die Zuordnung von Daten-LIFs (Zugriffsendpunkt) verwenden, werden nicht unterstützt.
- Das Exportieren von Volumes oder LUNs als Datastores auf verschiedenen Clustern mit denselben IP-Adressen in einer Multi-LIF-Konfiguration wird nicht unterstützt, da Unified Manager nicht erkennen kann, welcher Datastore zu welchem Cluster gehört.

  Beispiel: Angenommen, Cluster A verfügt über Datastore A. Datastore A wird über eine Daten-LIF mit derselben IP-Adresse x.x.x.x exportiert, und VM A wird auf diesem Datastore erstellt. Analog dazu verfügt Cluster B über Datastore B. Datastore B wird über eine Daten-LIF mit derselben IP-Adresse x.x.x.x exportiert, und VM B wird auf Datastore B erstellt. UM kann weder den Datastore A für die Topologie von VM A dem entsprechenden ONTAP Volume/LUN zuordnen noch VM B erfassen.

- Als Datenspeicher werden ausschließlich NAS- und SAN-Volumes (iSCSI und FCP für VMFS) unterstützt, virtuelle Volumes (vVols) werden nicht unterstützt.

- Es werden ausschließlich virtuelle iSCSI-Datenträger unterstützt. Virtuelle Datenträger vom Typ NVMe und SATA werden nicht unterstützt.
- Die Ansichten erlauben es nicht, Berichte zur Analyse der Performance der verschiedenen Komponenten zu erstellen.
- Bei der für nur virtuelle Infrastruktur auf Unified Manager unterstützten Disaster-Recovery-Konfiguration (DR) für die Storage Virtual Machine (Storage VM) muss die Konfiguration in vCenter Server manuell geändert werden, damit sie in Switchover- und Switchback-Szenarien auf die aktiven LUNs verweist. Ohne einen manuellen Eingriff sind die Datastores nicht mehr zugänglich.

vCenter Server in Active IQ Unified Manager anzeigen und hinzufügen

Für die Anzeige und Fehlerbehebung der Performance der virtuellen Maschinen (VMs) ist es erforderlich, die zugehörigen vCenter Server zu Ihrer Active IQ Unified Manager Instanz hinzuzufügen.

Bevor Sie beginnen

Vor dem Hinzufügen oder Anzeigen von vCenter Servern sollten die folgenden Punkte erfüllt sein:

- Ihnen sind die Namen der vCenter Server bekannt.
- Sie kennen die IP-Adresse des vCenter Server und verfügen über die erforderlichen Zugangsdaten. Die Zugangsdaten müssen die eines vCenter Server-Administrators oder eines Root-Benutzers mit schreibgeschütztem Zugriff auf vCenter Server sein.
- Der vCenter Server, den Sie hinzufügen möchten, führt vSphere 6.5 oder höher aus.

  Der Support für Unified Manager für VMware ESXi und vCenter Server ist in englischer und japanischer Sprache verfügbar.

- Die Datenerfassungseinstellung auf dem vCenter Server ist auf das Statistik-Level von `Level 3` festgelegt, wodurch das erforderliche Level der Metrikenerfassung für alle überwachten Objekte sichergestellt wird. Die Intervalldauer sollte `5 minutes` betragen, und der Speicherzeitraum sollte `1 day` betragen.

  Weitere Informationen enthält der Abschnitt “Data Collection Levels” im *vSphere Monitoring and Performance Guide* in der VMware-Dokumentation.

- Die Latenzwerte in vCenter Server werden in Millisekunden und nicht in Mikrosekunden konfiguriert, um eine erfolgreiche Berechnung der Latenzwerte zu gewährleisten.
- Beim Hinzufügen des Datenspeichers zu vCenter Server können Sie sowohl die IP-Adresse des Hosts als auch den vollqualifizierten Domainnamen (FQDN) verwenden. Falls Sie einen FQDN hinzufügen, muss der Domänenname vom Unified Manager Server aufgelöst werden können. Bei einer Linux-Installation muss der Domänenname beispielsweise in der `/etc/resolv.conf` Datei eingetragen sein.
- Die aktuelle Uhrzeit des vCenter Server ist mit der Zeitzone des vCenter Server synchronisiert.
- vCenter Server ist für eine erfolgreiche Erkennung erreichbar.
- Sie haben Lesezugriff auf das VMware SDK, wenn Sie den vCenter Server zu Unified Manager hinzufügen. Dies ist für die Konfigurationsabfrage erforderlich.

Für jeden hinzugefügten und erkannten vCenter Server erfasst Unified Manager die Konfigurationsdaten, wie z. B. Details zu vCenter Server und ESXi Server, ONTAP Mapping, Datastore-Details und die Anzahl der gehosteten VMs. Darüber hinaus erfasst es die Performance-Metriken der Komponenten.

Schritte

1. Unter **VMWARE** > **vCenter** kann geprüft werden, ob Ihr vCenter Server in der Liste verfügbar ist.

   Falls Ihr vCenter Server nicht verfügbar ist, müssen Sie vCenter Server hinzufügen.

   a. Klicken Sie auf **Add**.

   b. Die korrekte IP-Adresse für vCenter Server muss hinzugefügt werden, und das Gerät muss erreichbar sein.

   c. Der Benutzername und das Passwort des Administrators oder Root-Benutzers mit Nur-Lesezugriff auf den vCenter Server müssen hinzugefügt werden.

   d. Die benutzerdefinierte Portnummer ist hinzuzufügen, wenn ein anderer Port als der Standardport 443 verwendet wird.

   e. Auf **Speichern** klicken.

      Nach erfolgreicher Erkennung wird ein Serverzertifikat angezeigt, das Sie akzeptieren können.

   Wenn Sie das Zertifikat akzeptieren, wird vCenter Server zur Liste der verfügbaren vCenter Servers hinzugefügt. Das Hinzufügen des Geräts führt nicht zur Datenerfassung für die zugehörigen VMs, und die Erfassung erfolgt in den geplanten Intervallen.

2. Wenn Ihr vCenter Server auf der **vCenters** Seite verfügbar ist, lässt sich sein Status prüfen, indem Sie mit der Maus auf das Feld **Status** zeigen, sodass angezeigt wird, ob Ihr vCenter Server wie erwartet funktioniert oder ob eine Warnung oder ein Fehler vorliegt.

   Durch das Hinzufügen von vCenter Server können Sie die folgenden Status anzeigen. Es kann jedoch bis zu einer Stunde dauern, bis die Performance- und Latenzdaten der entsprechenden VMs nach dem Hinzufügen von vCenter Server korrekt angezeigt werden.

   - Grün: „Normal“, was anzeigt, dass vCenter Server erkannt wurde und Performance-Metriken erfolgreich erfasst wurden
   - Gelb: „Warnung“ (z. B. wenn der Statistiken-Level für vCenter Server nicht auf 3 oder höher eingestellt ist, um Statistiken für jedes Objekt zu erhalten)
   - Orange: „Fehler“ (weist auf interne Fehler hin, z. B. Ausnahmen, Fehler bei der Erfassung von Konfigurationsdaten oder dass der vCenter Server nicht erreichbar ist). Über das Symbol für die Spaltenanzeige (**Ein-/Ausblenden**) lässt sich die Statusmeldung für den Status eines vCenter Server anzeigen und das Problem beheben.

3. Falls der vCenter Server nicht erreichbar ist oder sich die Zugangsdaten geändert haben, lassen sich die Details des vCenter Servers durch Auswahl von **vCenter** > **Edit** bearbeiten.
4. Die erforderlichen Änderungen sind auf der Seite **VMware vCenter Server bearbeiten** vorzunehmen.
5. Auf **Speichern** klicken.

vCenter Server-Datenerfassung beginnt

vCenter Server erfasst Echtzeit-Performance-Datenproben im 20-Sekunden-Takt und fasst sie zu 5-Minuten-Messwerten zusammen. Der Zeitplan für die Performance-Datenerfassung von Unified Manager basiert auf den Standardeinstellungen von vCenter Server. Unified Manager verarbeitet die von vCenter Server erfassten 5-Minuten-Messwerte und berechnet einen stündlichen Durchschnitt der IOPS und Latenz für virtuelle Festplatten, VMs und Hosts. Für Datastores berechnet Unified Manager einen stündlichen Durchschnitt der IOPS und Latenz aus den von ONTAP erfassten Messwerten. Diese Werte stehen jeweils zur vollen Stunde

zur Verfügung. Die Performance-Metriken sind nicht sofort nach dem Hinzufügen von vCenter Server verfügbar, sondern erst mit Beginn der nächsten Stunde. Die Abfrage der Performance-Daten beginnt nach Abschluss eines Zyklus der Konfigurationsdatenerfassung.

Zur Abfrage von Konfigurationsdaten von vCenter Server verwendet Unified Manager denselben Zeitplan wie für die Erfassung von Clusterkonfigurationsdaten. Informationen zum Zeitplan für die Erfassung von Konfigurations- und Performance-Daten von vCenter Server finden Sie unter „Aktivität zur Erfassung von Clusterkonfigurations- und Performance-Daten“.

Verwandte Informationen

"Aktivität zur Erfassung von Clusterkonfigurations- und Performance-Daten"

Entfernung eines vCenter Server aus Active IQ Unified Manager

Sie können vCenter Server aus Ihrer Active IQ Unified Manager Instanz entfernen. Sie können beispielsweise einen vCenter Server entfernen, wenn die Erkennung des vCenter Server fehlschlägt oder wenn er nicht mehr erforderlich ist.

Das Entfernen eines vCenter Server löscht auch alle virtuellen Maschinen (VMs), die auf diesem vCenter gehostet werden, sowie seine Konfigurationsdaten. Nach dem Entfernen des vCenter Server wird dieser zusammen mit den zugehörigen Objekten und Verlaufsdaten nicht mehr überwacht. Diese Änderungen werden auf den Inventarseiten für vCenter und virtuelle Maschinen angezeigt.

Bevor Sie beginnen

Vor dem Entfernen von vCenter Servern ist Folgendes sicherzustellen:

- Sie verfügen über die Rolle des Anwendungsadministrators oder des Storage-Administrators.
- Die Namen der vCenter Server und die jeweils zugehörigen IP-Adressen sollten Ihnen bekannt sein.

Schritte

1. Im linken Navigationsbereich befindet sich **VMWARE>vCenter**.
2. Auf der Seite vCenters können Sie den vCenter Server auswählen, den Sie entfernen möchten, und auf **Remove** klicken.
3. Im Meldungsdialogfeld **vCenter entfernen** wird die Entfernungsanforderung mit **OK** bestätigt.

Informationen dazu, wie Active IQ Unified Manager virtuelle Maschinen überwacht

Bei Latenzproblemen in virtuellen Maschinen (VMs) kann es erforderlich sein, die VMs zu überwachen, um die Ursache zu analysieren und zu beheben. Die VMs sind verfügbar, wenn ihr vCenter Server und die ONTAP Cluster, die den VM Storage hosten, Unified Manager hinzugefügt wurden.

Die Details der VMs finden Sie auf der Seite **VMWARE** > > **Virtuelle Maschinen**. Informationen wie Verfügbarkeit, Status, genutzte und zugewiesene Kapazität, Netzwerklatenz sowie die IOPS und die Latenz der VM, des Datastore und des Hosts werden angezeigt. Bei einer VM, die mehrere Datastores unterstützt, zeigt die Tabelle die Metriken des Datastore mit der höchsten Latenz an, wobei ein Sternchensymbol (*) auf zusätzliche Datastores hinweist. Wenn Sie auf das Symbol klicken, werden die Metriken des zusätzlichen Datastore angezeigt. Einige dieser Spalten stehen nicht zum Sortieren und Filtern zur Verfügung.

Damit eine VM und ihre Details angezeigt werden können, muss die Erkennung (Abfrage oder

Metrikenerfassung) des ONTAP Clusters abgeschlossen sein. Wenn der Cluster aus Unified Manager entfernt wird, ist die VM nach dem nächsten Erkennungszyklus nicht mehr verfügbar.

Auf dieser Seite lässt sich auch die detaillierte Topologie einer VM anzeigen, wobei die Komponenten dargestellt werden, mit denen die VM verknüpft ist, z. B. Host, virtuelle Festplatte und der damit verbundene Datastore. Die Topologieansicht zeigt die zugrunde liegenden Komponenten in ihren jeweiligen Ebenen in folgender Reihenfolge an: **Virtuelle Festplatte** > **VM** > **Host** > **Netzwerk** > **Datastore** > **VMDK**.

Sie können den E/A-Pfad und die Latenzen auf Komponentenebene aus topologischer Sicht bestimmen und feststellen, ob Storage die Ursache des Performanceproblems ist. Die Übersichtsansicht der Topologie zeigt den E/A-Pfad an und hebt die Komponente mit IOPS- und Latenzproblemen hervor, damit Sie über die Schritte zur Fehlerbehebung entscheiden können. Sie können auch eine erweiterte Ansicht der Topologie aufrufen, in der jede Komponente separat zusammen mit ihrer Latenz dargestellt wird. Sie können eine Komponente auswählen, um den durch die Ebenen hervorgehobenen E/A-Pfad zu bestimmen.

Übersichtstopologie anzeigen

Zur Ermittlung von Performance Problemen durch Anzeigen der VMs in einer zusammenfassenden Topologie:

1. Der Aufruf erfolgt über **VMWARE** > **Virtuelle Maschinen**.
2. Die Suche nach Ihrer VM erfolgt durch Eingabe ihres Namens in das Suchfeld. Eine Filterung der Suchergebnisse anhand bestimmter Kriterien ist auch über die Schaltfläche **Filter** möglich. Falls Ihre VM nicht gefunden wird, muss der zugehörige vCenter Server hinzugefügt und erkannt worden sein.

> vCenter Server erlauben Sonderzeichen (wie %, &, *, $, #, @, !, \, /, :, *, ?, "`, <, >, |, ;, ') in den Namen von vSphere Entitäten wie VMs, Clustern, Datastores, Ordnern oder Dateien. Der VMware vCenter Server und der ESX/ESXi Server maskieren Sonderzeichen in den Anzeigenamen nicht. Wenn der Name jedoch in Unified Manager verarbeitet wird, wird er anders angezeigt. Beispielsweise wird eine VM, die im vCenter Server als `%$VC_AIQUM_clone_191124%` benannt ist, in Unified Manager als `%25$VC_AIQUM_clone_191124%25` angezeigt. Dieses Problem muss berücksichtigt werden, wenn eine VM mit einem Namen abgefragt wird, der Sonderzeichen enthält.

3. Status der VM überprüfen. Die VM-Status werden von vCenter Server abgerufen. Die folgenden Status sind verfügbar. Weitere Informationen zu diesen Status sind in der VMware-Dokumentation enthalten.
   - Normal
   - Warnung
   - Alarm
   - Nicht überwacht
   - Unbekannt
4. Über den Pfeil nach unten neben der VM lässt sich die Übersichtsansicht der Topologie der Komponenten über die Compute-, Netzwerk- und Storage-Ebenen hinweg anzeigen. Der Knoten mit Latenzproblemen ist hervorgehoben. Die Übersichtsansicht zeigt die höchste Latenz der Komponenten an. Verfügt eine VM beispielsweise über mehr als eine virtuelle Festplatte, zeigt diese Ansicht die virtuelle Festplatte mit der höchsten Latenz unter allen virtuellen Festplatten an.
5. Die Analyse der Latenz und des Durchsatzes des Datastore über einen bestimmten Zeitraum erfolgt über die Schaltfläche **Workload Analyzer** oberhalb des Symbols des Datastore Objekts. Daraufhin wird die Seite Workload Analysis geöffnet, auf der sich ein Zeitraum auswählen und die Performance-Diagramme des Datastore anzeigen lassen. Weitere Informationen zum Workload Analyzer finden Sie unter *Troubleshooting workloads using the workload analyzer*.

Erweiterte Topologie anzeigen

In der erweiterten Topologie der VM lassen sich die einzelnen Komponenten separat aufschlüsseln.

Schritte

1. In der Übersichtsansicht kann auf **Expand Topology** geklickt werden. Anschließend ist die detaillierte Topologie jeder Komponente separat mit den Latenzwerten für jedes Objekt zu sehen. Wenn eine Kategorie mehrere Knoten enthält, zum Beispiel mehrere Knoten im datastore oder in der VMDK, wird der Knoten mit der höchsten Latenz rot hervorgehoben.
2. Der E/A-Pfad eines bestimmten Objekts lässt sich prüfen, indem Sie auf das Objekt klicken, sodass der E/A-Pfad und die entsprechende Zuordnung angezeigt werden. So lässt sich beispielsweise die Zuordnung einer virtuellen Festplatte anzeigen, indem Sie auf die virtuelle Festplatte klicken, sodass ihre hervorgehobene Zuordnung zur entsprechenden VMDK angezeigt wird. Bei einer Performance-Verzögerung dieser Komponenten können Sie weitere Daten aus ONTAP erfassen und das Problem beheben.

> Für VMDKs werden keine Metriken ausgegeben. In der Topologie werden nur die VMDK-Namen angezeigt, nicht jedoch Metriken.

Verwandte Informationen

"Fehlerbehebung bei Workloads mithilfe des workload Analyzer"

Sichtbarkeit der virtuellen Infrastruktur in einer Disaster Recovery Einrichtung mit Active IQ Unified Manager

Sie können die Konfigurations- und Performance-Metriken der Datastores anzeigen, die in einer MetroCluster Konfiguration oder in einem Disaster-Recovery-Setup für eine Storage Virtual Machine (storage VM) (SVM DR) gehostet werden.

In Unified Manager können Sie die NAS-Volumes oder LUNs in einer MetroCluster Konfiguration anzeigen, die in vCenter Server als Datastores angebunden sind. Die in einer MetroCluster Konfiguration gehosteten Datastores werden in derselben topologischen Ansicht dargestellt wie ein Datastore in einer Standardumgebung.

Sie können auch die NAS Volumes oder LUNs in einer Storage VM Disaster Recovery-Konfiguration anzeigen, die den Datastores in vCenter Server zugeordnet sind.

Datenspeicher in der MetroCluster Konfiguration anzeigen

Vor dem Anzeigen von Datenspeichern in einer MetroCluster Konfiguration sind die folgenden Voraussetzungen zu beachten:

- Im Falle eines Switchover und Switchback sollte die Erkennung der primären und sekundären Cluster des HA-Paares sowie der vCenter Server abgeschlossen sein.
- Die primären und sekundären Cluster des HA-Paars sowie die vCenter Server müssen durch Unified Manager verwaltet werden.
- Die erforderliche Einrichtung muss auf ONTAP und vCenter Server abgeschlossen sein. Die ONTAP und vCenter Dokumentation enthält Informationen dazu.

  "ONTAP 9 Dokumentationszentrum"

Die folgenden Schritte dienen zum Anzeigen von Datenspeichern:

1. Auf der Seite **VMWARE** > **Virtuelle Maschinen** erfolgt die Auswahl der VM, die den Datenspeicher hostet. Anschließend erfolgt ein Klick auf den **Workload Analyzer** oder den Link zum Datenspeicherobjekt. Im Standardszenario, wenn der primäre Standort, der das Volume oder die LUN hostet, wie erwartet funktioniert, sind die vServer Clusterdetails des primären Standorts zu sehen.
2. Im Katastrophenfall und bei einem anschließenden Switchover zum sekundären Standort verweist die Datastore-Verknüpfung auf die Performance-Kennzahlen des Volumes oder der LUN im sekundären Cluster. Dies wird nach Abschluss des nächsten Zyklus der Cluster- und vServer-Erkennung (Erfassung) berücksichtigt.
3. Nach einem erfolgreichen Switchback spiegelt die Datastore-Verknüpfung wieder die Performance-Kennzahlen des Volumes oder der LUN im primären Cluster wider. Dies ist nach Abschluss des nächsten Zyklus der Cluster- und vServer-Erkennung sichtbar.

Anzeige von Datenspeichern in der Disaster-Recovery-Konfiguration von Storage-VMs

Vor dem Anzeigen von Datenspeichern in einer Storage VM Disaster Recovery Konfiguration sind die folgenden Voraussetzungen zu beachten:

- Im Falle eines Switchover und Switchback sollte die Erkennung der primären und sekundären Cluster des HA-Paares sowie der vCenter Server abgeschlossen sein.
- Sowohl der Quell- als auch der Ziel-Cluster sowie die Storage VM-Peers sollten von Unified Manager gemanagt werden.
- Die erforderliche Konfiguration muss auf ONTAP und dem vCenter Server abgeschlossen sein.
    - Bei NAS-Datastores (NFS und VMFS) umfassen die Schritte im Katastrophenfall das Hochfahren der sekundären Storage VM, die Überprüfung der Daten-LIFs und -Routen, die Wiederherstellung verlorener Verbindungen auf dem vCenter Server und das Starten der VMs.

      Für einen Switchback auf den primären Standort sollten die Daten zwischen den Volumes synchronisiert sein, bevor der primäre Standort die Daten bereitstellt.

    - Bei SAN-Datastores (iSCSI und FC für VMFS) formatiert der vCenter Server die gemountete LUN im VMFS-Format. Im Fall eines Notfalls umfassen die Schritte das Starten der sekundären Storage VM sowie die Überprüfung der Daten-LIFs und Routen. Wenn sich die IPs des iSCSI-Ziels von den primären LIFs unterscheiden, müssen sie manuell hinzugefügt werden. Die neuen LUNs sollten als Geräte unter dem iSCSI-Adapter des Storage-Adapters des Hosts verfügbar sein. Danach sollten neue VMFS-Datastores mit den neuen LUNs erstellt und die alten VMs mit neuen Namen registriert werden. Die VMs müssen betriebsbereit sein.

      Im Fall einer Wiederherstellung sollten die Daten zwischen den Volumes synchronisiert werden. Neue VMFS Datastores sollten dann erneut mit den LUNs erstellt und die alten VMs unter neuen Namen registriert werden.

      Informationen zur Einrichtung finden Sie in der Dokumentation zu ONTAP und vCenter Server.
  "ONTAP 9 Dokumentationszentrum"

Die folgenden Schritte dienen zum Anzeigen von Datenspeichern:

1. Auf der Seite **VMWARE** > **Virtuelle Maschinen** lässt sich die VM-Inventarliste auswählen, die den Datenspeicher hostet. Anschließend lässt sich der Link zum Datenspeicherobjekt auswählen. Im Standardszenario sind die Performancedaten der Volumes und LUNs in der primären Storage VM zu sehen.

2. Im Katastrophenfall verweist die Datastore-Verknüpfung nach einem anschließenden Switchover zur sekundären Storage VM auf die Performance-Metriken des Volumes oder der LUN in der sekundären Storage VM. Dies wird berücksichtigt, nachdem der nächste Zyklus der Cluster- und vServer-Erkennung (Erfassung) abgeschlossen ist.
3. Nach einem erfolgreichen Switchback spiegelt der Datastore-Link erneut die Performance-Metriken des Volumes oder der LUN in der primären Storage VM wider. Dies zeigt sich, nachdem der nächste Zyklus der Cluster- und vServer-Erkennung abgeschlossen ist.

Nicht unterstützte Szenarien

- Für eine MetroCluster Konfiguration gelten die folgenden Einschränkungen:
  - Cluster werden nur in den Zuständen `NORMAL` und `SWITCHOVER` berücksichtigt. Andere Zustände wie `PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK` und `NOT_REACHABLE` werden nicht unterstützt.
  - Sofern Automatic Switch Over (ASO) nicht aktiviert ist, kann bei einem Ausfall des primären Clusters der sekundäre Cluster nicht erkannt werden, und die Topologie verweist weiterhin auf das Volume oder die LUN im primären Cluster.
- Bei einer Konfiguration zur Notfallwiederherstellung von Storage VMs gilt die folgende Einschränkung:
  - Eine Konfiguration, bei der Site Recovery Manager (SRM) oder Storage Replication Adapter (SRA) für eine SAN Storage Umgebung aktiviert ist, wird nicht unterstützt.

Provisionierung und managen von Workloads

Bereitstellen und Verwalten von Workloads in Active IQ Unified Manager

Die aktive Managementfunktion von Active IQ Unified Manager bietet Performance Service Levels, Storage Efficiency Policies und Storage Provider APIs für die Provisionierung, Überwachung und das Managen von Storage Workloads in einem Datacenter.

Unified Manager bietet diese Funktionalität standardmäßig. Sie können sie unter **Speicherverwaltung** > **Funktionseinstellungen** deaktivieren, wenn Sie diese Funktionalität nicht nutzen möchten.

Wenn diese Funktion aktiviert ist, können Sie Workloads auf den ONTAP Clustern provisionieren, die von Ihrer Unified Manager Instanz verwaltet werden. Sie können den Workloads außerdem Richtlinien wie Performance Service Levels und Storage Efficiency Policies zuweisen und Ihre Storage Umgebung auf Grundlage dieser Richtlinien managen.

Dieses Feature ermöglicht die folgenden Funktionen:

- Die automatische Erkennung von Storage Workloads auf den hinzugefügten Clustern ermöglicht eine einfache Bewertung und ein einfaches Deployment von Storage Workloads
- Provisionierung von NAS-Workloads mit Unterstützung der Protokolle NFS und CIFS
- Provisionierung von SAN-Workloads mit Unterstützung für iSCSI- und FCP-Protokolle
- Unterstützung für die Protokolle NFS und CIFS auf derselben Dateifreigabe
- Management von Performance Service Levels und Speichereffizienzrichtlinien
- Zuweisung von Performance Service Levels und Storage-Effizienzrichtlinien zu Storage Workloads

Mit den Optionen **Provisioning**, **Storage** > **Workloads** und **Policies** im linken Bereich der UI lassen sich verschiedene Konfigurationen ändern.

Mit diesen Optionen können Sie folgende Funktionen ausführen:

- Storage Workloads auf der Seite **Storage** > **Workloads** anzeigen
- Erstellung von Storage Workloads auf der Seite „Provision Workload“
- Erstellen und Managen von Performance Service Levels aus Richtlinien
- Storage Efficiency Policies in Policies erstellen und managen
- Zuweisen von Richtlinien zu Storage Workloads auf der Seite „Workloads“

Verwandte Informationen

"Richtlinienbasierte Storage-Verwaltung"

Übersicht über Workloads

Informationen zum Workloads-Dashboard in Active IQ Unified Manager

Eine Arbeitslast repräsentiert die Ein-/Ausgabeoperationen (E/A) eines Storage Objekts, wie z. B. eines Volumes oder einer LUN. Die Art der Provisionierung des Storage basiert auf den erwarteten Anforderungen der Arbeitslast. Statistiken zur Arbeitslast werden von Active IQ Unified Manager erst erfasst, wenn Datenverkehr zum und vom Storage Objekt vorhanden ist. Beispielsweise sind die IOPS- und Latenzwerte der Arbeitslast verfügbar, nachdem Benutzer eine Datenbank oder E-Mail-Applikation verwenden.

Die Seite „Workloads“ zeigt eine Zusammenfassung der Storage Workloads der ONTAP Cluster an, die von Unified Manager gemanagt werden. Sie bietet kumulative Informationen auf einen Blick über die Storage Workloads, die dem Performance Service Level entsprechen, sowie über die nicht konformen Storage Workloads. Außerdem können Sie die Gesamtkapazität, die verfügbare und die genutzte Kapazität sowie die Performance (IOPS) der Cluster in Ihrem Datacenter beurteilen.

Es wird empfohlen, die Anzahl der Storage Workloads zu ermitteln, die nicht konform oder nicht verfügbar sind oder die von keinem Performance Service Level gemanagt werden, und die notwendigen Maßnahmen zu ergreifen, um deren Konformität, Kapazitätsauslastung und IOPS sicherzustellen.

Die Seite „Workloads“ enthält die folgenden zwei Abschnitte:

- Workload-Übersicht: Bietet einen Überblick über die Anzahl der Storage Workloads auf den von Unified Manager gemanagten ONTAP Clustern.
- Datacenter Übersicht: Bietet einen Überblick über die Kapazität und die IOPS der Storage Workloads im Datacenter. Die relevanten Daten werden auf Datacenter Level und für einzelne . angezeigt.

Abschnitt „Übersicht zu Workloads“

Der Abschnitt „Workload-Übersicht“ bietet auf einen Blick kumulative Informationen zu den Storage Workloads. Der Status der Storage Workloads wird auf der Grundlage zugewiesener und nicht zugewiesener Performance Service Levels angezeigt.

- **Zugewiesen**: Für Storage Workloads, denen Performance Service Levels zugewiesen wurden, werden die folgenden Status gemeldet:
  - **Konform**: Die Performance von Storage Workloads basiert auf den ihnen zugewiesenen Performance Service Levels. Wenn sich die Storage Workloads innerhalb der in den zugehörigen Performance Service Levels definierten Latenzschwelle befinden, werden sie als “konform” gekennzeichnet. Die konformen Workloads sind blau markiert.
  - **Nicht konform**: Während der Performance-Überwachung werden Storage Workloads als „`nicht konform`“ gekennzeichnet, wenn die Latenz der Storage Workloads die im zugehörigen Performance Service Level definierte Schwellenwertlatenz überschreitet. Die nicht konformen Workloads sind orange markiert.
  - **Nicht verfügbar**: Storage Workloads werden als „`unavailable`“ markiert, wenn sie offline sind oder der zugehörige Cluster nicht erreichbar ist. Nicht verfügbare Workloads werden rot markiert.
- **Nicht zugewiesen**: Storage Workloads, denen kein Performance Service Level zugewiesen ist, werden als “unassigned” gemeldet. Die Zahl wird durch das Informationssymbol angezeigt.

Die Gesamtanzahl der Arbeitslasten ergibt sich aus der Summe der zugewiesenen und nicht zugewiesenen Arbeitslasten.

Die in diesem Abschnitt angezeigte Gesamtzahl der Workloads lässt sich anklicken; die Workloads werden dann auf der Seite „Workloads“ angezeigt.

Der Unterabschnitt „Konformität nach Performance Service Levels“ zeigt die Gesamtzahl der verfügbaren Storage Workloads an:

- Entsprechend jedem Typ von Performance Service Level
- Bei denen eine Diskrepanz zwischen den zugewiesenen und den empfohlenen Performance Service Levels besteht

Abschnitt „Datacenter-Übersicht“

Der Abschnitt zur Datacenter-Übersicht stellt die verfügbare und genutzte Kapazität sowie die IOPS für alle Cluster im Datacenter grafisch dar. Mithilfe dieser Daten sollten Sie die Kapazität und die IOPS der Storage-Workloads managen. Der Abschnitt zeigt außerdem die folgenden Informationen zu den Storage-Workloads über alle Cluster hinweg an:

- Die gesamte, verfügbare und genutzte Kapazität aller Cluster in Ihrem Datacenter
- Die gesamten, verfügbaren und genutzten IOPS für alle Cluster in Ihrem Datacenter
- Die verfügbare und genutzte Kapazität auf Basis jedes Performance Service Level
- Die verfügbaren und genutzten IOPS auf Basis jedes Performance Service Level
- Der gesamte Speicherplatz und die IOPS, die von den Workloads ohne zugewiesenes Performance Service Level genutzt werden

Wie Kapazität und Performance des Datacenters auf Basis von Performance Service Levels berechnet werden

Die genutzte Kapazität und die IOPS werden anhand der gesamten genutzten Kapazität und der Performance aller Storage-Workloads in den Clustern ermittelt.

Die verfügbaren IOPS werden auf Basis der erwarteten Latenz und der empfohlenen Performance Service Levels auf den Nodes berechnet. Sie umfassen die verfügbaren IOPS für alle Performance Service Levels, deren erwartete Latenz kleiner oder gleich ihrer eigenen erwarteten Latenz ist.

Die verfügbare Kapazität wird auf Basis der erwarteten Latenz und der empfohlenen Performance Service Levels für Aggregate berechnet. Sie umfasst die verfügbare Kapazität für alle Performance Service Levels, deren erwartete Latenz kleiner oder gleich ihrer eigenen erwarteten Latenz ist.

Workloads in Active IQ Unified Manager anzeigen

Wenn Sie Cluster zu Unified Manager hinzufügen, werden die Storage Workloads auf jedem Cluster automatisch erkannt und auf der Seite „Workloads“ angezeigt.

Unified Manager beginnt erst dann mit der Analyse der Workloads zur Empfehlung (empfohlene PSLs), wenn die E/A-Operationen auf den Storage-Workloads beginnen.

FlexGroup Volumes und seine Bestandteile sind ausgeschlossen.

Übersicht über Workloads

Die Seite „Workloads Übersicht“ zeigt die Übersicht der Workloads im Datacenter sowie die Übersicht über Platz und Performance des Datacenters.

- Das Panel **Workloads Overview** zeigt die Gesamtzahl der Workloads sowie die Anzahl der Workloads mit oder ohne ihnen zugewiesene PSLs an. Die Aufschlüsselung der Workload-Anzahl für jede PSL wird ebenfalls angezeigt. Durch Klicken auf die Anzahl gelangen Sie zur Ansicht **All Workloads** mit den gefilterten Workloads. Außerdem lässt sich die Anzahl der Workloads anzeigen, die nicht der Systemempfehlung entsprechen, und ihnen lassen sich durch Klicken auf die Schaltfläche **Assign System-Recommended PSLs** die vom System empfohlenen PSLs zuweisen.
- Bereich **Data Center Overview**: Zeigt den verfügbaren und belegten Storage (TiB) sowie die Performance (IOPS) des Datacenter an. Außerdem wird eine Aufschlüsselung des verfügbaren und belegten Storage (TiB) sowie der Performance (IOPS) aller Workloads unter jeder PSL angezeigt.

Ansicht aller Workloads

Die Seite **Storage > Workloads > All Workloads** listet die Storage Workloads auf, die den von Unified Manager verwalteten ONTAP Clustern zugeordnet sind.

Für neu erkannte Storage Workloads, bei denen noch keine E/A-Operationen stattgefunden haben, lautet der Status “Waiting for I/O”. Sobald bei den Storage Workloads E/A-Operationen beginnen, startet Unified Manager die Analyse, und der Workload-Status ändert sich in “Learning…”. Nach Abschluss der Analyse, innerhalb von 24 Stunden nach Beginn der E/A-Operationen, werden für die Storage Workloads die empfohlenen PSLs angezeigt.

Über diese Seite können Sie außerdem Storage Efficiency Policies (SEPs) und Performance Service Levels (PSLs) Storage-Workloads zuweisen. Sie können mehrere Aufgaben ausführen:

- Storage Workloads hinzufügen oder provisionieren
- Liste der Workloads anzeigen und filtern
- Zuweisen von PSLs zu Storage Workloads
- Systemseitig empfohlene PSLs auswerten und Workloads zuordnen
- Zuweisung von SEPs zu Storage Workloads

Storage Workloads hinzufügen oder provisionieren

Sie können die Storage Workloads zu unterstützten LUNs (mit Unterstützung für iSCSI und FCP), NFS-

Dateifreigaben und SMB-Freigaben hinzufügen oder provisionieren.

Schritte

1. Die Auswahl erfolgt über **Storage > Workloads > All Workloads > Create**.
2. Erstellung von Arbeitslasten. Weitere Informationen finden Sie unter "Provisionierung und Verwaltung von Workloads".

Workloads anzeigen und filtern

Auf dem Bildschirm „All Workloads“ können Sie alle Workloads in Ihrem Datacenter anzeigen oder anhand ihrer PSLs oder Namen nach bestimmten Storage Workloads suchen. Über das Filtersymbol lassen sich spezifische Bedingungen für die Suche eingeben. Die Suche kann nach verschiedenen Filterbedingungen erfolgen, z. B. nach dem Hostcluster oder der Storage VM. Mit der Option „Capacity Total“ lässt sich nach der Gesamtkapazität der Workloads (in MB) filtern. In diesem Fall kann die Anzahl der zurückgegebenen Workloads jedoch variieren, da die Gesamtkapazität auf Byte Level verglichen wird.

Für jede Arbeitslast werden Informationen wie der Hostcluster und die Storage VM sowie die zugewiesenen PSL und SEP angezeigt.

Auf dieser Seite lassen sich außerdem die Performance-Details einer Arbeitslast anzeigen. Detaillierte Informationen zu den IOPS, der Kapazität und der Latenz der Arbeitslast lassen sich anzeigen, indem auf die Schaltfläche **Choose / Order Columns** geklickt und bestimmte Spalten zur Anzeige ausgewählt werden. Die Spalte „Performance View“ zeigt die durchschnittlichen und die Spitzen-IOPS für eine Arbeitslast an, und über das Symbol für den Workload Analyzer lässt sich die detaillierte IOPS-Analyse anzeigen.

Analyse von Performance- und Kapazitätskriterien für eine Workload

Über die Schaltfläche **Analyze Workload** im Popup **IOPS Analysis** gelangen Sie zur Seite „Workload Analysis“, auf der Sie einen Zeitraum auswählen und die Latenz-, Durchsatz- und Kapazitätstrends für den ausgewählten Workload anzeigen können. Weitere Informationen zum Workload Analyzer finden sich in "Fehlerbehebung bei Arbeitslasten mithilfe des Arbeitslastanalysators".

Zur Unterstützung bei der Fehlerbehebung lassen sich Performance-Informationen zu einer Arbeitslast anzeigen, wenn in der Spalte **Performance View** auf das Balkendiagrammsymbol geklickt wird. Auf der Seite zur Arbeitslastanalyse lassen sich Performance- und Kapazitätsdiagramme zur Analyse des Objekts über die Schaltfläche **Analyze Workload** anzeigen.

Weitere Informationen sind unter "Welche Daten zeigt der Workload Analyzer an" verfügbar.

Zuweisung von Richtlinien zu Workloads in Active IQ Unified Manager

Sie können Storage Efficiency Policies (SEPs) und Performance Service Levels (PSLs) Storage Workloads auf der Seite „All Workloads“ mithilfe der verschiedenen Navigationsoptionen zuweisen.

Einer einzelnen Arbeitslast Richtlinien zuweisen

Sie können einer einzelnen Arbeitslast entweder eine PSL oder eine SEP oder beides zuweisen. Dazu sind die folgenden Schritte erforderlich:

1. Auswahl der Arbeitslast.
2. Das Bearbeitungssymbol neben der Zeile und anschließend **Bearbeiten** auswählen.

Die Felder **Zugewiesenes Performance Service Level** und **Speichereffizienzrichtlinie** sind aktiviert.

3. Es ist der gewünschte PSL oder SEP oder beides auszuwählen.
4. Mit dem Häkchensymbol lassen sich die Änderungen übernehmen.

> Sie können auch eine Workload auswählen und auf **Weitere Aktionen** klicken, um die Richtlinien zuzuweisen.

Zuweisen von Richtlinien zu mehreren Storage Workloads

Sie können eine PSL oder eine SEP mehreren Storage Workloads gleichzeitig zuweisen. Dafür sind folgende Schritte erforderlich:

1. Die Kontrollkästchen für die Workloads, denen die Richtlinie zugewiesen werden soll, oder alle Workloads im Datacenter können ausgewählt werden.
2. **Weitere Aktionen** auswählen.
3. Zum Zuweisen einer PSL ist **Leistungs-Servicelevel zuweisen** auszuwählen. Zum Zuweisen einer SEP ist **Speichereffizienzrichtlinie zuweisen** auszuwählen. Ein Pop-up-Fenster wird angezeigt, in dem die Richtlinie ausgewählt werden kann.
4. Die passende Richtlinie auswählen und auf **Apply** klicken. Die Anzahl der Workloads, denen die Richtlinien zugewiesen sind, wird angezeigt. Die Workloads, denen die Richtlinien nicht zugewiesen sind, werden ebenfalls mit Angabe der Ursache aufgelistet.

> Das Anwenden von Richtlinien auf Workloads in großen Mengen kann je nach Anzahl der ausgewählten Workloads einige Zeit in Anspruch nehmen. Sie können auf die Schaltfläche **Run in background** klicken und mit anderen Aufgaben fortfahren, während der Vorgang im Hintergrund ausgeführt wird. Nach Abschluss der Massenzuweisung können Sie den Abschlussstatus anzeigen. Wenn Sie eine PSL auf mehrere Workloads anwenden, können Sie keine weitere Anfrage auslösen, solange der vorherige Auftrag der Massenzuweisung ausgeführt wird.

Zuweisung der vom System empfohlenen PSLs zu Workloads

Sie können diesen Storage Workloads in einem Datacenter, denen keine PSLs zugewiesen sind oder deren zugewiesene PSLs nicht der Systemempfehlung entsprechen, systemseitig empfohlene PSLs zuweisen. Zum Verwenden dieser Funktion steht die Schaltfläche **Assign System Recommended PSLs** zur Verfügung. Sie müssen keine spezifischen Workloads auswählen.

Die Empfehlung wird intern durch Systemanalysen ermittelt und für Workloads übersprungen, deren IOPS und andere Parameter nicht mit den Definitionen der verfügbaren PSLs übereinstimmen. Speicherworkloads mit `Waiting for I/O` und Lernstatus sind ebenfalls ausgeschlossen.

> Es gibt spezielle Schlüsselwörter, nach denen Unified Manager im Workload-Namen sucht, um die Systemanalysen zu überschreiben und eine andere PSL für den Workload zu empfehlen. Wenn der Workload die Buchstaben “ora” im Namen enthält, wird die **Extreme Performance**PSL empfohlen. Und wenn der Workload die Buchstaben “vm” im Namen enthält, wird die **Performance**PSL empfohlen.

Weitere Informationen enthält der Artikel in der Wissensdatenbank (KB) "„Assign System Recommended Performance Service Level“ in ActiveIQ Unified Manager ist nicht an eine stark schwankende Workload anpassbar."

Bereitstellung von Dateifreigabe-Volumes in Active IQ Unified Manager

Auf der Seite „Provision Workload“ können Sie auf einem vorhandenen Cluster und einer vorhandenen Storage Virtual Machine (storage VM) Dateifreigabe-Volumes erstellen, die die Protokolle CIFS/SMB und NFS unterstützen.

Bevor Sie beginnen

- Die Storage VM muss über ausreichend Speicherplatz für die Provisionierung des Dateifreigabe-Volumes verfügen.
- Auf Ihrer Storage VM sollte entweder der SMB Service oder der NFS Service oder beide aktiviert sein.
- Für die Auswahl und Zuweisung des Performance Service Level (PSL) und der Storage Efficiency Policy (SEP) für den Workload ist es erforderlich, dass die Richtlinien bereits erstellt wurden, bevor Sie mit der Erstellung des Workloads beginnen.

Schritte

1. Auf der Seite **Provision Workload** können Sie den Namen des Workloads hinzufügen, den Sie erstellen möchten, und anschließend den Cluster aus der verfügbaren Liste auswählen.
2. Basierend auf dem ausgewählten Cluster filtert das Feld **STORAGE VM** die für diesen Cluster verfügbaren Storage VMs. Die erforderliche Storage VM wird aus der Liste ausgewählt.

   Basierend auf den von der Storage VM unterstützten SMB- und NFS-Services ist die NAS-Option im Abschnitt „Hostinformationen“ aktiviert.

3. Im Abschnitt „Storage und Optimierung“ erfolgt die Zuweisung der Storage-Kapazität und des PSL sowie optional eines SEP zur Arbeitslast.

   Die Spezifikationen für den SEP werden der LUN zugewiesen, und die Definitionen für den PSL gelten beim Erstellen der Arbeitslast.

4. Zum Erzwingen der der Workload zugewiesenen PSL ist das Kästchen **Enforce performance limits** zu aktivieren.

   Die Zuweisung einer PSL zu einer Arbeitslast stellt sicher, dass das Aggregat, auf dem die Arbeitslast erstellt wird, die in der jeweiligen Richtlinie definierten Performance- und Kapazitätsziele unterstützen kann. Wenn einer Arbeitslast beispielsweise die PSL „Extreme Performance“ zugewiesen wird, sollte das Aggregat, auf dem die Arbeitslast provisioniert werden soll, die Performance- und Kapazitätsziele der Richtlinie „Extreme Performance“ unterstützen können, z. B. SSD Storage.

   Sofern Sie dieses Kästchen nicht aktivieren, wird die PSL nicht auf die Arbeitslast angewendet, und der Status der Arbeitslast im Dashboard als nicht zugewiesen angezeigt.

5. Es ist die Option **NAS** auszuwählen.

   Falls die Option **NAS** nicht aktiviert angezeigt wird, ist zu prüfen, ob die ausgewählte Storage-VM SMB oder NFS oder beides unterstützt.

   Wenn Ihre Storage VM sowohl für SMB- als auch für NFS-Services aktiviert ist, können Sie die Kästchen **Freigabe per NFS** und **Freigabe per SMB** auswählen und eine Dateifreigabe erstellen, die sowohl NFS- als auch SMB-Protokolle unterstützt. Wenn nur eine SMB- oder eine CIFS-Freigabe erstellt werden soll, ist nur das entsprechende Kästchen auszuwählen.

6. Für NFS-Dateifreigabe-Volumes ist die IP-Adresse des Hosts oder Netzwerks erforderlich, über die bzw. das auf das Dateifreigabe-Volume zugegriffen wird. Für mehrere Hosts sind kommagetrennte Werte möglich.

   Beim Hinzufügen der Host-IP-Adresse wird intern geprüft, ob die Host-Details mit der Storage VM übereinstimmen, und die Exportrichtlinie für diesen Host wird erstellt oder, falls bereits eine Richtlinie vorhanden ist, wiederverwendet. Wenn mehrere NFS-Freigaben für denselben Host erstellt werden, wird eine verfügbare Exportrichtlinie für denselben Host mit übereinstimmenden Regeln für alle Dateifreigaben wiederverwendet. Die Möglichkeit, Regeln einzelner Richtlinien festzulegen oder Richtlinien durch Angabe spezifischer Richtlinienschlüssel wiederzuverwenden, ist verfügbar, wenn Sie die NFS-Freigabe mithilfe von APIs provisionieren.

7. Für eine SMB-Freigabe wird festgelegt, welche Benutzer oder Benutzergruppen auf die SMB-Freigabe zugreifen können, und ihnen werden die erforderlichen Berechtigungen zugewiesen. Für jede Benutzergruppe wird bei der Erstellung der Dateifreigabe eine neue Zugriffssteuerungsliste (ACL) generiert.
8. Auf **Speichern** klicken.

   Die Workload wird der Liste der Storage-Workloads hinzugefügt.

Bereitstellung von LUNs in Active IQ Unified Manager

Auf der Seite „Provision Workload“ können Sie LUNs erstellen, die die Protokolle CIFS/SMB und NFS unterstützen, und zwar auf einem bestehenden Cluster und einer Storage Virtual Machine (storage VM).

Bevor Sie beginnen

- Die Storage VM muss über ausreichend Speicherplatz für die Provisionierung der LUN verfügen.
- Sowohl iSCSI als auch FCP müssen auf der Storage VM aktiviert sein, auf der Sie die LUN erstellen.
- Für die Auswahl und Zuweisung des Performance Service Level (PSL) und der Storage Efficiency Policy (SEP) für den Workload ist es erforderlich, dass die Richtlinien bereits erstellt wurden, bevor Sie mit der Erstellung des Workloads beginnen.

Schritte

1. Auf der Seite **Provision Workload** können Sie den Namen des Workloads hinzufügen, den Sie erstellen möchten, und anschließend den Cluster aus der verfügbaren Liste auswählen.

   Basierend auf dem von Ihnen ausgewählten Cluster filtert das Feld **STORAGE VM** die für diesen Cluster verfügbaren Storage VMs.

2. Die Storage-VM, die die iSCSI- und FCP-Services unterstützt, wird aus der Liste ausgewählt.

   Aufgrund Ihrer Auswahl ist die SAN-Option im Abschnitt „Hostinformationen“ aktiviert.

3. Im Abschnitt **Storage und Optimierung** lassen sich der Arbeitslast die Speicherkapazität und der PSL sowie optional der SEP zuweisen.

   Die Spezifikationen für den SEP werden der LUN zugewiesen, und die Definitionen für den PSL gelten beim Erstellen der Arbeitslast.

4. Für das Erzwingen der zugewiesenen PSL für den Workload muss das Kästchen **Enforce performance limits** aktiviert sein.

Die Zuweisung einer PSL zu einer Arbeitslast stellt sicher, dass das Aggregat, auf dem die Arbeitslast erstellt wird, die in der jeweiligen Richtlinie definierten Performance- und Kapazitätsziele unterstützen kann. Wenn einer Arbeitslast beispielsweise die PSL „Extreme Performance“ zugewiesen wird, sollte das Aggregat, auf dem die Arbeitslast provisioniert werden soll, die Performance- und Kapazitätsziele der Richtlinie „Extreme Performance“ unterstützen können, z. B. SSD-Storage.

Sofern dieses Kästchen nicht aktiviert ist, wird die PSL nicht auf die Workload angewendet, und der Status der Workload im Dashboard wird als `unassigned` angezeigt.

5. Die Option **SAN** wird ausgewählt. Wenn die Option **SAN** nicht aktiviert angezeigt wird, sollte geprüft werden, ob die ausgewählte Storage-VM iSCSI und FCP unterstützt.
6. Auswahl des Host-Betriebssystems.
7. Die Hostzuordnung zur Steuerung des Zugriffs der Initiatoren auf die LUN ist festzulegen. Vorhandene Initiatorgruppen (igroups) können zugewiesen oder neue igroups definiert und zugeordnet werden.

   Wenn Sie während der Provisionierung der LUN eine neue Initiatorgruppe erstellen, können Sie diese erst nach dem nächsten Erkennungszyklus (bis zu 15 Minuten) verwenden. Daher empfiehlt sich die Verwendung einer vorhandenen Initiatorgruppe aus der Liste der verfügbaren Initiatorgruppen.

   Wenn Sie eine neue Initiatorgruppe erstellen möchten, wählen Sie die Schaltfläche **Create a new initiator group** aus, und geben Sie die Informationen für die Initiatorgruppe ein.

8. Auf **Speichern** klicken.

   Die LUN wird der Liste der Storage-Workloads hinzugefügt.

Verwalten von Performance Service Levels

Verwaltung von Performance Service Levels in Active IQ Unified Manager

Ein Performance Service Level (PSL) ermöglicht Ihnen, die Performance- und Storage-Ziele für eine Arbeitslast zu definieren. Einer Arbeitslast kann bei der Erstellung oder nachträglich durch Bearbeiten ein PSL zugewiesen werden.

Die Verwaltung und Überwachung von Storage Ressourcen basieren auf Service Level Objectives (SLOs). SLOs werden durch Service Level Agreements definiert, die auf der erforderlichen Performance und Kapazität basieren. In Unified Manager beziehen sich SLOs auf die PSL Definitionen der Applikationen, die auf NetApp Storage ausgeführt werden. Storage Services werden anhand der Performance und Auslastung der zugrunde liegenden Ressourcen differenziert. Ein PSL ist eine Beschreibung der Ziele des Storage Service. Ein PSL ermöglicht dem Storage Provider, die Performance- und Kapazitätsziele für den Workload festzulegen. Nach der Zuweisung eines PSL zu einem Workload wird der entsprechende Workload auf ONTAP anhand seiner Performance- und Kapazitätsziele gemanagt. Jedes PSL wird durch Spitzen-, erwartete und absolute minimale IOPs sowie die erwartete Latenz kontrolliert.

Unified Manager verfügt über folgende Arten von PSLs:

- **Systemdefiniert**: Unified Manager bietet einige vordefinierte Richtlinien, die nicht geändert werden können. Diese vordefinierten PSLs sind:
  - Extreme Performance

- Performance
- Wert

  Die PSLs Extreme Performance, Performance und Value eignen sich für die meisten gängigen Storage-Workloads in einem Datacenter.

Unified Manager bietet außerdem drei Performance Service Levels (PSLs) für Datenbankanwendungen. Diese PSLs sind extrem leistungsstark, unterstützen kurzzeitige IOPS-Spitzen und eignen sich für Datenbankanwendungen mit höchstem Durchsatzbedarf.

- Extrem für Datenbankprotokolle
- Extrem für gemeinsam genutzte Datenbankdaten
- Extrem für Datenbankdaten

- **Benutzerdefiniert**: Falls die vordefinierten Performance Service Levels (PSLs) Ihre Anforderungen nicht erfüllen, können Sie neue PSLs erstellen, die Ihren Anforderungen entsprechen. Informationen finden Sie unter "Erstellen und Bearbeiten von Performance Service Levels".
- **Beyond Extreme**: Die Beyond Extreme PSLs sind die vom System empfohlenen PSLs, die für Workloads vorgeschlagen werden, die höhere IOPs als Extreme erfordern. Die Workloads werden intern anhand ihrer IOPS, Kapazität und Latenz analysiert, und auf dem Bildschirm **Storage > Workloads > All Workloads** wird für jeden dieser Workloads ein Beyond Extreme PSL empfohlen. Sie können die PSLs auf die Workloads anwenden, um eine optimale Performance sicherzustellen.

  Die IOPs-Parameter für die Workloads werden dynamisch in Abhängigkeit vom Workload-Verhalten generiert und im Format `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>` an den Namen des Beyond Extreme PSL angehängt. Wenn das System beispielsweise ermittelt, dass ein Workload Spitzen-IOPs und erwartete IOPs von `106345` bzw. `37929` aufweist, wird der für den Workload generierte Beyond Extreme PSL als `Beyond Extreme 106345 37929` benannt. Obwohl diese PSLs vom System empfohlen werden, werden sie beim Zuweisen zu Workloads als `User-defined` vom Typ gekennzeichnet.

Workloads durch Zuweisung von PSLs managen

Sie können PSLs auf der Seite **Richtlinien** > **Performance Service Levels** sowie mithilfe der Storage Provider APIs aufrufen. Das Managen von Storage Workloads durch Zuweisung von PSLs ist komfortabel, da die Storage Workloads nicht einzeln gemanagt werden müssen. Änderungen lassen sich ebenfalls durch Neuzuweisung eines anderen PSLs managen, anstatt die Workloads einzeln zu managen. Unified Manager unterstützt Sie bei der Zuweisung von PSLs zu Ihren Workloads auf Grundlage interner Bewertungen und Empfehlungen.

Informationen zur Zuordnung von systemseitig empfohlenen PSLs zu Workloads finden Sie unter "Zuweisung der vom System empfohlenen PSLs zu Workloads"

Auf der Seite „Performance Service Levels“ sind die verfügbaren PSL-Richtlinien aufgeführt; außerdem können sie hinzugefügt, bearbeitet und gelöscht werden.

> Eine systemdefinierte PSL oder eine PSL, die aktuell einer Arbeitslast zugewiesen ist, kann nicht geändert werden. Eine einer Arbeitslast zugewiesene PSL oder die einzige verfügbare PSL kann nicht gelöscht werden.

Diese Seite zeigt folgende Informationen an:

Feld	Beschreibung
Name	Name der PSL.
Typ	Ob die Richtlinie systemdefiniert oder benutzerdefiniert ist.
Erwartete IOPS/TB	Die Mindestanzahl an IOPS, die eine Applikation voraussichtlich auf einer LUN oder Dateifreigabe ausführt. Die erwarteten IOPS geben die mindestens erwartete Anzahl zugewiesener IOPS basierend auf der zugewiesenen Größe des Storage Objekts an.
Maximale IOPS/TB	Die maximale Anzahl an IOPS, die eine Applikation auf einer LUN oder Dateifreigabe ausführen kann. Peak IOPS gibt die maximal mögliche Anzahl an zugewiesenen IOPS an, basierend auf der dem Storage Objekt zugewiesenen Größe oder der vom Storage Objekt verwendeten Größe. Peak IOPS basieren auf einer Zuweisungsrichtlinie. Die Zuweisungsrichtlinie ist entweder allocated-space oder used-space. Wenn die Zuweisungsrichtlinie auf allocated-space festgelegt ist, werden die Peak IOPS auf Grundlage der Größe des Storage Objekts berechnet. Wenn die Zuweisungsrichtlinie auf used-space festgelegt ist, werden die Peak IOPS auf Grundlage der im Storage Objekt gespeicherten Datenmenge unter Berücksichtigung der Storage Effizienz berechnet. Standardmäßig ist die Zuweisungsrichtlinie auf used-space festgelegt.

Feld	Beschreibung
Absolutes Minimum an IOPS	Der absolute Mindestwert für IOPS wird als Überschreibungswert verwendet, wenn die erwarteten IOPS unter diesem Wert liegen. Die Standardwerte der systemdefinierten PSLs sind die folgenden: • Extreme Performance: Bei erwarteten IOPS >= 6144/TB beträgt das absolute Minimum an IOPS 1000 • Performance: Wenn die erwarteten IOPS >= 2048/TB und < 6144/TB sind, dann beträgt das absolute Minimum an IOPS = 500 • Wert: Wenn die erwarteten IOPS >= 128/TB und < 2048/TB sind, dann beträgt das absolute Minimum an IOPS 75 Die Standardwerte der systemdefinierten Datenbank-PSLs sind die folgenden: • Extremwert für Datenbankprotokolle: Wenn die erwartete IOPS-Zahl >= 22528 ist, beträgt die absolute Mindest-IOPS-Zahl 4000 • Extremwert für gemeinsam genutzte Datenbankdaten: Wenn die erwarteten IOPS >= 16384 sind, beträgt die absolute Mindestzahl an IOPS 2000 • Extreme für Datenbankdaten: Wenn die erwarteten IOPS >= 12288 sind, dann betragen die absoluten minimalen IOPS 2000 Der höhere Wert der absoluten Mindest-IOPS für benutzerdefinierte PSLs darf maximal 75000 betragen. Der niedrigere Wert wird wie folgt berechnet: 1000/erwartete Latenz
Erwartete Latenz	Erwartete Latenz für Storage IOPS in Millisekunden pro Operation (ms/op).
Kapazität	Gesamte verfügbare und genutzte Kapazität in den Clustern.
Arbeitslasten	Anzahl der Storage Workloads, denen die PSL zugewiesen wurde.

Informationen darüber, wie die Spitzen-IOPS und die erwarteten IOPS zum Erreichen einer konsistenten differenzierten Performance auf ONTAP Clustern beitragen, enthält der folgende KB-Artikel: "Was ist leistungsorientierte Budgetierung?"

Für Workloads, die den durch PSLs definierten Schwellenwert überschreiten, generierte Ereignisse

Wenn Arbeitslasten in der vorangegangenen Stunde 30 % der Zeit den erwarteten Latenzwert überschreiten,

generiert Unified Manager eines der folgenden Ereignisse, um Sie auf ein potenzielles Performanceproblem hinzuweisen:

- Der in der Performance Service Level Policy definierte Latenzschwellenwert des Workload-Volumes wurde überschritten
- Der Schwellenwert für die Workload-LUN-Latenz wurde gemäß der Performance Service Level Richtlinie überschritten.

Möglicherweise empfiehlt sich eine Analyse der Workload, um festzustellen, was die höheren Latenzwerte verursacht.

Weitere Informationen sind unter den folgenden Links verfügbar:

- "Volume-Ereignisse"
- "Was geschieht, wenn eine Performance-Schwellenwertrichtlinie verletzt wird"
- "Wie Unified Manager die Workload-Latenz zur Identifizierung von Performance-Problemen nutzt"
- "Was Performance-Ereignisse sind"

Systemdefinierte PSLs

Die folgende Tabelle enthält Informationen zu den systemdefinierten PSLs:

Performance-Service-Level	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/op)	Maximale IOPS	Erwartete IOPS	Absolutes Minimum an IOPS
Extreme Performance	Bietet extrem hohen Durchsatz bei sehr geringer Latenz Ideal für latenzkritische Applikationen	1	12288	6144	1000
Performance	Bietet hohen Durchsatz bei geringer Latenz Ideal für Datenbank- und virtualisierte Applikationen	2	4096	2048	500

Performance-Service-Level	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/op)	Maximale IOPS	Erwartete IOPS	Absolutes Minimum an IOPS
Wert	Bietet eine hohe Storage Kapazität und moderate Latenz Ideal für Applikationen mit einer hohen Kapazität wie E-Mail, Webinhalte, Dateifreigaben und Sicherungsziele	17	512	128	75
Extrem für Datenbankprotokolle	Bietet maximalen Durchsatz bei geringster Latenz. Ideal für Datenbankapplikationen zur Unterstützung von Datenbankprotokollen. Diese PSL bietet den höchsten Durchsatz, da Datenbankprotokolle extrem ungleichmäßig anfallen und Protokollierung ständig erforderlich ist.	1	45056	22528	4000

Performance-Service-Level	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/op)	Maximale IOPS	Erwartete IOPS	Absolutes Minimum an IOPS
Extrem für gemeinsam genutzte Datenbankdaten	Bietet einen sehr hohen Durchsatz bei geringster Latenz. Ideal für Daten aus Datenbankapplikationen, die in einem gemeinsamen Datenspeicher abgelegt, aber datenbankübergreifend gemeinsam genutzt werden.	1	32768	16384	2000
Extrem für Datenbankdaten	Bietet hohen Durchsatz bei geringster Latenz. Ideal für Daten aus Datenbank Applikationen, z. B. Informationen zu Datenbanktabellen und Metadaten.	1	24576	12288	2000

Erstellen und Bearbeiten von Performance Service Levels in Active IQ Unified Manager

Wenn die vom System definierten Performance Service Levels nicht mit Ihren Workload-Anforderungen übereinstimmen, können Sie Ihre eigenen Performance Service Levels erstellen, die für Ihre Workloads optimiert sind.

Bevor Sie beginnen

- Sie benötigen die Rolle des Anwendungsadministrators.
- Der Name des Performance Service Level muss eindeutig sein, und die folgenden reservierten Schlüsselwörter können nicht verwendet werden:

  `Prime`, `Extreme`, `Performance`, `Value`, `Unassigned`, `Learning`, `Idle`, `Default`, und `None`.

Auf der Seite „Performance Service Levels“ lassen sich benutzerdefinierte Performance Service Levels erstellen und bearbeiten, indem die Service Level-Ziele definiert werden, die für die Applikationen erforderlich sind, die auf Storage zugreifen.

Ein Performance Service Level kann nicht geändert werden, wenn es derzeit einer Arbeitslast zugewiesen ist.

Schritte

1. Im linken Navigationsbereich ist unter **Einstellungen Richtlinien** > **Performance Service Levels** zu wählen.
2. Auf der Seite **Performance Service Levels** wählen Sie die entsprechende Schaltfläche aus, je nachdem, ob Sie einen neuen Performance Service Level erstellen oder einen bestehenden Performance Service Level bearbeiten möchten.

Zu…	Folgen Sie diesen Schritten…
Erstellen eines neuen Performance Service Levels	Klicken Sie auf **Add**.
Bearbeiten eines vorhandenen Performance Service Levels	Die Auswahl eines vorhandenen Performance Service Level und der anschließende Klick auf **Bearbeiten** sind erforderlich.

   Die Seite zum Hinzufügen oder Bearbeiten eines Performance Service Level wird angezeigt.

3. Das Performance Service Level lässt sich durch Angabe der Performance-Ziele anpassen; anschließend kann durch Klicken auf **Submit** das Performance Service Level gespeichert werden.

Sie können das neue oder geänderte Performance Service Level auf Workloads (LUNs, NFS-Dateifreigaben, CIFS-Freigaben) auf der Seite „Workloads“ oder bei der Provisionierung eines neuen Workloads anwenden.

Verwaltung von Richtlinien zur Storage-Effizienz

Verwalten von Speichereffizienzrichtlinien in Active IQ Unified Manager

Eine Speichereffizienzrichtlinie (SEP) ermöglicht die Definition der Speichereffizienzmerkmale einer Arbeitslast. Einer Arbeitslast kann bei ihrer Erstellung oder nachträglich durch Bearbeiten eine SEP zugewiesen werden.

Speichereffizienz umfasst den Einsatz von Technologien wie Thin Provisionierung, Deduplizierung und Datenkomprimierung, die die Storage Auslastung erhöhen und die Storage Kosten senken. Beim Erstellen von SEPs können Sie diese platzsparenden Technologien einzeln oder zusammen verwenden, um eine maximale Speichereffizienz zu erzielen. Wenn Sie die Richtlinien Ihren Storage Workloads zuordnen, werden ihnen die angegebenen Richtlinieneinstellungen zugewiesen. Unified Manager ermöglicht Ihnen, systemdefinierte und benutzerdefinierte SEPs zuzuweisen, um die Storage Ressourcen in Ihrem Datacenter zu optimieren.

Unified Manager bietet zwei systemdefinierte SEPs: Hoch und Niedrig. Diese SEPs sind auf die meisten Storage-Workloads in einem Datacenter anwendbar. Sie können jedoch eigene Richtlinien erstellen, wenn die systemdefinierten SEPs Ihre Anforderungen nicht erfüllen.

Ein systemdefiniertes SEP oder ein SEP, das aktuell einer Arbeitslast zugewiesen ist, kann nicht geändert werden. Ein SEP, das einer Arbeitslast zugewiesen ist oder das einzige verfügbare SEP ist, kann nicht gelöscht werden.

Die Seite „Richtlinien zur Speichereffizienz“ listet die verfügbaren SEPs auf und ermöglicht das Hinzufügen, Bearbeiten und Löschen benutzerdefinierter SEPs. Auf dieser Seite werden folgende Informationen angezeigt:

Feld	Beschreibung
Name	Name der SEP.
Typ	Ob die Richtlinie systemdefiniert oder benutzerdefiniert ist.
Platzreserve	Ob das Volume Thin Provisioning oder Thick Provisioning verwendet.
Deduplizierung	Ob die Deduplizierung für die Workload aktiviert ist: • Inline: Die Deduplizierung erfolgt während des Schreibvorgangs auf die Workload • Hintergrund: Die Deduplizierung erfolgt in der Workload • Deaktiviert: Die Deduplizierung ist für die Arbeitslast deaktiviert
Komprimierung	Ob Datenkomprimierung für die Arbeitslast aktiviert ist: • Inline: Die Datenkomprimierung erfolgt beim Schreiben in die Workload • Hintergrund: Die Datenkomprimierung erfolgt in der Workload • Deaktiviert: Die Datenkomprimierung ist für den Workload deaktiviert
Arbeitslasten	Anzahl der Storage Workloads, denen die SEP zugewiesen wurde

Richtlinien zum Erstellen einer benutzerdefinierten Storage Effizienzrichtlinie

Falls die vorhandenen SEPs die Richtlinienanforderungen für Ihre Storage Workloads nicht erfüllen, können Sie einen benutzerdefinierten SEP erstellen. Es wird jedoch empfohlen, nach Möglichkeit die systemdefinierten SEPs für Ihre Storage Workloads zu verwenden und benutzerdefinierte SEPs nur bei Bedarf zu erstellen.

Die den Workloads zugewiesenen SEP können auf der Seite „All Workloads“ und auf der Seite „Volume / Health details“ angezeigt werden. Das Datenreduktionsverhältnis auf Clusterebene (ohne Snapshot Kopien) auf der Grundlage dieser Storage Effizienzen kann im Bereich „Capacity“ auf dem „Dashboard“ und in der Ansicht „Capacity: All Clusters“ angezeigt werden.

Erstellen und Bearbeiten von Speichereffizienzrichtlinien in Active IQ Unified Manager

Wenn die vom System definierten Speichereffizienzrichtlinien nicht mit Ihren Arbeitslastanforderungen übereinstimmen, können Sie eigene Speichereffizienzrichtlinien erstellen, die für Ihre Arbeitslasten optimiert sind.

Bevor Sie beginnen

- Sie benötigen die Rolle des Anwendungsadministrators.
- Der Name der Speichereffizienzrichtlinie muss eindeutig sein, und die folgenden reservierten Schlüsselwörter dürfen nicht verwendet werden:

`High`, `Low`, `Unassigned`, `Learning`, `Idle`, `Default`, und `None`.

Sie erstellen und bearbeiten benutzerdefinierte Speichereffizienzrichtlinien auf der Seite „Speichereffizienzrichtlinien“, indem Sie die Speichereffizienzmerkmale definieren, die Sie für die Applikationen benötigen, die auf Storage zugreifen.

Eine Speichereffizienzrichtlinie kann nicht geändert werden, wenn sie aktuell einer Arbeitslast zugewiesen ist.

Schritte

1. Im linken Navigationsbereich ist unter **Einstellungen Richtlinien** > **Speichereffizienz** auszuwählen.
2. Auf der Seite **Storage Efficiency Policies** wird je nach Bedarf die entsprechende Schaltfläche ausgewählt, um eine neue Storage Efficiency Policy zu erstellen oder eine vorhandene Storage Efficiency Policy zu bearbeiten.

Zu…	Folgen Sie diesen Schritten…
Erstellung einer neuen Speichereffizienzrichtlinie	Auf **Hinzufügen** klicken
Vorhandene Speichereffizienzrichtlinie bearbeiten	Sie können eine vorhandene Speichereffizienzrichtlinie auswählen und auf **Bearbeiten** klicken

   Daraufhin erscheint die Seite zum Hinzufügen oder Bearbeiten einer Speichereffizienzrichtlinie.

3. Zur Anpassung der Storage Efficiency Policy die Merkmale der Storage-Effizienz angeben und anschließend zum Speichern der Storage Efficiency Policy auf **Submit** klicken.

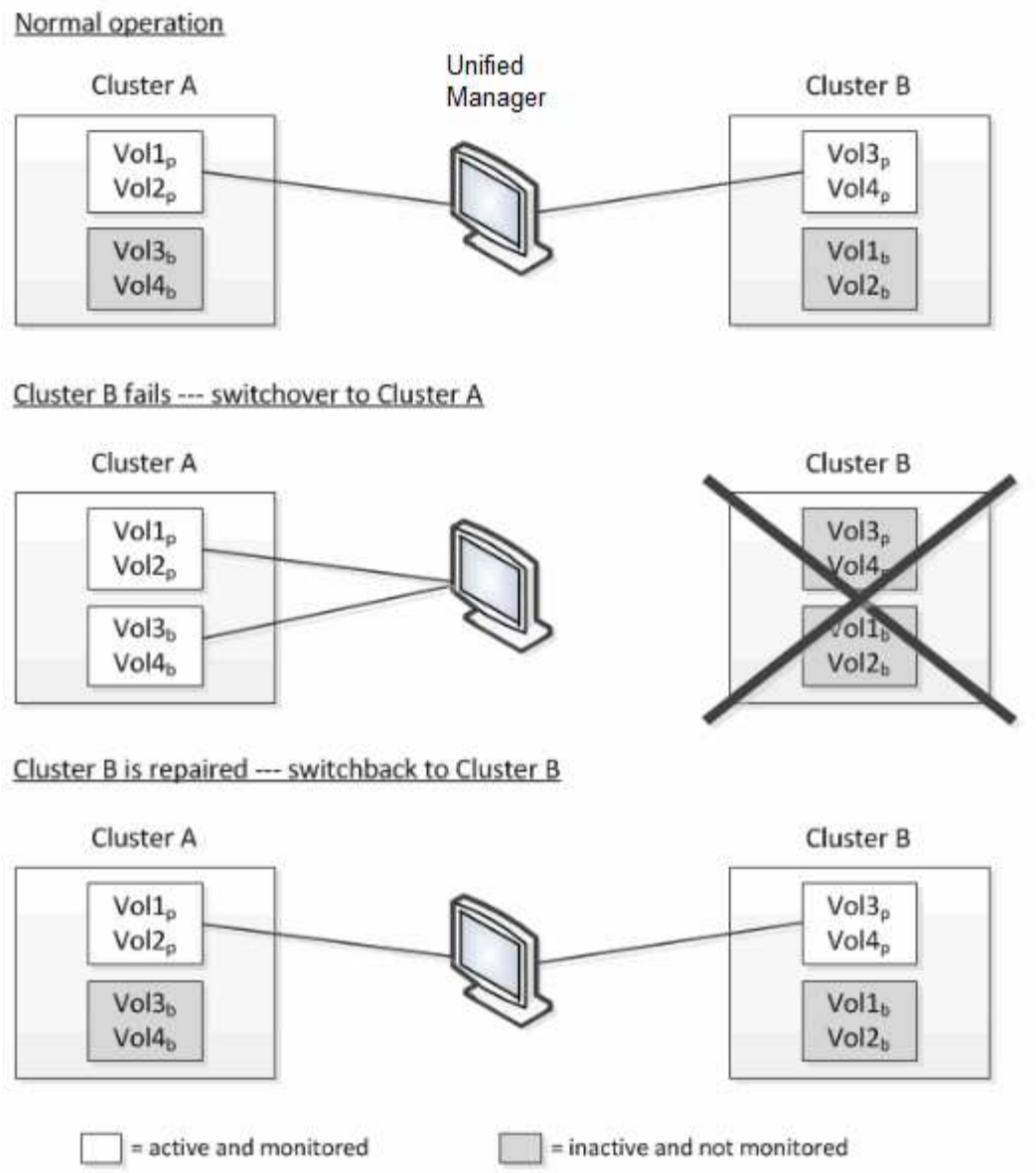
Sie können die neue oder geänderte Speichereffizienzrichtlinie auf Workloads (LUNs, NFS-Dateifreigaben, CIFS-Freigaben) auf der Seite „Workloads“ oder bei der Provisionierung eines neuen Workloads anwenden.

Management und Überwachung von MetroCluster Konfigurationen

Informationen zum Volume Verhalten bei Umschaltung und Rückschaltung in Active IQ Unified Manager

Ereignisse, die einen Switchover oder Switchback auslösen, bewirken, dass aktive Volumes in der Disaster-Recovery-Gruppe von einem Cluster auf den anderen Cluster verschoben werden. Die Volumes auf dem Cluster, die aktiv waren und Daten an Clients bereitstellten, werden gestoppt, und die Volumes auf dem anderen Cluster werden aktiviert und beginnen mit der Datenbereitstellung. Unified Manager überwacht nur die Volumes, die aktiv sind und ausgeführt werden.

Da Volumes von einem Cluster in einen anderen verschoben werden, wird empfohlen, beide Cluster zu überwachen. Eine einzelne Instanz von Unified Manager kann in einer MetroCluster Konfiguration beide Cluster überwachen. Aufgrund der Entfernung zwischen den beiden Standorten ist es jedoch manchmal erforderlich, zwei Unified Manager Instanzen zur Überwachung beider Cluster einzusetzen. Die folgende Abbildung zeigt eine einzelne Instanz von Unified Manager:



Die Volumes mit einem „p“ im Namen kennzeichnen die primären Volumes, und die Volumes mit einem „b“ im Namen sind gespiegelte Backup-Volumes, die von SnapMirror erstellt werden.

Im Normalbetrieb:

- Cluster A verfügt über zwei aktive Volumes: Vol1p und Vol2p.
- Cluster B verfügt über zwei aktive Volumes: Vol3p und Vol4p.
- Cluster A hat zwei inaktive Volumes: Vol3b und Vol4b.
- Cluster B verfügt über zwei inaktive Volumes: Vol1b und Vol2b.

Informationen zu jedem der aktiven Volumes (Statistiken, Ereignisse usw.) werden von Unified Manager erfasst. Die Statistiken für Vol1p und Vol2p werden von Cluster A erfasst, und die Statistiken für Vol3p und Vol4p werden von Cluster B erfasst.

Nachdem ein katastrophaler Ausfall eine Umschaltung aktiver Volumes von Cluster B auf Cluster A verursacht hat:

- Cluster A verfügt über vier aktive Volumes: Vol1p, Vol2p, Vol3b und Vol4b.

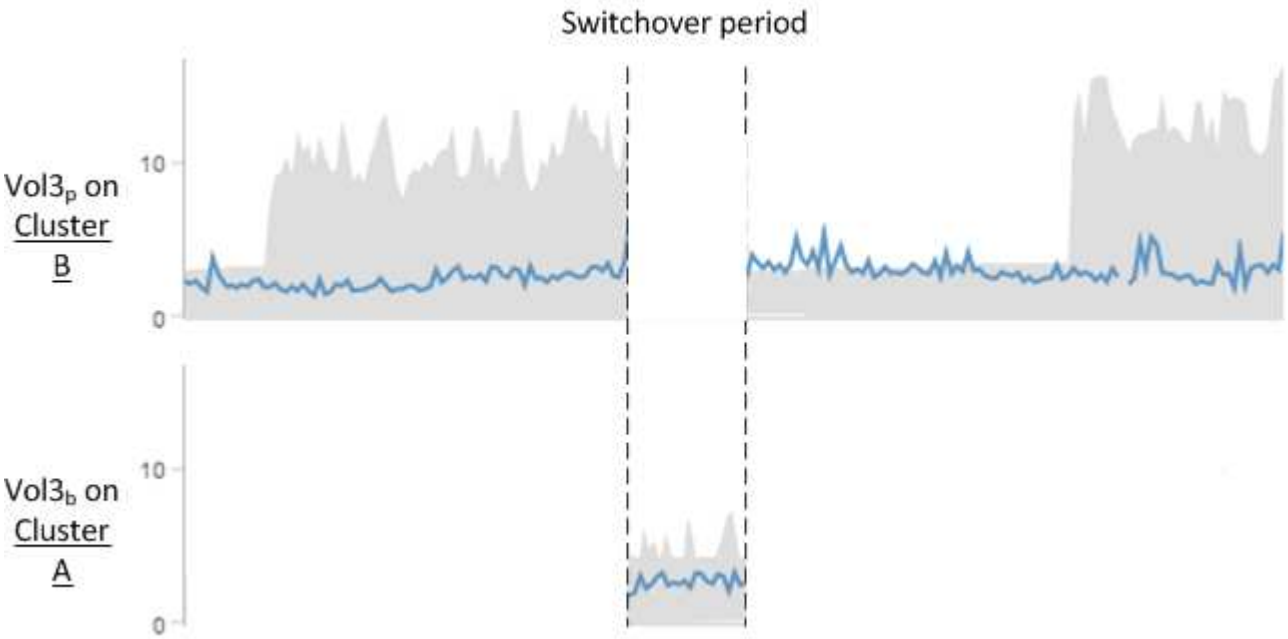
- Cluster B verfügt über vier inaktive Volumes: Vol3p, Vol4p, Vol1b und Vol2b.

Wie im Normalbetrieb werden Informationen zu jedem aktiven Volume von Unified Manager erfasst. In diesem Fall werden die Statistiken für Vol1p und Vol2p jedoch von Cluster A erfasst, ebenso wie die Statistiken für Vol3b und Vol4b.

Vol3p und Vol3b sind nicht dieselben Volumes, da sie sich auf unterschiedlichen Clustern befinden. Die Informationen in Unified Manager für Vol3p sind nicht dieselben wie für Vol3b:

- Während des Wechsels zu Cluster A sind Vol3p Statistiken und Ereignisse nicht sichtbar.
- Beim ersten Switchover erscheint Vol3b wie ein neues Volume ohne jegliche historischen Informationen.

Nach der Reparatur von Cluster B und der Durchführung eines Switchbacks ist Vol3p auf Cluster B wieder aktiv, mit den historischen Statistiken und einer Lücke in den Statistiken für den Zeitraum während des Switchovers. Vol3b ist von Cluster A aus erst nach einem weiteren Switchover sichtbar:



- MetroCluster Volumes, die inaktiv sind, beispielsweise Vol3b auf Cluster A nach Switchback, werden mit der Meldung “This volume was deleted” gekennzeichnet. Das Volume ist nicht tatsächlich gelöscht, wird aber derzeit nicht von Unified Manager überwacht, da es nicht das aktive Volume ist.
- Wenn ein einzelner Unified Manager beide Cluster in einer MetroCluster Konfiguration überwacht, liefert die Volume-Suche Informationen für das jeweils aktive Volume. Beispielsweise würde eine Suche nach „Vol3“ Statistiken und Ereignisse für Vol3b auf Cluster A liefern, falls ein Switchover stattgefunden hat und Vol3 auf Cluster A aktiv geworden ist.

Grundlegendes zur Cluster-Konnektivität in einer MetroCluster FC Konfiguration in Active IQ Unified Manager

Die Konnektivität zwischen den Clustern in einer MetroCluster over FC-Konfiguration kann einen der folgenden Status aufweisen: Optimal, Eingeschränkt oder Nicht verfügbar. Das Verständnis der Konnektivitätsstatus ermöglicht Ihnen, Ihre MetroCluster

Konfigurationen effektiv zu managen.

Verbindungsstatus	Beschreibung	Symbol angezeigt
Optimal	Die Verbindungen zwischen den Clustern in der MetroCluster Konfiguration sind normal.	
Betroffen	Ein oder mehrere Fehler beeinträchtigen den Status der Failover-Verfügbarkeit; beide Cluster in der MetroCluster Konfiguration sind jedoch weiterhin aktiv. Dies ist beispielsweise der Fall, wenn die ISL-Verbindung unterbrochen ist, wenn die Intercluster-IP-Verbindung unterbrochen ist oder wenn der Partnercluster nicht erreichbar ist.	
Ausgefallen	Die Verbindung zwischen den Clustern in der MetroCluster Konfiguration ist unterbrochen, da einer oder beide Cluster ausgefallen sind oder sich im Failover-Modus befinden. Dies kann beispielsweise der Fall sein, wenn der Partner-Cluster aufgrund einer Katastrophe ausgefallen ist oder zu Testzwecken ein geplanter Switchover erfolgt.	Umschaltung mit Fehlern:  Umschaltung erfolgreich: 

Informationen zu MetroCluster über FC-Datenspiegelung in Active IQ Unified Manager

MetroCluster over FC Konfigurationen bieten Datenspiegelung und zusätzlich die Möglichkeit, ein Failover einzuleiten, wenn ein gesamter Standort nicht verfügbar wird. Der Status der Datenspiegelung zwischen den Clustern in einer MetroCluster over FC Konfiguration kann entweder „Normal“ oder „Spiegelung nicht verfügbar“ sein. Das Verständnis des Status ermöglicht Ihnen, Ihre MetroCluster Konfigurationen effektiv zu managen.

Status der Datenspiegelung	Beschreibung	Symbol angezeigt
Normal	Die Datenspiegelung zwischen den Clustern in der MetroCluster Konfiguration ist normal.	

Status der Datenspiegelung	Beschreibung	Symbol angezeigt
Spiegelung nicht verfügbar	Die Datenspiegelung zwischen den Clustern in der MetroCluster Konfiguration ist aufgrund eines Switchovers nicht verfügbar. Dies kann beispielsweise der Fall sein, wenn der Partnercluster aufgrund eines Notfalls ausgefallen ist oder ein geplanter Switchover zu Testzwecken erfolgt.	Umschaltung mit Fehlern:  Umschaltung erfolgreich: 

Überwachung von MetroCluster Konfigurationen in Active IQ Unified Manager

Sie können Verbindungsprobleme in Ihrer MetroCluster Konfiguration überwachen. Die Details umfassen den Status der Komponenten und der Verbindungen innerhalb eines Clusters sowie den Verbindungsstatus zwischen den Clustern in der MetroCluster Konfiguration. Dieser Abschnitt beschreibt, wie Verbindungsprobleme in Clustern überwacht werden, die durch MetroCluster FC- und MetroCluster IP-Konfigurationen geschützt sind.

Sie können die MetroCluster Konfigurationen in den folgenden Ansichten im linken Navigationsbereich von Active IQ Unified Manager überwachen:

- **Storage** > **Cluster** > **Schutz: MetroCluster** Ansicht
- **Schutz** > **Beziehungen** > **Beziehung: MetroCluster** Ansicht

Unified Manager verwendet Systemstatuswarnungen, um den Status der Komponenten und der Konnektivität in der MetroCluster Konfiguration anzuzeigen.

Bevor Sie beginnen

- Sowohl die lokalen als auch die Remote-Cluster in einer MetroCluster Konfiguration müssen zu Active IQ Unified Manager hinzugefügt werden.
- In einer MetroCluster over IP Konfiguration sollte, wenn ein Mediator unterstützt werden soll, der Mediator über die entsprechende API konfiguriert und dem Cluster hinzugefügt werden.
- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Überwachung von Verbindungsproblemen in der MetroCluster over FC Konfiguration

Bei Clustern in einer MetroCluster over FC Konfiguration werden die Konnektivitätsdiagramme auf der Detailseite **Cluster / Health** angezeigt. Dabei gelten die folgenden Schritte.

Schritte

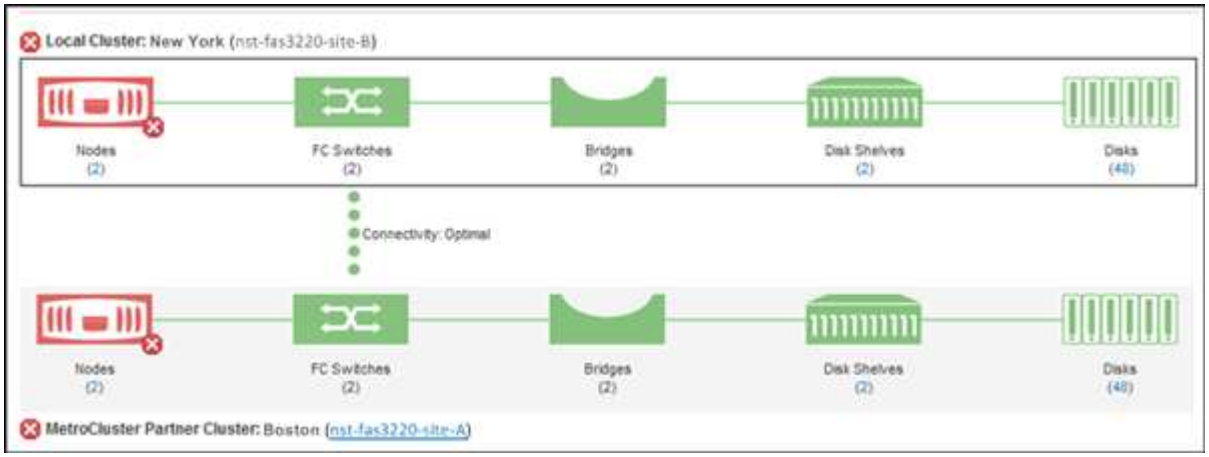
1. Im linken Navigationsbereich wird **Storage** > **Cluster** ausgewählt.

   Eine Liste aller überwachten Cluster wird angezeigt.

2. In der Ansicht **Schutz: MetroCluster** lässt sich der Name des Clusters auswählen, für den die Details zur

MetroCluster over FC Konfiguration angezeigt werden sollen. Alternativ können Sie nach Clustern in einer MetroCluster Konfiguration filtern.

3. Auf der Detailseite **Cluster / Systemstatus** erfolgt die Auswahl der Registerkarte **MetroCluster Connectivity**. Die Registerkarte **MetroCluster Connectivity** ist nur für MetroCluster over FC Konfigurationen verfügbar.



Die Topologie der MetroCluster Konfiguration wird im entsprechenden Clusterobjektbereich angezeigt. Mithilfe der Informationen auf der Seite „Cluster-/Systemstatusdetails“ lassen sich etwaige Verbindungsprobleme beheben. Wenn beispielsweise die Verbindung zwischen dem Knoten und dem Switch in einem Cluster unterbrochen ist, wird folgendes Symbol angezeigt:



Wenn Sie den Mauszeiger über das Symbol bewegen, können Sie detaillierte Informationen über das generierte Ereignis einsehen.

Wenn Sie in Ihrer MetroCluster Konfiguration Verbindungsprobleme identifizieren, müssen Sie sich bei System Manager anmelden oder auf die ONTAP CLI zugreifen, um die Probleme zu beheben.

Weitere Informationen zur Bestimmung des Clusterzustands finden sich unter "Bestimmen des Cluster-Systemstatus in der MetroCluster over FC Konfiguration".

Überwachung von Verbindungsproblemen in der MetroCluster over IP Konfiguration

Bei Clustern in einer MetroCluster over IP Konfiguration werden die Verbindungsdiagramme auf der Seite **Clusters** angezeigt. Hierfür gelten die folgenden Schritte.

Schritte

1. Im linken Navigationsbereich wird **Storage** > **Cluster** ausgewählt.

   Eine Liste aller überwachten Cluster wird angezeigt.

2. In der Ansicht **Schutz: MetroClusters** können Sie den Namen des Clusters auswählen, für den Sie die Details der MetroCluster over IP-Konfiguration anzeigen möchten. Alternativ können Sie nach Clustern in einer MetroCluster Konfiguration filtern.
3. Zum Erweitern der Zeile dient das Caret v-Symbol. Das Caret-Symbol wird nur bei Clustern angezeigt, die durch eine MetroCluster over IP Konfiguration geschützt sind.

   Die Topologie der Quell- und Spiegelstandorte sowie gegebenenfalls der für die Verbindung verwendete

Mediator sind einsehbar. Die folgenden Informationen sind einsehbar:

- Konnektivität zwischen den Standorten
- Etwaige Probleme mit Systemstatus und Verfügbarkeit auf beiden Standorten
- Probleme im Zusammenhang mit Mediator
- Probleme im Zusammenhang mit der Replikation.

> Die folgenden Status werden gemeldet: Kritisch (), Fehler () oder Normal (). Sie können auch den aggregierten Datenreplizierungsstatus der Primärdaten und der gespiegelten Daten in derselben Topologie anzeigen.

Im folgenden Diagramm ist ersichtlich, dass keine standortübergreifende Konnektivität zwischen dem Quell- und dem Ziel-Cluster besteht und der Mediator zwischen ihnen nicht konfiguriert ist.



4. Das Statussymbol kann angeklickt werden. Eine Meldung mit der Fehlerdefinition wird angezeigt. Wenn für das Problem in Ihrer MetroCluster over IP Konfiguration ein Ereignis ausgelöst wurde, kann in der Meldung auf die Schaltfläche **View Event** geklickt werden, um die Ereignisdetails anzuzeigen. Sobald das Problem und das Ereignis behoben wurden, wechselt das Statussymbol in dieser Topologie wieder zu „Normal“ ( ).
5. Weitere Konfigurationsdetails stehen in den Abschnitten **MetroCluster Übersicht** und **Schutz** auf der Registerkarte **Konfiguration** der Detailseite **Cluster / Systemstatus** zur Verfügung.

> Nur bei einer MetroCluster over IP Konfiguration kann die Clustertopologie auf der Seite **Clusters** angezeigt werden. Bei Clustern in einer MetroCluster over FC Konfiguration wird die Topologie auf der Registerkarte **MetroCluster Connectivity** auf der Detailseite **Cluster / Systemstatus** angezeigt.

Verwandte Informationen

- "Cluster-/Systemstatusdetailseite"
- Informationen zur Ansicht **Beziehung:MetroCluster** sind unter "Überwachung von MetroCluster Konfigurationen" verfügbar.

- Informationen zur Ansicht **Beziehung: Transferstatus des letzten Monats** sind unter "Beziehung: Ansicht des Übertragungsstatus des letzten Monats" verfügbar.
- Informationen zur Ansicht **Beziehung: Transferrate des letzten Monats** finden sich unter "Beziehung: Ansicht der Datentransferrate des letzten Monats".
- Informationen zur Ansicht **Beziehung: Alle Beziehungen** sind unter "Beziehung: Ansicht Alle Beziehungen" verfügbar.

Überwachung der MetroCluster Replikation in Active IQ Unified Manager

Sie können den allgemeinen Systemstatus der logischen Verbindungen während der Spiegelung der Daten überwachen und diagnostizieren. Sie können Probleme oder Risiken identifizieren, die die Spiegelung von Clusterkomponenten wie Aggregaten, Knoten und Storage Virtual Machines unterbrechen.

Unified Manager verwendet Systemstatuswarnungen, um den Status der Komponenten und die Konnektivität in der MetroCluster Konfiguration zu überwachen.

Bevor Sie beginnen

Sowohl der lokale als auch der Remote-Cluster in der MetroCluster Konfiguration müssen zu Unified Manager hinzugefügt werden

Ansicht der Replikation für MetroCluster over IP Konfigurationen

Bei MetroCluster over IP Konfigurationen wird der Status der Datenreplizierung in der Topologie-Übersicht für einen durch MetroCluster over IP geschützten Cluster in den folgenden Ansichten im linken Navigationsbereich von Unified Manager angezeigt:

- **Storage** > **Cluster** > **Schutz: MetroCluster** Ansicht
- **Schutz** > **Beziehungen** > **Beziehung: MetroCluster** Ansicht

Informationen finden sich unter "Überwachung von Verbindungsproblemen in MetroCluster over IP".

Replikation für MetroCluster over FC-Konfigurationen anzeigen

Mit diesen Schritten lassen sich etwaige Probleme bei der Datenreplizierung in der MetroCluster over FC Konfiguration ermitteln.

Schritte

1. Im linken Navigationsbereich wird **Storage** > **Cluster** ausgewählt.

   Eine Liste der überwachten Cluster wird angezeigt.

2. In der Ansicht **Systemstatus: Alle Cluster** können Sie den Namen des Clusters auswählen, für den Sie die MetroCluster Replikationsdetails anzeigen möchten. Auf der Seite **Cluster / Systemstatusdetails** können Sie auf die Registerkarte **MetroCluster Replikation** klicken.

   Die Topologie der zu replizierenden MetroCluster Konfiguration wird am lokalen Standort im entsprechenden Clusterobjektbereich zusammen mit Informationen über den Remote-Standort angezeigt, an dem die Daten gespiegelt werden. Wenn Sie den Mauszeiger über das Symbol bewegen, können Sie detaillierte Informationen über das generierte Ereignis anzeigen.

Anhand der auf der Seite „Cluster/Systemstatus-Details“ angezeigten Informationen lassen sich

Replizierungsprobleme beheben. Wenn Sie in Ihrer MetroCluster Konfiguration Spiegelungsprobleme identifizieren, müssen Sie sich bei System Manager anmelden oder auf die ONTAP CLI zugreifen, um die Probleme zu beheben.

Verwandte Informationen

"Cluster-/Systemstatusdetailseite"

Quoten managen

Informationen zu Kontingentgrenzen in Active IQ Unified Manager

Benutzerkontingentgrenzen sind Werte, anhand derer der Unified Manager Server beurteilt, ob die Speicherplatznutzung eines Benutzers sich der festgelegten Grenze nähert oder diese bereits erreicht hat. Wenn die weiche Grenze überschritten wird oder das endgültige Limit erreicht ist, generiert der Unified Manager Server Benutzerkontingentereignisse.

Standardmäßig sendet der Unified Manager Server eine Benachrichtigungs-E-Mail an Benutzer, die das weiche Kontingentlimit überschritten oder das endgültige Limit erreicht haben und für die Benutzerkontingentereignisse konfiguriert sind. Benutzer mit der Rolle Application Administrator können Warnungen konfigurieren, die die angegebenen Empfänger über Kontingentereignisse von Benutzern oder Benutzergruppen benachrichtigen.

Sie können Kontingentlimits entweder mit ONTAP System Manager oder der ONTAP CLI festlegen.

Benutzer- und Benutzergruppenkontingente in Active IQ Unified Manager anzeigen

Die Seite „Storage VM / Systemstatusdetails“ zeigt Informationen zu den auf der SVM konfigurierten Benutzer- und Benutzergruppenkontingenten an. Angezeigt werden der Name des Benutzers oder der Benutzergruppe, die für die Datenträger und Dateien festgelegten Grenzwerte, der belegte Datenträger- und Dateispeicherplatz sowie die E-Mail-Adresse für Benachrichtigungen.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritte

1. Die Auswahl erfolgt im linken Navigationsbereich über **Storage** > **Storage VMs**.
2. In der Ansicht **Systemstatus: Alle Storage VMs** ist eine Storage VM auszuwählen und anschließend die Registerkarte **Benutzer- und Gruppenkontingente** anzuklicken.

Verwandte Informationen

"Hinzufügen von Benutzern"

Regeln zum Generieren von E-Mail-Adressen in Active IQ Unified Manager

Sie können Regeln erstellen, um die E-Mail-Adresse auf der Grundlage des Benutzerkontingents festzulegen, das Clustern, storage virtual machines (SVMs),

Volumes, qtrees, Benutzern oder Benutzergruppen zugeordnet ist. Bei einer Kontingentüberschreitung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen die Richtlinien auf der Seite „Regeln zur Generierung von E-Mail-Adressen für Benutzer- und Gruppenkontingente“ gelesen haben.

Sie müssen die Regeln für die Kontingent-E-Mail-Adressen definieren und sie in der Reihenfolge eingeben, in der sie ausgeführt werden sollen. Wenn Sie beispielsweise die E-Mail-Adresse abc@xyz.com verwenden möchten, um Benachrichtigungen über Kontingentüberschreitungen für abc zu erhalten, und die E-Mail-Adresse dl-$GROUP@$DOMAIN für alle anderen Gruppen, müssen die Regeln in folgender Reihenfolge aufgelistet werden:

- if ($USER == 'abc') then abc@xyz.com
- if ($GROUP == *) then dl-$GROUP@$DOMAIN

Wenn keines der Kriterien für die von Ihnen angegebenen Regeln erfüllt ist, gilt die Standardregel:

if ($USER_OR_GROUP == *) then $USER_OR_GROUP@$DOMAIN

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **General** > **Quota Email Rules**.
2. Die Regel wird anhand Ihrer Kriterien eingegeben.
3. Durch Klicken auf **Validate** können Sie die Syntax der Regel überprüfen.

   Wenn die Syntax der Regel fehlerhaft ist, wird eine Fehlermeldung angezeigt. Sie müssen die Syntax korrigieren und erneut auf **Validate** klicken.

4. Auf **Speichern** klicken.
5. Zu prüfen ist, ob die von Ihnen erstellte E-Mail-Adresse auf der Registerkarte **Benutzer- und Gruppenkontingente** der Detailseite **Storage VM / Systemstatus** angezeigt wird.

Ein E-Mail-Benachrichtigungsformat für Benutzer- und Gruppenkontingente in Active IQ Unified Manager erstellen

Sie können ein Benachrichtigungsformat für die E-Mails erstellen, die ein Benutzer oder eine Benutzergruppe erhalten, wenn ein kontingentbezogenes Problem auftritt (weiches Limit überschritten oder endgültiges Limit erreicht).

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich auf **Allgemein** > **E-Mail-Format für Kontingente** klicken.
2. In den Feldern **Von**, **Betreff** und **E-Mail-Details** können die Details eingegeben oder geändert werden.
3. Über **Vorschau** lässt sich eine Vorschau der E-Mail-Benachrichtigung anzeigen.

4. Zum Schließen des Vorschaufensters **Schließen** auswählen.
5. Bei Bedarf lässt sich der Inhalt der E-Mail-Benachrichtigung anpassen.
6. Auf **Speichern** klicken.

Bearbeiten von E-Mail-Adressen für Benutzer- und Gruppenkontingente in Active IQ Unified Manager

Sie können die E-Mail-Adressen basierend auf dem Benutzerkontingent ändern, das Clustern, Storage Virtual Machines (SVMs), Volumes, qtrees, Benutzern oder Benutzergruppen zugeordnet ist. Sie können die E-Mail-Adresse ändern, wenn Sie die E-Mail-Adresse überschreiben möchten, die durch die im Dialogfeld „Regeln zum Generieren von E-Mail-Adressen für Benutzer- und Gruppenkontingente“ festgelegten Regeln generiert wurde.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Sie müssen die "Richtlinien für die Erstellung von Regeln" geprüft haben.

Wenn Sie eine E-Mail-Adresse bearbeiten, gelten die Regeln zur Generierung der E-Mail-Adressen für Benutzerkontingent und Gruppenkontingent nicht mehr für das Kontingent. Damit Benachrichtigungen an die gemäß den festgelegten Regeln generierte E-Mail-Adresse gesendet werden, müssen Sie die E-Mail-Adresse löschen und die Änderung speichern.

Schritte

1. Im linken Navigationsbereich auf **Storage** > **SVMs** klicken.
2. In der Ansicht **Systemstatus: Alle Storage VMs** wird eine SVM ausgewählt, anschließend wird auf die Registerkarte **Benutzer- und Gruppenkontingente** geklickt.
3. Unterhalb der Registerkartenleiste befindet sich **E-Mail-Adresse bearbeiten**.
4. Im Dialogfeld **E-Mail-Adresse bearbeiten** ist die entsprechende Aktion auszuführen:

Wenn…	Dann…
Sie möchten, dass Benachrichtigungen an die durch die angegebenen Regeln generierte E-Mail-Adresse gesendet werden	a. Sie können die E-Mail-Adresse im Feld **E-Mail-Adresse** löschen. b. Auf **Speichern** klicken. c. Durch Drücken von F5 wird der Browser aktualisiert und das Dialogfeld „E-Mail-Adresse bearbeiten“ neu geladen. Die durch die angegebene Regel generierte E-Mail-Adresse wird im Feld „E-Mail-Adresse“ angezeigt.
Sie möchten, dass Benachrichtigungen an eine bestimmte E-Mail-Adresse gesendet werden	a. Die E-Mail-Adresse wird im Feld **E-Mail-Adresse** geändert. b. Anschließend erfolgt die Auswahl von **Save**. Die Regeln zum Generieren der E-Mail-Adressen für Benutzerkontingent und Gruppenkontingent sind auf das Kontingent nicht mehr anwendbar.

Weitere Informationen zu Quoten

Informationen zum Kontingentprozess von Active IQ Unified Manager

Quoten können weich oder hart sein. Weiche Quoten veranlassen ONTAP, eine Benachrichtigung zu senden, wenn festgelegte Grenzwerte überschritten werden, und harte Quoten verhindern, dass ein Schreibvorgang erfolgreich ist, wenn festgelegte Grenzwerte überschritten werden.

Wenn ONTAP eine Anfrage von einem Benutzer oder einer Benutzergruppe zum Schreiben auf ein FlexVol volume erhält, prüft es, ob für diesen Benutzer oder diese Benutzergruppe Quoten auf diesem volume aktiviert sind und ermittelt Folgendes:

- Ob das endgültige Limit erreicht wird

  Falls ja, schlägt der Schreibvorgang fehl, wenn das endgültige Limit erreicht ist und die Benachrichtigung über das endgültige Limit gesendet wird.

- Ob das weiche Limit überschritten wird

  Wenn ja, ist der Schreibvorgang erfolgreich, wenn das Soft-Limit überschritten wird und die Soft-Quota-Benachrichtigung gesendet wird.

- Ob ein Schreibvorgang das Softlimit nicht überschreitet

  Wenn ja, ist der Schreibvorgang erfolgreich und es wird keine Benachrichtigung gesendet.

Informationen zu Quoten in Active IQ Unified Manager

Quotas ermöglichen es, den von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Speicherplatz und die Anzahl der Dateien einzuschränken oder nachzuverfolgen. Quotas werden mithilfe der `/etc/quotas`Datei angegeben. Quotas werden auf ein bestimmtes Volume oder einen bestimmten Qtree angewendet.

Informationen zu Quoten in Active IQ Unified Manager

Sie können Quoten verwenden, um die Ressourcennutzung in FlexVol Volumes zu begrenzen, Benachrichtigungen zu erhalten, wenn die Ressourcennutzung bestimmte Werte erreicht, oder die Ressourcennutzung zu verfolgen.

Sie legen aus folgenden Gründen ein Kontingent fest:

- Um den Speicherplatz oder die Anzahl der Dateien zu begrenzen, die von einem Benutzer oder einer Gruppe verwendet werden können oder die in einem qtree enthalten sein können
- Zum Nachverfolgen des von einem Benutzer, einer Gruppe oder einem qtree verwendeten Speicherplatzes oder der Anzahl der Dateien, ohne ein Limit festzulegen
- Zum Warnen von Benutzern, wenn ihre Festplatten- oder Dateinutzung hoch ist

Beschreibung der Dialogfelder für Kontingente

Das Dialogfeld „Kontingente“ in Active IQ Unified Manager kann verwendet werden

Sie können die entsprechende Option auf der Registerkarte „Benutzer- und Gruppenkontingente“ in der Ansicht „Systemstatus: Alle Storage-VMs“ verwenden, um das Format der E-Mail-Benachrichtigung zu konfigurieren, die bei einem kontingentbezogenen Problem gesendet wird, und um Regeln zu konfigurieren, die E-Mail-Adressen basierend auf dem Benutzerkontingent festlegen.

Informationen zur Seite „E-Mail-Benachrichtigungsformat“ in Active IQ Unified Manager

Auf der Seite „E-Mail-Benachrichtigungsformat“ finden Sie die Regeln für die E-Mail, die ein Benutzer oder eine Benutzergruppe erhält, wenn ein kontingentbezogenes Problem auftritt (weiches Limit überschritten oder endgültiges Limit erreicht).

Die E-Mail-Benachrichtigung wird nur dann gesendet, wenn die folgenden Ereignisse für das Benutzerkontingent oder Gruppenkontingent generiert werden: Soft Limit für den Speicherplatz des Benutzerkontingents oder Gruppenkontingents überschritten, Soft Limit für die Anzahl der Dateien des Benutzerkontingents oder Gruppenkontingents überschritten, endgültiges Limit für den Speicherplatz des Benutzerkontingents oder Gruppenkontingents erreicht oder endgültiges Limit für die Anzahl der Dateien des Benutzerkontingents oder Gruppenkontingents erreicht.

- **Von**

  Hier wird die E-Mail-Adresse angezeigt, von der die E-Mail gesendet wird und die Sie ändern können. Standardmäßig ist dies die E-Mail-Adresse, die auf der Benachrichtigungsseite angegeben ist.

- **Thema**

  Zeigt den Betreff der Benachrichtigungs-E-Mail an.

- **E-Mail-Details**

  Hier wird der Text der Benachrichtigungs-E-Mail angezeigt. Sie können den Text entsprechend Ihren Anforderungen anpassen. Beispielsweise können Sie Informationen zu den Kontingentattributen hinzufügen und die Anzahl der Schlüsselwörter reduzieren. Die Schlüsselwörter selbst sollten Sie jedoch nicht ändern.

  Gültige Schlüsselwörter sind wie folgt:

  - $EVENT_NAME

    Gibt den Namen des Ereignisses an, das die E-Mail-Benachrichtigung ausgelöst hat.

  - $QUOTA_TARGET

    Gibt den Qtree oder das Volume an, für das das Kontingent gilt.

  - $QUOTA_USED_PERCENT

    Gibt den Prozentsatz des endgültigen Festplatten-Limits, des weichen Festplatten-Limits, des endgültigen Datei-Limits oder des weichen Datei-Limits an, der vom Benutzer oder der Benutzergruppe verwendet wird.

◦ $QUOTA_LIMIT

Gibt das endgültige Festplattenlimit oder das endgültige Dateilimit an, das vom Benutzer oder von der Benutzergruppe erreicht wird und bei dem eines der folgenden Ereignisse generiert wird:

- Endgültiges Limit für Festplattenspeicher des Benutzer- oder Gruppenkontingents erreicht
- Weicher Grenzwert für Festplattenspeicher bei Benutzer- oder Gruppenkontingent erreicht
- Endgültiges Limit für die Dateianzahl des Benutzer- oder Gruppenkontingents erreicht
- Soft-Limit für Dateianzahl des Benutzer- oder Gruppenkontingents erreicht

◦ $QUOTA_USED

Gibt den belegten Speicherplatz oder die Anzahl der vom Benutzer oder der Benutzergruppe erstellten Dateien an.

◦ $QUOTA_USER

Gibt den Namen des Benutzers oder der Benutzergruppe an.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie die Änderungen am E-Mail-Benachrichtigungsformat in der Vorschau anzeigen, speichern oder verwerfen:

- **Vorschau**

  Zeigt eine Vorschau der Benachrichtigungs-E-Mail an.

- **Auf Werkseinstellungen zurücksetzen**

  Stellt das Benachrichtigungsformat auf die werkseitigen Standardwerte zurück.

- **Speichern**

  Speichert die am Benachrichtigungsformat vorgenommenen Änderungen.

Informationen zu den Regeln für Kontingent-E-Mail-Adressen in Active IQ Unified Manager

Auf der Seite „Regeln zum Generieren von E-Mail-Adressen für Benutzer- und Gruppenkontingente“ können Sie Regeln erstellen, um E-Mail-Adressen auf der Grundlage des Benutzerkontingents festzulegen, das Clustern, SVMs, Volumes, qtrees, Benutzern oder Benutzergruppen zugeordnet ist. Wenn ein Kontingent überschritten wird, wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

Regelbereich

Sie müssen die Regeln für eine Kontingent-E-Mail-Adresse festlegen. Sie können auch Kommentare hinzufügen, um die Regeln zu erläutern.

Definition von Regeln

Sie müssen die Regeln in der Reihenfolge eingeben, in der sie ausgeführt werden sollen. Wenn das Kriterium der ersten Regel erfüllt ist, wird die E-Mail-Adresse auf Grundlage dieser Regel generiert. Wenn das Kriterium

nicht erfüllt ist, wird das Kriterium der nächsten Regel berücksichtigt und so weiter. Jede Zeile enthält eine separate Regel. Die Standardregel ist die letzte Regel in der Liste. Sie können die Prioritätsreihenfolge der Regeln ändern. Die Reihenfolge der Standardregel kann jedoch nicht geändert werden.

Wenn Sie beispielsweise die E-Mail-Adresse qtree1@xyz.com verwenden möchten, um Benachrichtigungen über Quotenüberschreitungen für qtree1 zu erhalten, und die E-Mail-Adresse admin@xyz.com für alle anderen qtrees verwenden möchten, müssen die Regeln in der folgenden Reihenfolge aufgelistet werden:

- if ($QTREE == 'qtree1') then qtree1@xyz.com
- if ($QTREE == *) then admin@xyz.com

Wenn keines der Kriterien für die von Ihnen angegebenen Regeln erfüllt ist, gilt die Standardregel:

if ($USER_OR_GROUP == *) then $USER_OR_GROUP@$DOMAIN

Wenn mehr als ein Benutzer dasselbe Kontingent hat, werden die Namen der Benutzer als kommagetrennte Werte angezeigt, und die Regeln gelten nicht für das Kontingent.

Hinzufügen von Kommentaren

Sie können Kommentare hinzufügen, um die Regeln zu erläutern. Am Anfang jedes Kommentars steht ein #, und jede Zeile enthält einen separaten Kommentar.

Regelsyntax

Die Syntax der Regel muss einer der folgenden entsprechen:

- wenn (`valid variableoperator *`) dann `email ID@domain name`

  if ist ein Schlüsselwort und wird kleingeschrieben. Der Operator ist ==. Die E-Mail-ID kann beliebige Zeichen, die gültigen Variablen $USER_OR_GROUP, $USER oder $GROUP oder eine Kombination aus beliebigen Zeichen und den gültigen Variablen $USER_OR_GROUP, $USER oder $GROUP enthalten. Der Domainname kann beliebige Zeichen, die gültige Variable $DOMAIN oder eine Kombination aus beliebigen Zeichen und der gültigen Variable $DOMAIN enthalten. Gültige Variablen können in Groß- oder Kleinbuchstaben geschrieben werden, dürfen aber keine Kombination aus beidem sein. Beispielsweise sind $domain und $DOMAIN gültig, aber $Domain ist keine gültige Variable.

- wenn (`valid variableoperator` `` `string` ``) dann `email ID@domain name`

  if ist ein Schlüsselwort und wird kleingeschrieben. Der Operator kann contains oder == sein. Die E-Mail-ID kann beliebige Zeichen, die gültigen Variablen $USER_OR_GROUP, $USER oder $GROUP oder eine Kombination aus beliebigen Zeichen und den gültigen Variablen $USER_OR_GROUP, $USER oder $GROUP enthalten. Der Domainname kann beliebige Zeichen, die gültige Variable $DOMAIN oder eine Kombination aus beliebigen Zeichen und der gültigen Variable $DOMAIN enthalten. Gültige Variablen können in Groß- oder Kleinbuchstaben geschrieben werden, dürfen aber keine Kombination aus beidem sein. Beispielsweise sind $domain und $DOMAIN gültig, $Domain ist jedoch keine gültige Variable.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie die erstellten Regeln speichern, validieren oder abbrechen:

- **Validieren**

  Prüft die Syntax der erstellten Regel. Treten während der Prüfung Fehler auf, wird die fehlerhafte Regel zusammen mit einer Fehlermeldung angezeigt.

- **Auf Werkseinstellungen zurücksetzen**

  Damit können Sie die Adressregeln auf die werkseitigen Standardwerte zurücksetzen.

- **Speichern**

  Die Syntax der Regel wird geprüft, und die Regel wird gespeichert, wenn keine Fehler vorliegen. Wenn bei der Validierung Fehler auftreten, wird die Regel, die den Fehler verursacht, zusammen mit einer Fehlermeldung angezeigt.

Fehlerbehebung

Hinzufügen von Speicherplatz zum Unified Manager Datenbankverzeichnis

Hinzufügen von Festplattenspeicher zum Datenbankverzeichnis in Active IQ Unified Manager

Das Unified Manager Datenbankverzeichnis enthält alle von ONTAP Systemen erfassten Systemstatus- und Performance-Daten. Unter bestimmten Umständen kann es erforderlich sein, die Größe des Datenbankverzeichnisses zu erhöhen.

Das Datenbankverzeichnis kann beispielsweise voll werden, wenn Unified Manager Daten von einer großen Anzahl von Clustern erfasst, von denen jedes viele Knoten hat. Sie erhalten ein Warnereignis, wenn das Datenbankverzeichnis zu 90 % gefüllt ist, und ein kritisches Ereignis, wenn das Verzeichnis zu 95 % gefüllt ist.

Sobald das Verzeichnis zu 95% gefüllt ist, werden keine zusätzlichen Daten mehr von Clustern erfasst.

Die zum Erweitern der Kapazität des Datenverzeichnisses erforderlichen Schritte unterscheiden sich je nachdem, ob Unified Manager auf einem VMware ESXi Server, einem Red Hat Linux Server oder einem Microsoft Windows Server ausgeführt wird.

Hinzufügen von Speicherplatz zur Datenfestplatte der VMware Virtual Machine in Active IQ Unified Manager

Wenn Sie den Speicherplatz auf der Datenfestplatte für die Unified Manager Datenbank erhöhen müssen, können Sie nach der Installation Kapazität hinzufügen, indem Sie den Festplattenspeicher über die Unified Manager Wartungs-Managementplattform vergrößern.

Bevor Sie beginnen

- Sie müssen Zugriff auf den vSphere Client haben.
- Die virtuelle Maschine darf keine lokal gespeicherten Snapshots enthalten.
- Sie benötigen die Zugangsdaten für den Wartungsbenutzer.

Wir empfehlen Ihnen, Ihre virtuelle Maschine zu sichern, bevor Sie die Größe der virtuellen Festplatten erhöhen.

Schritte

1. Im vSphere Client können Sie die virtuelle Maschine Unified Manager auswählen und dann die Festplattenkapazität für Daten `disk 3` erweitern. Einzelheiten sind der VMware Dokumentation zu

entnehmen.

In einigen seltenen Fällen verwendet das Unified Manager Deployment statt „Festplatte 3“ „Festplatte 2“ als Datenfestplatte. Falls dies in Ihrem Deployment der Fall ist, ist der Speicherplatz der jeweils größeren Festplatte zu erhöhen. Die Datenfestplatte verfügt stets über mehr Speicherplatz als die andere Festplatte.

2. Im vSphere Client werden die virtuelle Maschine Unified Manager und anschließend die Registerkarte **Console** ausgewählt.
3. Im Fenster der Managementplattform erfolgt anschließend die Anmeldung an der Wartungskonsole mit Ihrem Benutzernamen und Passwort.
4. Im **Hauptmenü** erfolgt die Eingabe der Nummer für die Option **Systemkonfiguration**.
5. Im **Systemkonfigurationsmenü** ist die Zahl für die Option **Datenträgergröße erhöhen** einzugeben.

Hinzufügen von Speicherplatz zum Datenverzeichnis des Linux Hosts in Active IQ Unified Manager

Falls Sie bei der ursprünglichen Einrichtung des Linux-Hosts dem `/opt/netapp/data` Verzeichnis nicht genügend Speicherplatz zur Unterstützung von Unified Manager zugewiesen und anschließend Unified Manager installiert haben, können Sie nach der Installation zusätzlichen Speicherplatz hinzufügen, indem Sie den Speicherplatz im `/opt/netapp/data` Verzeichnis erhöhen.

Bevor Sie beginnen

Sie benötigen Zugriff als Root-Benutzer auf den Red Hat Enterprise Linux Rechner, auf dem Unified Manager installiert ist.

Wir empfehlen Ihnen, die Unified Manager Datenbank zu sichern, bevor Sie die Größe des Datenverzeichnisses erhöhen.

Schritte

1. Die Anmeldung als Root-Benutzer erfolgt auf dem Linux-Rechner, auf dem zusätzlicher Festplattenspeicher hinzugefügt werden soll.
2. Das Beenden des Unified Manager Service und der zugehörigen MySQL Software erfolgt in der angegebenen Reihenfolge: `systemctl stop ocieau ocie mysqld`
3. Es wird ein temporärer Sicherungsordner (zum Beispiel `/backup-data`) mit ausreichendem Speicherplatz für die Daten im aktuellen `/opt/netapp/data` Verzeichnis benötigt.
4. Der Inhalt und die Berechtigungskonfiguration des vorhandenen `/opt/netapp/data`Verzeichnisses sind in das Sicherungsdatenverzeichnis zu kopieren:

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

5. Wenn SE Linux aktiviert ist:

   a. SE Linux-Typ für Ordner in einem vorhandenen `/opt/netapp/data` Ordner:

      ```
      se_type=`ls -Z /opt/netapp/data| awk '{print $4}'| awk -F: '{print $3}'|
      head -1
      ```

      Das System gibt eine Bestätigung zurück, die in etwa wie folgt aussieht:

```
echo $se_type
mysqld_db_t
```

a. Der `chcon` Befehl legt den SE Linux Typ für das Backup-Verzeichnis fest:

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Entfernen des Inhalts des `/opt/netapp/data` Verzeichnisses:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Die Größe des `/opt/netapp/data` Verzeichnisses ist mithilfe von LVM-Befehlen oder durch Hinzufügen zusätzlicher Festplatten auf mindestens 150 GB zu erweitern.

> Wenn Sie `/opt/netapp/data` von einer Festplatte erstellt haben, sollten Sie nicht versuchen, `/opt/netapp/data` sie als NFS- oder CIFS-Freigabe einzubinden. Denn in diesem Fall funktionieren einige LVM-Befehle, wie beispielsweise `resize` und `extend`, möglicherweise nicht wie erwartet, wenn Sie versuchen, den Speicherplatz zu erweitern.

8. Stellen Sie sicher, dass Eigentümer (mysql) und Gruppe (root) des `/opt/netapp/data`Verzeichnisses unverändert sind:

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

   Das System gibt eine Bestätigung zurück, die in etwa wie folgt aussieht:

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

9. Bei aktiviertem SE Linux muss der Kontext für das `/opt/netapp/data`Verzeichnis weiterhin auf mysqld_db_t gesetzt sein:
   a. `touch /opt/netapp/data/abc`
   b. `ls -Z /opt/netapp/data/abc`

      Das System gibt eine Bestätigung zurück, die in etwa wie folgt aussieht:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Es empfiehlt sich, die Datei `abc` zu löschen, damit diese überflüssige Datei in Zukunft keinen Datenbankfehler verursacht.
11. Den Inhalt aus `backup-data` back in das entpackte `/opt/netapp/data` Verzeichnis kopieren:

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

12. Wenn SE Linux aktiviert ist, ist der folgende Befehl auszuführen:

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

13. Start des MySQL-Dienstes:

    ```
    systemctl start mysqld
    ```

14. Nach dem Start des MySQL-Service erfolgt der Start der Services ocie und ocieau in der angegebenen Reihenfolge:

    ```
    systemctl start ocie ocieau
    ```

15. Nachdem alle Services gestartet sind, kann der Sicherungsordner `/backup-data` gelöscht werden:

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

Hinzufügen von Speicherplatz zum logischen Laufwerk des Microsoft Windows Servers in Active IQ Unified Manager

Wenn eine Vergrößerung des Speicherplatzes für die Unified Manager Datenbank erforderlich ist, kann die Kapazität des logischen Laufwerks erweitert werden, auf dem Unified Manager installiert ist.

Bevor Sie beginnen

Sie benötigen Windows-Administratorrechte.

Wir empfehlen Ihnen, die Unified Manager Datenbank zu sichern, bevor Sie Speicherplatz hinzufügen.

Schritte

1. Die Anmeldung als Administrator auf dem Windows-Server, dem zusätzlicher Festplattenspeicher hinzugefügt werden soll, ist erforderlich.
2. Im Folgenden ist der Schritt für die Methode zum Hinzufügen von mehr Platz aufgeführt:

Option	Beschreibung
Auf einem physischen Server sollte die Kapazität des logischen Laufwerks erhöht werden, auf dem der Unified Manager server installiert ist.	Die Schritte sind im Microsoft-Thema beschrieben: "Erweitern eines Basisvolumens"
Auf einem physischen Server wird eine Festplatte hinzugefügt.	Die Schritte sind im Microsoft-Thema beschrieben: "Hinzufügen von Festplatten"
Auf einer virtuellen Maschine die Größe einer Festplattenpartition erhöhen.	Die Schritte im VMware-Thema: "Vergrößern einer Festplattenpartition"

Das Erfassungsintervall für Leistungsstatistiken in Active IQ Unified Manager ändern

Das Standardintervall für die Erfassung von Performance Statistiken beträgt 5 Minuten. Sie können dieses Intervall auf 10 oder 15 Minuten ändern, falls die Erfassung von Daten

großer Cluster nicht innerhalb der Standardzeit abgeschlossen wird. Diese Einstellung betrifft die Erfassung von Statistiken aller Cluster, die von dieser Unified Manager Instanz überwacht werden.

Bevor Sie beginnen

Sie müssen über eine Benutzerkennung und ein Passwort verfügen, die für die Anmeldung an der Managementplattform für die Wartung des Unified Manager Servers autorisiert sind.

Die Bannermeldungen weisen auf das Problem hin, dass Erfassungen von Performance-Statistiken nicht rechtzeitig abgeschlossen werden `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>.`

Das Erfassungsintervall sollte nur dann geändert werden, wenn dies aufgrund eines Problems bei der Erfassung von Statistiken erforderlich ist. Diese Einstellung sollte aus keinem anderen Grund geändert werden.

> Eine Änderung dieses Werts gegenüber der Standardeinstellung von 5 Minuten kann sich auf die Anzahl und Häufigkeit der von Unified Manager gemeldeten Performance-Ereignisse auswirken. Beispielsweise lösen systemdefinierte Performance-Schwellenwerte Ereignisse aus, wenn die Richtlinie 30 Minuten lang überschritten wird. Bei einer Erfassungsdauer von 5 Minuten muss die Richtlinie in sechs aufeinanderfolgenden Erfassungsperioden überschritten werden. Bei einer Erfassungsdauer von 15 Minuten muss die Richtlinie nur in zwei Erfassungsperioden überschritten werden.

Eine Meldung am unteren Rand der Seite „Cluster Setup“ gibt das aktuelle Intervall für die Erfassung statistischer Daten an.

Schritte

1. Sie melden sich per SSH als Wartungsbenutzer am Unified Manager Host an.

   Die Eingabeaufforderungen der Unified Manager Wartungs-Managementplattform werden angezeigt.

2. Die Nummer der Menüoption mit der Bezeichnung **Konfiguration des Performance-Abfrageintervalls** eingeben und anschließend die Eingabetaste drücken.
3. Falls Sie dazu aufgefordert werden, geben Sie das Passwort des Wartungsbenutzers erneut ein.
4. Sie geben die Zahl für das neue Abfrageintervall ein, die Sie festlegen möchten, und drücken anschließend die Eingabetaste.

Wenn Sie das Unified Manager Erfassungsintervall auf 10 oder 15 Minuten geändert haben und derzeit eine Verbindung zu einem externen Datenanbieter (z. B. Graphite) besteht, müssen Sie das Übertragungsintervall des Datenanbieters so ändern, dass es dem Unified Manager Erfassungsintervall entspricht oder größer ist.

Ändern der Zeitspanne, für die Active IQ Unified Manager Ereignis- und Leistungsdaten speichert

Unified Manager speichert standardmäßig Ereignisdaten und Performance-Daten für 6 Monate für alle überwachten Cluster. Nach Ablauf dieser Frist werden ältere Daten automatisch gelöscht, um Platz für neue Daten zu schaffen. Dieser Standardzeitraum eignet sich für die meisten Konfigurationen gut, aber bei sehr großen Konfigurationen mit vielen Clustern und Knoten kann es erforderlich sein, die Aufbewahrungsdauer zu

verkürzen, damit Unified Manager optimal arbeitet.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Auf der Seite „Datenaufbewahrung“ können Sie die Aufbewahrungsfristen für diese beiden Datentypen ändern. Diese Einstellungen wirken sich auf die Aufbewahrung von Daten aus allen Clustern aus, die von dieser Unified Manager Instanz überwacht werden.

> Unified Manager erfasst alle 5 Minuten Performance-Statistiken. Jeden Tag werden die 5-Minuten-Statistiken zu stündlichen Performance-Statistiken zusammengefasst. Standardmäßig werden 30 Tage lang historische Performance-Daten in 5-Minuten-Intervallen und 6 Monate lang zusammengefasste stündliche Performance-Daten aufbewahrt.

Die Aufbewahrungsfrist sollte nur verkürzt werden, wenn der Speicherplatz knapp wird oder Sicherungs- und andere Vorgänge sehr lange dauern. Eine Verkürzung der Aufbewahrungsfrist hat folgende Auswirkungen:

- Alte Performance-Daten werden nach Mitternacht aus der Unified Manager Datenbank gelöscht.
- Alte Ereignisdaten werden sofort aus der Unified Manager Datenbank gelöscht.
- Ereignisse, die vor dem Aufbewahrungszeitraum liegen, können in der Benutzeroberfläche nicht mehr angezeigt werden.
- Bereiche in der UI, in denen stündliche Performance Statistiken angezeigt werden, sind vor dem Aufbewahrungszeitraum leer.
- Wenn die Aufbewahrungsfrist für Ereignisse die Aufbewahrungsfrist für Performance-Daten überschreitet, wird unter dem Performance-Regler eine Meldung angezeigt, die darauf hinweist, dass für ältere Performance-Ereignisse in den zugehörigen Diagrammen möglicherweise keine zugrunde liegenden Daten vorhanden sind.

Schritte

1. Im linken Navigationsbereich wählen Sie **Richtlinien** > **Datenaufbewahrung** aus.
2. Auf der Seite **Datenaufbewahrung** kann im Bereich Ereignisaufbewahrung oder Performance-Datenaufbewahrung mit dem Schieberegler die Anzahl der Monate festgelegt werden, für die Daten aufbewahrt werden; anschließend kann **Speichern** ausgewählt werden.

Behebung eines unbekannten Authentifizierungsfehlers in Active IQ Unified Manager

Wenn Sie eine authentifizierungsbezogene Operation wie das Hinzufügen, Bearbeiten, Löschen oder Testen von Remote-Benutzern oder -Gruppen durchführen, kann die folgende Fehlermeldung erscheinen: `Unknown authentication error.`

Ursache

Dieses Problem kann auftreten, wenn Sie für die folgenden Optionen einen falschen Wert festgelegt haben:

- Administratorname des Active Directory Authentifizierungsdienstes
- Individueller Name des OpenLDAP Authentifizierungsdienstes für die Authentifizierung

Korrekturmaßnahme

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Je nach ausgewähltem Authentifizierungsdienst sind die entsprechenden Informationen für Administrator Name oder Bind Distinguished Name einzugeben.
3. Über **Authentifizierung testen** lässt sich die Authentifizierung anhand der von Ihnen angegebenen Daten prüfen.
4. Auf **Speichern** klicken.

Behebung eines Fehlers „Benutzer nicht gefunden“ in Active IQ Unified Manager

Wenn Sie einen authentifizierungsbezogenen Vorgang ausführen, z. B. das Hinzufügen, Bearbeiten, Löschen oder Testen von Remote-Benutzern oder -Gruppen, wird die folgende Fehlermeldung angezeigt: `User not found.`

Ursache

Dieses Problem kann auftreten, wenn der Benutzer auf dem AD-Server oder LDAP-Server vorhanden ist und wenn Sie den Basis-individuellen Namen auf einen falschen Wert gesetzt haben.

Korrekturmaßnahme

1. Im linken Navigationsbereich wählen Sie **Allgemein** > **Remote-Authentifizierung** aus.
2. Hier werden die entsprechenden Informationen für den Basis-individuellen Namen eingegeben.
3. Auf **Speichern** klicken.

Behebung des Problems, das durch das Hinzufügen von LDAP über den Authentifizierungsdienst „Other authentication service“ in Active IQ Unified Manager verursacht wird

Wenn Sie „Andere“ als Authentifizierungsdienst auswählen, behalten die Objektklassen für Benutzer und Gruppen die Werte aus der zuvor ausgewählten Vorlage bei. Wenn der LDAP-Server nicht dieselben Werte verwendet, kann der Vorgang fehlschlagen.

Ursache

Die Benutzer sind in OpenLDAP nicht korrekt konfiguriert.

Korrekturmaßnahme

Sie können dieses Problem manuell beheben, indem Sie eine der folgenden Problemumgehungen verwenden.

Wenn Ihre LDAP-Benutzerobjektklasse und Gruppenobjektklasse „user“ bzw. „group“ sind, sind die folgenden Schritte erforderlich:

1. Die Auswahl erfolgt im linken Navigationsbereich über **Allgemein** > **Remote-Authentifizierung**.
2. Im Dropdown-Menü **Authentifizierungsdienst** erfolgt die Auswahl von **Active Directory** und anschließend von **Andere**.
3. Die Textfelder werden ausgefüllt.

Wenn Ihre LDAP-Benutzerobjektklasse bzw. Gruppenobjektklasse posixAccount und posixGroup lauten, sind die folgenden Schritte durchzuführen:

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Remote-Authentifizierung**.
2. Im Dropdown-Menü **Authentifizierungsdienst** erfolgt die Auswahl von **OpenLDAP** und anschließend **Andere**.
3. Die Textfelder werden ausgefüllt.

Falls die ersten beiden Lösungsansätze nicht anwendbar sind, erfolgt der Aufruf der `option-set` API, und die `auth.ldap.userObjectClass`- und `auth.ldap.groupObjectClass`-Optionen werden auf die korrekten Werte gesetzt.

Behebung eines Problems mit der Protokollrotation des NetApp Manageability SDK in Active IQ Unified Manager

Nach dem Hinzufügen eines ONTAPI API-basierten Clusters zu Unified Manager auf einem Windows-Betriebssystem erhöht sich die `nmsdk.log` Dateigröße und überschreitet die Größenbeschränkung von 10 MB.

Ursache

Dieses Problem kann auftreten, wenn keine Logrotation stattfindet.

Korrekturmaßnahme

1. Beenden von Unified Manager.
2. Bei der Installation von Unified Manager unter Windows kommt Logrotate Version 0.0.0.18 zum Einsatz. Weitere Informationen finden Sie in der "Leitfaden zur Sicherheitshärtung für den technischen Bericht zu NetApp Manageability SDK".
3. Starten von Unified Manager.

Verwalten von Ereignissen und Warnmeldungen

Ereignisse managen

Informationen zu Active IQ Plattformereignissen in Active IQ Unified Manager

Unified Manager kann Ereignisse anzeigen, die von der Active IQ Plattform erkannt wurden. Diese Ereignisse werden durch die Anwendung einer Reihe von Regeln auf AutoSupport Meldungen erstellt, die von allen von Unified Manager überwachten Storage-Systemen generiert werden.

Weitere Informationen sind unter "Wie Plattformereignisse von Active IQ generiert werden" verfügbar.

Unified Manager prüft automatisch, ob eine neue Regeldatei vorhanden ist, und lädt eine neue Datei nur dann herunter, wenn neuere Regeln verfügbar sind. An Standorten ohne externen Netzwerkzugriff müssen Sie die Regeln manuell über **Storage Management** > **Event Setup** > **Upload Rules** hochladen.

Diese Active IQ Ereignisse überschneiden sich nicht mit bestehenden Unified Manager Ereignissen und identifizieren Vorfälle oder Risiken in Bezug auf Systemkonfiguration, Verkabelung, bewährte Verfahren und Verfügbarkeitsprobleme.

Weitere Informationen zum Aktivieren von Plattformereignissen finden Sie unter "Aktivieren von Active IQ Portalereignissen". Weitere Informationen zum Hochladen der Regeldatei finden Sie unter "Hochladen einer neuen Active IQ Regeldatei".

NetApp Active IQ ist ein cloudbasierter Service, der prädiktive Analysen und proaktiven Support zur Optimierung des Speichersystembetriebs in der NetApp Hybrid Cloud bietet. Siehe "NetApp Active IQ" für weitere Informationen.

Was Event Management System Ereignisse sind

Informationen zu Ereignissen des Event Management System in Active IQ Unified Manager

Das Event Management System (EMS) erfasst Ereignisdaten aus verschiedenen Teilen des ONTAP Kernels und stellt Mechanismen zur Ereignisweiterleitung bereit. Diese ONTAP Ereignisse können im Unified Manager als EMS Ereignisse gemeldet werden. Die zentrale Überwachung und Verwaltung vereinfacht die Konfiguration kritischer EMS Ereignisse und Warnbenachrichtigungen auf der Grundlage dieser EMS Ereignisse.

Beim Hinzufügen des Clusters zu Unified Manager wird dem Cluster die Unified Manager-Adresse als Benachrichtigungsziel hinzugefügt. Ein EMS-Ereignis wird gemeldet, sobald es im Cluster auftritt.

Es gibt zwei Methoden zum Empfangen von EMS-Ereignissen im Unified Manager:

- Eine bestimmte Anzahl wichtiger EMS Ereignisse wird automatisch gemeldet.
- Sie können einzelne EMS-Ereignisse abonnieren.

Die von Unified Manager generierten EMS-Ereignisse werden je nach der Methode, mit der das Ereignis generiert wurde, unterschiedlich gemeldet:

Funktionalität	Automatische EMS Meldungen	Abonnierte EMS-Nachrichten
Verfügbare EMS-Ereignisse	Teilmenge der EMS-Ereignisse	Alle EMS-Ereignisse
Name der EMS-Meldung bei Auslösung	Unified Manager Ereignisname (konvertiert aus dem EMS Ereignisnamen)	Unspezifisch im Format "Error EMS received". Die detaillierte Meldung enthält die Punktnotation des tatsächlichen EMS-Ereignisses.
Empfangene Nachrichten	Sobald der Cluster erkannt wurde	Nach dem Hinzufügen jedes erforderlichen EMS-Ereignisses zu Unified Manager und nach dem nächsten 15-minütigen Abfragezyklus
Ereignislebenszyklus	Wie bei anderen Unified Manager-Ereignissen: Status „Neu“, „Bestätigt“, „Behoben“ und „Veraltet“	Das EMS-Ereignis ist nach der Aktualisierung des Clusters, 15 Minuten nach seiner Erstellung, obsolet
Erfasst Ereignisse während der Ausfallzeit von Unified Manager	Ja, beim Systemstart kommuniziert das System mit jedem Cluster, um fehlende Ereignisse abzurufen	Nein
Ereignisdetails	Vorgeschlagene Korrekturmaßnahmen werden direkt aus ONTAP importiert, um einheitliche Lösungen zu gewährleisten.	Korrekturmaßnahmen sind auf der Seite „Ereignisdetails“ nicht verfügbar

Einige der neuen automatischen EMS-Ereignisse sind Informationsereignisse, die anzeigen, dass ein vorheriges Ereignis behoben wurde. Beispielsweise zeigt das Informationsereignis "FlexGroup Constituents Space Status All OK" an, dass das Fehlerereignis "FlexGroup Constituents Have Space Issues" behoben wurde. Informationsereignisse können nicht mit demselben Ereignislebenszyklus verwaltet werden wie andere Ereignisse nach Typ des Schweregrads; das Ereignis wird jedoch automatisch als veraltet markiert, wenn dasselbe Volume ein weiteres Fehlerereignis “Space Issues” erhält.

EMS-Ereignisse, die automatisch zu Active IQ Unified Manager hinzugefügt werden

Die folgenden ONTAP EMS Ereignisse werden automatisch zu Unified Manager hinzugefügt. Diese Ereignisse werden generiert, wenn sie auf einem Cluster ausgelöst werden, den Unified Manager überwacht.

Die folgenden EMS-Ereignisse sind bei der Überwachung von Clustern verfügbar, auf denen ONTAP 9.5 oder höher ausgeführt wird:

Unified Manager Ereignisname	EMS Ereignisname	Betroffene Ressource	Unified Manager Schweregrad
Zugriff auf die Cloud-Ebene für die Aggregatverschiebung verweigert	arl.netra.ca.check.failed	Aggregat	Fehler

Unified Manager Ereignisname	EMS Ereignisname	Betroffene Ressource	Unified Manager Schweregrad
Zugriff auf Cloud Tier bei Aggregatverlagerung während Storage Failover verweigert	gb.netra.ca.check.failed	Aggregat	Fehler
FabricPool Spiegelreplikations-Resynchronisierung abgeschlossen	wafl.ca.resync.complete	Cluster	Fehler
FabricPool Speicherplatz fast voll	fabricpool.nearly.full	Cluster	Fehler
NVMe-oF Schonfrist gestartet	nvmf.graceperiod.start	Cluster	Warnung
NVMe-oF Kulanzfrist aktiv	nvmf.graceperiod.active	Cluster	Warnung
NVMe-oF Kulanzfrist abgelaufen	nvmf.graceperiod.expired	Cluster	Warnung
LUN zerstört	lun.destroy	LUN	Informationen
Cloud AWS MetaDataConnFail	cloud.aws.metadataConnFail	Node	Fehler
Cloud AWS IAMCredsExpired	cloud.aws.iamCredsExpired	Node	Fehler
Cloud AWS IAMCredsInvalid	cloud.aws.iamCredsInvalid	Node	Fehler
Cloud AWS IAMCredsNotFound	cloud.aws.iamCredsNotFound	Node	Fehler
Cloud AWS IAMCredsNotInitialized	cloud.aws.iamNotInitialized	Node	Informationen
Cloud AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	Node	Fehler
Cloud AWS IAMRoleNotFound	cloud.aws.iamRoleNotFound	Node	Fehler
Cloud Tier Host nicht auflösbar	objstore.host.unresolvable	Node	Fehler
Cloud Tier Intercluster Netzwerkschnittstelle ausgefallen	objstore.interclusterlifDown	Node	Fehler
Anfrage stimmt nicht mit der Cloud-Tier-Signatur überein	osc.signatureMismatch	Node	Fehler
Einer der NFSv4 Pools ist erschöpft	Nblade.nfsV4PoolExhaust	Node	Kritisch
QoS Monitor Speicher maximal belegt	qos.monitor.memory.maxed	Node	Fehler

Unified Manager Ereignisname	EMS Ereignisname	Betroffene Ressource	Unified Manager Schweregrad
QoS Monitor-Speicher reduziert	qos.monitor.memory.abated	Node	Informationen
NVMeNS zerstören	NVMeNS.destroy	Namensraum	Informationen
NVMeNS Online	NVMeNS.offline	Namensraum	Informationen
NVMeNS offline	NVMeNS.online	Namensraum	Informationen
NVMeNS hat keinen Speicherplatz mehr	NVMeNS.out.of.space	Namensraum	Warnung
Synchrone Replikation nicht synchron	sms.status.out.of.sync	SnapMirror Beziehung	Warnung
Synchrone Replikation wiederhergestellt	sms.status.in.sync	SnapMirror Beziehung	Informationen
Automatische Resynchronisierung der synchronen Replikation fehlgeschlagen	sms.resync.attempt.failed	SnapMirror Beziehung	Fehler
Viele CIFS-Verbindungen	Nblade.cifsManyAuths	SVM	Fehler
Maximale Anzahl an CIFS-Verbindungen überschritten	Nblade.cifsMaxOpenSameFile	SVM	Fehler
Maximale Anzahl von CIFS-Verbindungen pro Benutzer überschritten	Nblade.cifsMaxSessPerUsrConn	SVM	Fehler
CIFS NetBIOS Namenskonflikt	Nblade.cifsNbNameConflict	SVM	Fehler
Versuche zum Verbinden einer nicht vorhandenen CIFS-Freigabe	Nblade.cifsNoPrivShare	SVM	Kritisch
CIFS Shadow Copy Operation fehlgeschlagen	cifs.shadowcopy.failure	SVM	Fehler
Virus vom AV Server erkannt	Nblade.vscanVirusDetected	SVM	Fehler
Keine AV-Serververbindung für Virenscan	Nblade.vscanNoScannerConn	SVM	Kritisch
Kein AV Server registriert	Nblade.vscanNoRegdScanner	SVM	Fehler
Keine Verbindung zu einem antwortenden AV-Server	Nblade.vscanConnInactive	SVM	Informationen
AV Server ist zu ausgelastet, um neue Scan-Anfragen anzunehmen	Nblade.vscanConnBackPressure	SVM	Fehler

Unified Manager Ereignisname	EMS Ereignisname	Betroffene Ressource	Unified Manager Schweregrad
Unbefugter Benutzer versucht, auf den AV Server zuzugreifen	Nblade.vscanBadUserPrivAccess	SVM	Fehler
FlexGroup Bestandteile haben Platzprobleme.	flexgroup.constituents.have.space.issues	Volumen	Fehler
FlexGroup Status des Speicherplatzes der Bestandteile, alles OK	flexgroup.constituents.space.status.all.ok	Volumen	Informationen
FlexGroup Bestandteile haben Inode-Probleme	flexgroup.constituents.have.inodes.issues	Volumen	Fehler
FlexGroup Konstituenten Inode-Status alle OK	flexgroup.constituents.inodes.status.all.ok	Volumen	Informationen
Logischer Speicherplatz des Volume nahezu voll	monitor.vol.nearFull.inc.sav	Volumen	Warnung
Logischer Speicherplatz des Volume voll	monitor.vol.full.inc.sav	Volumen	Fehler
Normaler logischer Speicherplatz des Volume	monitor.vol.one.ok.inc.sav	Volumen	Informationen
WAFL Volume AutoSize Fehler	wafl.vol.autoSize.fail	Volumen	Fehler
WAFL Volume AutoSize abgeschlossen	wafl.vol.autoSize.done	Volumen	Informationen
Timeout der WAFL READDIR Dateioperation	wafl.readdir.expired	Volumen	Fehler

Abonnement von ONTAP EMS Ereignissen in Active IQ Unified Manager

Sie können Ereignisse des Event Management System (EMS) abonnieren, die von Systemen generiert werden, auf denen ONTAP Software installiert ist. Ein Teil der EMS-Ereignisse wird automatisch an Unified Manager gemeldet, weitere EMS-Ereignisse jedoch nur, wenn Sie diese Ereignisse abonniert haben.

Bevor Sie beginnen

Ein Abonnement von EMS-Ereignissen, die Unified Manager bereits automatisch hinzufügt, sollte vermieden werden, da der Empfang von zwei Ereignissen für dasselbe Problem zu Verwirrung führen kann.

Sie können eine beliebige Anzahl von EMS-Ereignissen abonnieren. Alle Ereignisse, die Sie abonnieren, werden validiert, und nur die validierten Ereignisse werden auf die Cluster angewendet, die Sie in Unified Manager überwachen. Der *ONTAP 9 EMS-Ereigniskatalog* enthält detaillierte Informationen zu allen EMS-Meldungen für die angegebene Version der ONTAP 9 Software. Die entsprechende Version des *EMS-Ereigniskatalogs* mit einer Liste der anwendbaren Ereignisse ist auf der Seite zur ONTAP 9 Produktdokumentation verfügbar.

"ONTAP 9 Produktbibliothek"

Sie können Benachrichtigungen für die ONTAP EMS-Ereignisse konfigurieren, die Sie abonniert haben, und

benutzerdefinierte Skripte erstellen, die bei diesen Ereignissen ausgeführt werden.

> Wenn Sie die ONTAP EMS-Ereignisse, die Sie abonniert haben, nicht erhalten, liegt möglicherweise ein Problem mit der DNS-Konfiguration des Clusters vor, das verhindert, dass das Cluster den Unified Manager-Server erreicht. Zur Behebung dieses Problems muss der Clusteradministrator die DNS-Konfiguration des Clusters korrigieren und anschließend Unified Manager neu starten. Dadurch werden die ausstehenden EMS-Ereignisse an den Unified Manager-Server weitergeleitet.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Ereigniseinrichtung**.
2. Auf der Seite „Event Setup“ erfolgt die Auswahl der Schaltfläche **Subscribe to EMS events**.
3. Im Dialogfeld „EMS-Ereignisse abonnieren“ geben Sie den Namen des ONTAP EMS-Ereignisses ein, das Sie abonnieren möchten.

   In der ONTAP Cluster-Shell lässt sich zum Anzeigen der Namen der EMS-Ereignisse, die Sie abonnieren können, der `event route show` Befehl (vor ONTAP 9) oder der `event catalog show` Befehl (ONTAP 9 oder höher) verwenden.

   "Konfiguration und Empfang von Warnmeldungen aus ONTAP EMS Event Subscription in Active IQ Unified Manager"

4. Klicken Sie auf **Add**.

   Das hinzugefügte EMS-Ereignis wird in der Liste der abonnierten EMS-Ereignisse aufgeführt, in der Spalte "Gilt für Cluster" wird jedoch der Status “Unknown” angezeigt.

5. Durch Klicken auf **Save and Close** wird das EMS-Ereignisabonnement beim Cluster registriert.
6. **EMS-Ereignisse abonnieren** erneut auswählen.

   In der Spalte „Gilt für Cluster“ erscheint für das von Ihnen hinzugefügte EMS-Ereignis der Status „`Ja`“.

   Wenn der Status nicht „`Yes`“ lautet, ist die Schreibweise des ONTAP EMS Ereignisnamens zu prüfen. Wenn der Name falsch eingegeben wurde, muss das betreffende Ereignis entfernt und anschließend erneut hinzugefügt werden.

Wenn das ONTAP EMS-Ereignis auftritt, wird das Ereignis auf der Seite „Ereignisse“ angezeigt. Sie können das Ereignis auswählen, um auf der Seite „Ereignisdetails“ Details zum EMS-Ereignis anzuzeigen. Sie können außerdem den Status des Ereignisses managen oder Benachrichtigungen für das Ereignis erstellen.

Hier wird erläutert, wie Active IQ Unified Manager ein empfangenes Ereignis verarbeitet

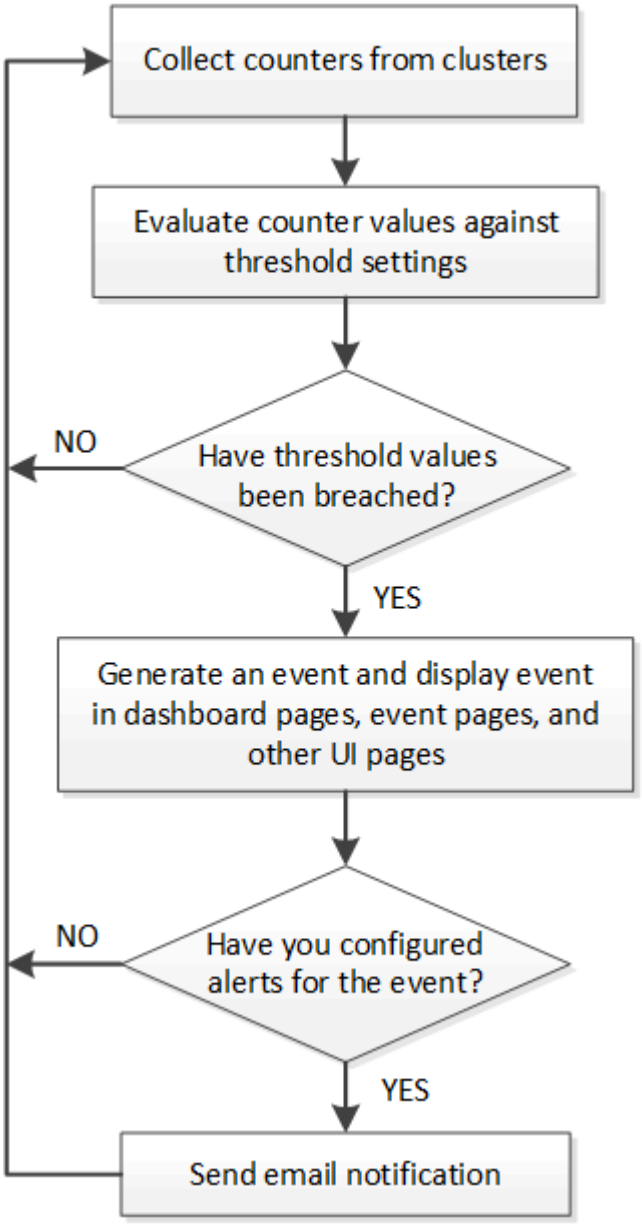
Wenn Unified Manager ein Ereignis empfängt, erscheint es auf der Dashboard-Seite, auf der Inventarseite „Event Management“, auf den Registerkarten „Summary“ und „Explorer“ der Seite „Cluster/Performance“ sowie auf der objektspezifischen Inventarseite (z. B. der Inventarseite „Volumes/Health“).

Wenn Unified Manager mehrere aufeinanderfolgende Vorkommen desselben Ereigniszustands für dieselbe Clusterkomponente erkennt, behandelt er alle Vorkommen als ein einziges Ereignis und nicht als separate Ereignisse. Die Dauer des Ereignisses erhöht sich, um anzuzeigen, dass das Ereignis noch aktiv ist.

Je nachdem, wie Sie die Einstellungen auf der Seite „Benachrichtigungseinrichtung“ konfigurieren, können Sie andere Benutzer über diese Ereignisse benachrichtigen. Die Benachrichtigung löst folgende Aktionen aus:

- Eine E-Mail über das Ereignis kann an alle Benutzer mit der Rolle Unified Manager Administrator gesendet werden.
- Das Ereignis kann an zusätzliche E-Mail-Empfänger gesendet werden.
- Ein SNMP Trap lässt sich an den Trap-Empfänger senden.
- Mit einem benutzerdefinierten Skript lässt sich eine Aktion ausführen.

Das folgende Diagramm zeigt diesen Arbeitsablauf.



Ereignisdetails in Active IQ Unified Manager

Sie können Details zu einem Ereignis anzeigen, das Unified Manager auslöst, damit Korrekturmaßnahmen ergriffen werden können. Wenn beispielsweise das Systemstatusereignis Volume Offline vorliegt, können Sie auf dieses Ereignis klicken, um

die Details anzuzeigen und Korrekturmaßnahmen durchzuführen.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Die Ereignisdetails umfassen Informationen wie die Quelle des Ereignisses, die Ursache des Ereignisses und alle zum Ereignis gehörenden Hinweise.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.

   Standardmäßig werden in der Ansicht „Alle aktiven Ereignisse“ die neuen und bestätigten (aktiven) Ereignisse angezeigt, die in den letzten 7 Tagen generiert wurden und die Auswirkungsstufe „Incident“ oder „Risiko“ aufweisen.

2. Wenn Sie eine bestimmte Kategorie von Ereignissen, z. B. Kapazitätsereignisse oder Performance Ereignisse, anzeigen möchten, können Sie auf **View** klicken und im Menü der Ereignistypen eine Auswahl treffen.
3. Details lassen sich anzeigen, indem der Name des entsprechenden Ereignisses ausgewählt wird.

   Die Ereignisdetails werden auf der Seite „Ereignisdetails“ angezeigt.

Nicht zugewiesene Ereignisse in Active IQ Unified Manager

Sie können nicht zugewiesene Ereignisse anzeigen und jedes einzelne einem Benutzer zuweisen, der es beheben kann.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.

   Standardmäßig zeigt die Inventarseite „Event Management“ neue und bestätigte Ereignisse an.

2. Im Bereich **Filter** erfolgt die Auswahl der Filteroption **Nicht zugewiesen** im Abschnitt **Zugewiesen an**.

Bestätigen und Beheben von Ereignissen in Active IQ Unified Manager

Sie sollten ein Ereignis bestätigen, bevor Sie mit der Bearbeitung des Problems beginnen, durch das das Ereignis ausgelöst wurde, damit Sie nicht weiterhin wiederholte Alarmbenachrichtigungen erhalten. Nachdem Sie für ein bestimmtes Ereignis eine Korrekturmaßnahme durchgeführt haben, sollten Sie das Ereignis als gelöst markieren.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Sie können mehrere Ereignisse gleichzeitig bestätigen und beheben.

Information Ereignisse können nicht quittiert werden.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.
2. In der Ereignisliste stehen zum Bestätigen der Ereignisse die folgenden Aktionen zur Verfügung:

Wenn Sie möchten…	Folgendes ist zu tun…
Ein einzelnes Ereignis bestätigen und als gelöst markieren	a. Den Ereignisnamen auswählen. b. Auf der Seite mit den Ereignisdetails lässt sich die Ursache des Ereignisses ermitteln. c. Auf **Bestätigen** klicken. d. Eine geeignete Korrekturmaßnahme ist einzuleiten. e. Anschließend **Als gelöst markieren** auswählen.
Bestätigung und Kennzeichnung mehrerer Ereignisse als gelöst	a. Die Ermittlung der Ursache der Ereignisse erfolgt auf der jeweiligen Ereignisdetailseite. b. Auswählen der Ereignisse. c. Auf **Bestätigen** klicken. d. Es sind geeignete Korrekturmaßnahmen einzuleiten. e. Anschließend **Als gelöst markieren** auswählen.

   Nachdem das Ereignis als behoben markiert wurde, wird es in die Liste der behobenen Ereignisse verschoben.

3. **Optional**: Im Bereich **Notizen und Aktualisierungen** lässt sich eine Notiz dazu hinzufügen, wie das Ereignis behandelt wurde; anschließend kann auf **Post** geklickt werden.

Zuweisung von Ereignissen an bestimmte Benutzer in Active IQ Unified Manager

Sie können nicht zugewiesene Ereignisse sich selbst oder anderen Benutzern, einschließlich Remote-Benutzern, zuweisen. Sie können zugewiesene Ereignisse bei Bedarf einem anderen Benutzer neu zuweisen. Wenn beispielsweise bei einem Storage Objekt häufig Probleme auftreten, können Sie die Ereignisse für diese Probleme dem Benutzer zuweisen, der dieses Objekt verwaltet.

Bevor Sie beginnen

- Der Name und die E-Mail-Adresse des Benutzers müssen korrekt konfiguriert sein.
- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.
2. Auf der Inventarseite **Event Management** erfolgt die Auswahl eines oder mehrerer Events, die zugewiesen werden sollen.
3. Die Zuweisung des Ereignisses erfolgt durch Auswahl einer der folgenden Optionen:

Wenn das Ereignis zugewiesen werden soll …	Fahren Sie dann wie folgt fort…
Sie selbst	Anschließend erfolgt die Auswahl von **Zuweisen an** > **Mich**.
Ein anderer Benutzer	a. Die Auswahl erfolgt über **Zuweisen an** > **Anderer Benutzer**. b. Im Dialogfeld „Besitzer zuweisen“ können Sie den Benutzernamen eingeben oder einen Benutzer aus der Dropdown-Liste auswählen. c. **Zuweisen** auswählen. Der Benutzer erhält eine E-Mail-Benachrichtigung. Wenn Sie keinen Benutzernamen eingeben oder keinen Benutzer aus der Dropdown-Liste auswählen und auf **Zuweisen** klicken, bleibt das Ereignis nicht zugewiesen.

Unerwünschte Ereignisse in Active IQ Unified Manager deaktivieren

Alle Ereignisse sind standardmäßig aktiviert. Sie können Ereignisse global deaktivieren, um zu verhindern, dass Benachrichtigungen für Ereignisse generiert werden, die in Ihrer Umgebung nicht relevant sind. Sie können deaktivierte Ereignisse wieder aktivieren, wenn Sie wieder Benachrichtigungen darüber erhalten möchten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Wenn Sie Ereignisse deaktivieren, werden die zuvor im System generierten Ereignisse als veraltet markiert, und die für diese Ereignisse konfigurierten Warnmeldungen werden nicht ausgelöst. Wenn Sie deaktivierte Ereignisse wieder aktivieren, werden die Benachrichtigungen für diese Ereignisse ab dem nächsten Überwachungszyklus generiert.

Wenn Sie ein Ereignis für ein Objekt deaktivieren, z. B. das `vol offline`Ereignis, und es später wieder aktivieren, generiert Unified Manager keine neuen Ereignisse für Objekte, die offline waren, als das Ereignis deaktiviert war. Unified Manager generiert nur dann ein neues Ereignis, wenn sich der Objektstatus nach der Reaktivierung des Ereignisses ändert.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Ereigniseinrichtung**.
2. Auf der Seite **Event Setup** können Sie Ereignisse deaktivieren oder aktivieren, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Ereignisse deaktivieren	a. Klicken Sie auf **Deaktivieren**. b. Im Dialogfeld „Ereignisse deaktivieren“ erfolgt die Auswahl des Schweregrads des Ereignisses. c. In der Spalte „Übereinstimmende Ereignisse“ sind die Ereignisse auszuwählen, die auf Grundlage des Schweregrads des Ereignisses deaktiviert werden sollen. Anschließend werden diese Ereignisse mit dem Pfeil nach rechts in die Spalte „Ereignisse deaktivieren“ verschoben. d. Anschließend erfolgt die Auswahl von **Save and Close**. e. Stellen Sie sicher, dass die deaktivierten Ereignisse in der Listenansicht der Seite „Ereigniseinrichtung“ angezeigt werden.
Ereignisse aktivieren	a. Für das oder die zu aktivierenden Ereignisse ist das Kästchen auszuwählen. b. Klicken Sie auf **Enable**.

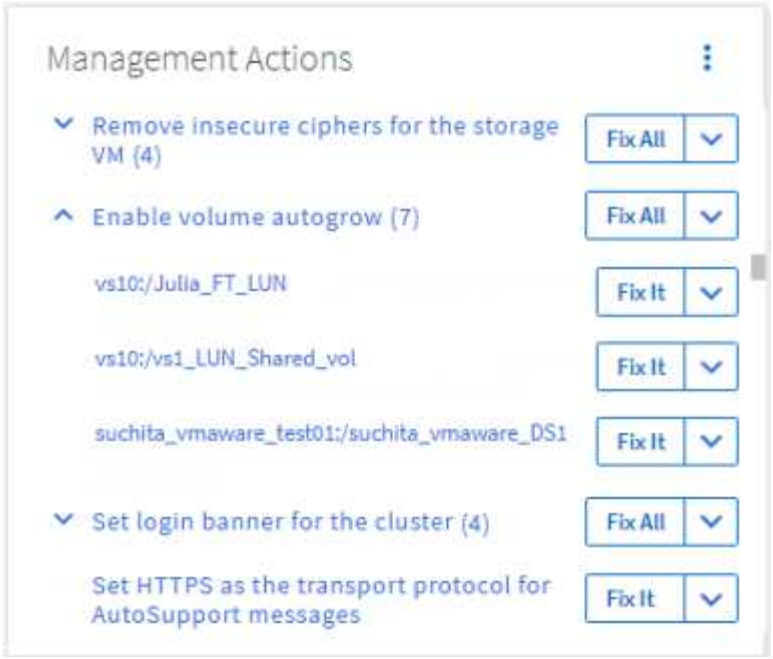
Probleme lassen sich mithilfe der automatischen Fehlerbehebung in Active IQ Unified Manager beheben

Es gibt bestimmte Ereignisse, die Unified Manager gründlich diagnostizieren und mithilfe der Schaltfläche **Fix It** eine einzelne Lösung bereitstellen kann. Falls verfügbar, werden diese Lösungen im Dashboard, auf der Seite mit den Ereignisdetails und über die Auswahl „Workload-Analyse“ im linken Navigationsmenü angezeigt.

Die meisten Ereignisse bieten verschiedene Lösungsmöglichkeiten, die auf der Seite „Ereignisdetails“ angezeigt werden, sodass Sie die beste Lösung mit ONTAP System Manager oder der ONTAP CLI implementieren können. Die Aktion **Fix It** ist verfügbar, wenn Unified Manager festgestellt hat, dass es nur eine Lösung zur Behebung des Problems gibt und dass diese mit einem ONTAP CLI-Befehl implementiert werden kann.

Schritte

1. Ereignisse, die über das **Dashboard** behoben werden können, lassen sich durch Klicken auf **Dashboard** anzeigen.



2. Zum Beheben von Problemen, die Unified Manager lösen kann, dient die Schaltfläche **Fix It**. Zum Beheben eines Problems, das auf mehreren Objekten vorhanden ist, dient die Schaltfläche **Fix All**.

Informationen zu den Problemen, die durch automatische Fehlerbehebung behoben werden können, sind unter "Welche Probleme kann Unified Manager beheben" zu finden.

Aktivieren und Deaktivieren der Active IQ Ereignisberichterstattung in Active IQ Unified Manager

Ereignisse der Active IQ Plattform werden standardmäßig in der Benutzeroberfläche des Unified Manager generiert und angezeigt. Falls diese Ereignisse als zu häufig empfunden werden oder sie in Unified Manager nicht angezeigt werden sollen, kann ihre Generierung deaktiviert werden. Sie können sie später wieder aktivieren, wenn Sie diese Benachrichtigungen erneut erhalten möchten.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Wenn Sie diese Funktion deaktivieren, empfängt Unified Manager sofort keine Ereignisse der Active IQ Plattform mehr.

Wenn Sie diese Funktion aktivieren, beginnt Unified Manager kurz nach Mitternacht, basierend auf der Zeitzone des Clusters, Active IQ Plattformereignisse zu empfangen. Der Startzeitpunkt richtet sich danach, wann Unified Manager AutoSupport Nachrichten von den einzelnen Clustern empfängt.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Funktionseinstellungen**.
2. Auf der Seite **Funktionseinstellungen** können Sie Active IQ Plattformereignisse deaktivieren oder aktivieren, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Active IQ Plattformereignisse deaktivieren	Im Bereich **Active IQ Portal Events** den Schieberegler nach links verschieben.
Aktivieren von Active IQ Plattformereignissen	Im Bereich **Active IQ Portal Events** wird der Schieberegler nach rechts verschoben.

Hochladen einer neuen Active IQ Regeldatei in Active IQ Unified Manager

Unified Manager sucht automatisch nach einer neuen Active IQ-Ereignisdatei (Regeln) und lädt eine neue Datei herunter, wenn neuere Regeln verfügbar sind. An Standorten ohne externen Netzwerkzugriff ist jedoch ein manuelles Hochladen der Regeldatei erforderlich.

Active IQ Regeln werden auch als Config Advisor (CA) Sicherheitsregeln bezeichnet.

Bei der Installation oder dem Upgrade von Unified Manager auf eine bestimmte Version an einem Standort ohne Netzwerkverbindung sind die mitgelieferten Active IQ-Regeln automatisch zum Upload verfügbar. Es wird jedoch empfohlen, etwa einmal im Monat eine neue Regeldatei von der Support Site von NetApp herunterzuladen, um sicherzustellen, dass aktualisierte Ereignisse generiert werden und Ihre Storage Systeme weiterhin optimal funktionieren.

Bevor Sie beginnen

- Die Ereignisberichterstattung im Active IQ portal muss aktiviert sein. Diese Funktion ist standardmäßig aktiviert. Informationen hierzu enthält "Aktivieren von Active IQ Portalereignissen".
- Sie müssen die Regeldatei von der NetApp Support Site herunterladen.

  Die Regeldatei befindet sich hier: https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

Schritte

1. Auf einem Computer mit Netzwerkzugriff können Sie die NetApp Support Site aufrufen und die aktuelle rules `.zip`-Datei herunterladen.

   Das mitgelieferte Regelpaket umfasst das Regel-Repository, Datenquellen und einen NetApp KB-Artikel.

   Auf Windows-Systemen an einem Standort ohne Netzwerkverbindung ist der NetApp KB-Artikel standardmäßig nicht im Installationsprogramm enthalten. Die Datei *secure_rules.zip* kann von der Support-Website heruntergeladen und hochgeladen werden, um den KB-Artikel für alle Regeln anzuzeigen.

2. Die Regeldatei wird auf ein Medium übertragen, das in den Sicherheitsbereich mitgenommen werden kann, und anschließend auf ein System im Sicherheitsbereich kopiert.
3. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Ereigniseinrichtung**.
4. Auf der Seite **Event Setup** ist auf die Schaltfläche **Upload Rules** zu klicken.
5. Im Dialogfeld **Upload Rules** können Sie zu der Regel `.zip`datei navigieren, die Sie heruntergeladen haben, sie auswählen und auf **Upload** klicken.

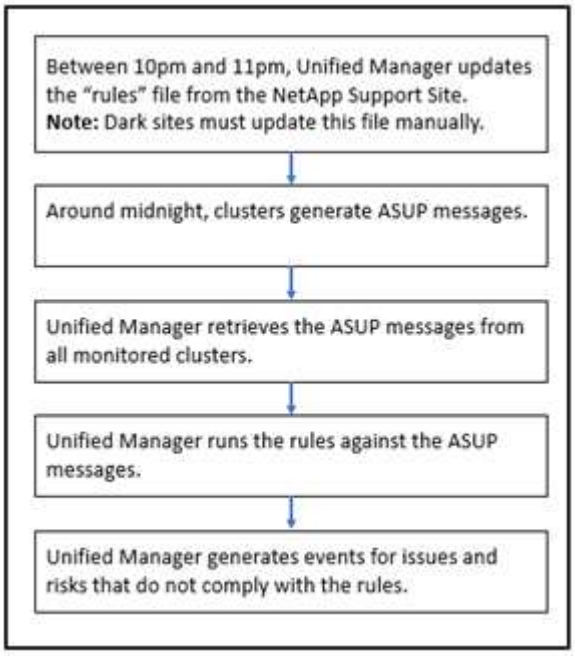
   Dieser Vorgang kann einige Minuten dauern.

Die Regeldatei wird auf dem Unified Manager Server entpackt. Nachdem Ihre verwalteten Cluster nach Mitternacht eine AutoSupport Datei generiert haben, prüft Unified Manager die Cluster anhand der Regeldatei und generiert bei Bedarf neue Risiko- und Incident-Ereignisse.

Weitere Informationen enthält dieser Knowledge Base (KB)-Artikel: "Manuelles Aktualisieren von AIQCASecure-Regeln in Active IQ Unified Manager".

Wie Active IQ Unified Manager Active IQ-Plattformereignisse generiert

Vorfälle und Risiken der Active IQ Plattform werden wie im folgenden Diagramm gezeigt in Unified Manager Ereignisse umgewandelt.

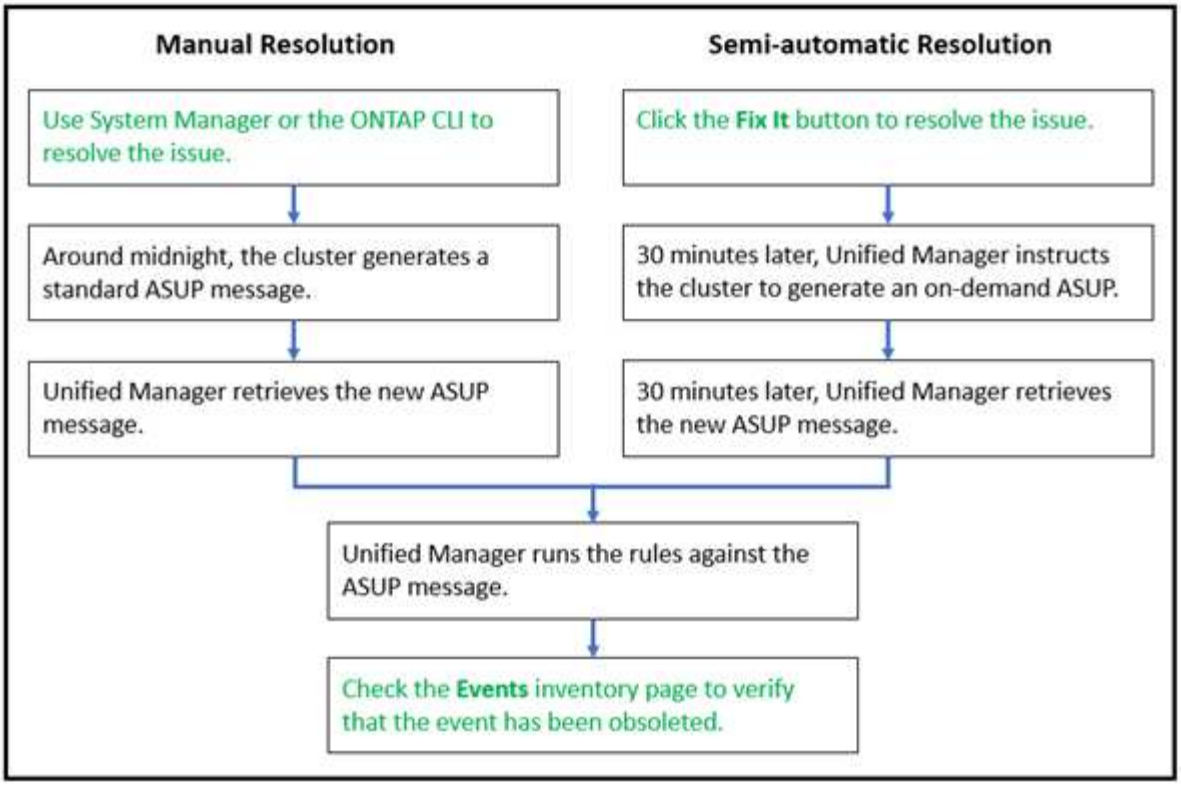


Wie Sie sehen können, wird die auf der Active IQ Plattform kompilierte Regeldatei stets aktuell gehalten, Cluster AutoSupport Meldungen werden täglich generiert, und Unified Manager aktualisiert die Liste der Ereignisse täglich.

Active IQ Plattformereignisse in Active IQ Unified Manager beheben

Vorfälle und Risiken der Active IQ Plattform ähneln anderen Unified Manager Ereignissen, da sie anderen Benutzern zur Behebung zugewiesen werden können und dieselben verfügbaren Status aufweisen. Wenn diese Ereignisse jedoch mit der Schaltfläche **Fix It** behoben werden, kann die Behebung innerhalb weniger Stunden überprüft werden.

Das folgende Diagramm zeigt die Maßnahmen, die Sie ergreifen müssen (grün), und die Maßnahmen, die Unified Manager ergreift (schwarz), wenn Ereignisse behoben werden, die von der Active IQ Plattform generiert wurden.



Bei einer manuellen Behebung müssen Sie sich bei System Manager oder der ONTAP Befehlszeilenschnittstelle anmelden, um das Problem zu beheben. Die Überprüfung des Problems ist erst möglich, nachdem der Cluster um Mitternacht eine neue AutoSupport Meldung generiert hat.

Bei einer halbautomatischen Behebung mithilfe der Schaltfläche **Fix It** können Sie innerhalb weniger Stunden überprüfen, ob die Behebung erfolgreich war.

Konfiguration der Einstellungen zur Ereignisaufbewahrung in Active IQ Unified Manager

Sie können die Anzahl der Monate festlegen, für die ein Ereignis auf dem Unified Manager Server aufbewahrt wird, bevor es automatisch gelöscht wird.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Das Speichern von Ereignissen über einen Zeitraum von mehr als 6 Monaten hinaus kann die Server Performance beeinträchtigen und wird daher nicht empfohlen.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **General** > **Data Retention**.
2. Auf der Seite **Datenaufbewahrung** den Schieberegler im Bereich Ereignisaufbewahrung auf die Anzahl der Monate einstellen, für die Ereignisse aufbewahrt werden sollen, und anschließend auf **Speichern** klicken.

Was ein Wartungsfenster für Unified Manager ist

Informationen zu den Wartungsfenstern von Active IQ Unified Manager

Sie definieren ein Unified Manager Wartungsfenster, um Ereignisse und Warnmeldungen für einen bestimmten Zeitraum zu unterdrücken, wenn Sie eine Clusterwartung geplant haben und keine Flut unerwünschter Benachrichtigungen erhalten möchten.

Wenn das Wartungsfenster beginnt, wird auf der Inventarseite von Event Management ein Ereignis mit dem Namen „Object Maintenance Window Started“ protokolliert. Dieses Ereignis wird automatisch als veraltet markiert, wenn das Wartungsfenster endet.

Während eines Wartungsfensters werden zwar weiterhin Ereignisse für alle Objekte in diesem Cluster generiert, sie werden jedoch auf keiner der UI Seiten angezeigt, und für diese Ereignisse werden keine Warnungen oder andere Arten von Benachrichtigungen gesendet. Die während eines Wartungsfensters für alle Storage Objekte generierten Ereignisse können jedoch angezeigt werden, indem auf der Bestandsseite „Ereignisverwaltung“ eine der Anzeigeoptionen ausgewählt wird.

Sie können ein Wartungsfenster so planen, dass es zu einem späteren Zeitpunkt gestartet wird, die Start- und Endzeiten für ein geplantes Wartungsfenster ändern und ein geplantes Wartungsfenster abbrechen.

Planen Sie ein Wartungsfenster, um Cluster-Ereignisbenachrichtigungen in Active IQ Unified Manager zu deaktivieren

Wenn Sie für einen Cluster eine geplante Ausfallzeit haben, beispielsweise für ein Cluster-Upgrade oder das Verschieben eines der Knoten, können Sie die Ereignisse und Warnungen, die normalerweise während dieses Zeitraums generiert würden, durch das Planen eines Wartungsfensters in Unified Manager unterdrücken.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Während eines Wartungsfensters werden zwar weiterhin Ereignisse generiert, die sich auf alle Objekte in diesem Cluster beziehen, sie werden jedoch nicht auf der Ereignisseite angezeigt, und für diese Ereignisse werden keine Warnungen oder andere Benachrichtigungen gesendet.

Die für das Wartungsfenster eingegebene Zeit basiert auf der Zeit auf dem Unified Manager Server.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. In der Spalte **Wartungsmodus** für den Cluster erfolgt die Auswahl der Schieberegler-Schaltfläche und das Verschieben nach rechts.

   Das Kalenderfenster wird angezeigt.

3. Das Start- und Enddatum sowie die Uhrzeit für das Wartungsfenster können festgelegt werden; anschließend ist **Apply** auszuwählen.

   Neben dem Schieberegler erscheint die Meldung „Geplant“.

Wenn der Startzeitpunkt erreicht ist, wechselt der Cluster in den Wartungsmodus und es wird ein Ereignis mit dem Titel „Object Maintenance Window Started“ generiert.

Ändern oder Stornieren eines geplanten Wartungsfensters in Active IQ Unified Manager

Wenn Sie ein Unified Manager Wartungsfenster konfiguriert haben, das in der Zukunft stattfinden soll, können Sie die Start- und Endzeiten ändern oder das Stattfinden des Wartungsfensters abbrechen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Das Abbrechen eines aktuell laufenden Wartungsfensters ist sinnvoll, wenn Sie die Clusterwartung vor dem geplanten Ende des Wartungsfensters abgeschlossen haben und wieder Ereignisse und Warnmeldungen vom Cluster empfangen möchten.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. In der Spalte **Wartungsmodus** für den Cluster:

Wenn Sie möchten…	Ausführung dieses Schritts…
Ändern des Zeitrahmens für ein geplantes Wartungsfenster	a. Neben dem Schieberegler befindet sich der Text „Geplant“. b. Start- und/oder Enddatum sowie -uhrzeit ändern und **Anwenden** auswählen.
Verlängerung der Dauer eines aktiven Wartungsfensters	a. Der Text „Active“ neben dem Schieberegler wird ausgewählt. b. Das Enddatum und die Endzeit werden geändert, und anschließend wird auf **Anwenden** geklickt.
Abbrechen eines geplanten Wartungsfensters	Der Schieberegler wird ausgewählt und nach links bewegt.
Abbrechen eines aktiven Wartungsfensters	Der Schieberegler wird ausgewählt und nach links bewegt.

Anzeigen von Ereignissen, die während eines Wartungsfensters in Active IQ Unified Manager generiert wurden

Bei Bedarf können Sie die Ereignisse anzeigen, die während eines Unified Manager Wartungsfensters für alle Storage-Objekte generiert wurden. Die meisten Ereignisse erscheinen nach Abschluss des Wartungsfensters und nachdem alle Systemressourcen wieder betriebsbereit sind im Status „Veraltet“.

Bevor Sie beginnen

Bevor Ereignisse verfügbar sind, muss mindestens ein Wartungsfenster abgeschlossen sein.

Ereignisse, die während eines Wartungsfensters aufgetreten sind, werden standardmäßig nicht auf der Inventarseite „Ereignisverwaltung“ angezeigt.

Schritte

1. Im linken Navigationsbereich ist **Ereignisse** zu wählen.

Standardmäßig werden alle aktiven (neuen und bestätigten) Ereignisse auf der Inventarseite Event Management angezeigt.

2. Im Ansichtsbereich kann die Option **Alle während der Wartung generierten Ereignisse** ausgewählt werden.

   Die Liste der Ereignisse, die in den letzten 7 Tagen während aller Wartungsfenstersitzungen und auf allen Clustern ausgelöst wurden, wird angezeigt.

3. Falls für einen einzelnen Cluster mehrere Wartungsfenster stattgefunden haben, können Sie auf das Kalendersymbol **Triggered Time** klicken und den Zeitraum für die Ereignisse des Wartungsfensters auswählen, die Sie anzeigen möchten.

Verwalten von Hostsystemressourcenereignissen in Active IQ Unified Manager

Unified Manager enthält einen Dienst, der Ressourcenprobleme auf dem Hostsystem überwacht, auf dem Unified Manager installiert ist. Probleme wie unzureichender Speicherplatz oder Arbeitsspeicher auf dem Hostsystem können Ereignisse der Managementstation auslösen, die als Bannermeldungen am oberen Rand der Benutzeroberfläche angezeigt werden.

Ereignisse der Managementstation weisen auf ein Problem mit dem Hostsystem hin, auf dem Unified Manager installiert ist. Beispiele für Probleme mit der Managementstation sind geringer Speicherplatz auf dem Hostsystem, ein fehlender regulärer Datenerfassungszyklus von Unified Manager sowie eine nicht oder verspätet abgeschlossene Statistikanalyse, weil die nächste Datenerfassungsabfrage gestartet wurde.

Im Gegensatz zu allen anderen Unified Manager Ereignismeldungen erscheinen diese speziellen Warnungs- und kritischen Ereignisse der Managementstation als Bannermeldungen.

Schritt

1. Zum Anzeigen von Ereignisinformationen der Managementstation sind folgende Schritte erforderlich:

Wenn Sie möchten…	Folgendes ist zu tun…
Details des Ereignisses anzeigen	Durch Klicken auf das Ereignisbanner wird die Seite mit den Ereignisdetails angezeigt, die Lösungsvorschläge für das Problem enthält.
Alle Ereignisse der Managementstation anzeigen	a. Im linken Navigationsbereich auf **Event Management** klicken. b. Im Filterbereich auf der Inventarseite „Ereignisverwaltung“ befindet sich in der Liste „Quelltyp“ das Kästchen für „Verwaltungsstation“.

Mehr über Ereignisse

Ereigniszustände in Active IQ Unified Manager

Der Status eines Ereignisses hilft Ihnen festzustellen, ob eine geeignete Korrekturmaßnahme erforderlich ist. Ein Ereignis kann neu, bestätigt, gelöst oder veraltet sein. Dabei gilt, dass sowohl neue als auch bestätigte Ereignisse als aktive Ereignisse

betrachtet werden.

Die Ereigniszustände sind wie folgt:

- **Neu**

  Der Status eines neuen Ereignisses.

- **Anerkannt**

  Der Zustand eines Ereignisses, wenn Sie es zur Kenntnis genommen haben.

- **Gelöst**

  Der Status eines Ereignisses, wenn es als behoben markiert ist.

- **Veraltet**

  Der Zustand eines Ereignisses, wenn es automatisch korrigiert wird oder wenn die Ursache des Ereignisses nicht mehr vorliegt.

  Ein veraltetes Ereignis kann weder bestätigt noch behoben werden.

Beispiel für verschiedene Zustände eines Ereignisses

Die folgenden Beispiele veranschaulichen die manuellen und automatischen Ereignisstatusänderungen.

Wenn das Ereignis „Cluster nicht erreichbar“ ausgelöst wird, ist der Ereignisstatus „Neu“. Wenn Sie das Ereignis bestätigen, ändert sich der Ereignisstatus zu „Bestätigt“. Nachdem Sie eine geeignete Korrekturmaßnahme ergriffen haben, müssen Sie das Ereignis als behoben markieren. Der Ereignisstatus ändert sich dann zu „Behoben“.

Wird das Ereignis „Cluster nicht erreichbar“ aufgrund eines Stromausfalls ausgelöst, nimmt der Cluster nach Wiederherstellung der Stromversorgung ohne Eingreifen eines Administrators den Betrieb wieder auf. Daher ist das Ereignis „Cluster nicht erreichbar“ nicht mehr gültig, und sein Status ändert sich im nächsten Überwachungszyklus zu „Veraltet“.

Unified Manager sendet eine Benachrichtigung, wenn sich ein Ereignis im Status „Veraltet“ oder „Gelöst“ befindet. Die E-Mail-Betreffzeile und der E-Mail-Inhalt einer Benachrichtigung enthalten Informationen über den Ereignisstatus. Ein SNMP-Trap enthält ebenfalls Informationen über den Ereignisstatus.

Informationen zu Ereignis-Schweregradtypen in Active IQ Unified Manager

Jedem Ereignis ist ein Typ des Schweregrads zugeordnet, der Sie bei der Priorisierung der Ereignisse unterstützt, die eine sofortige Korrekturmaßnahme erfordern.

- **Kritisch**

  Es ist ein Problem aufgetreten, das zu einer Serviceunterbrechung führen könnte, wenn nicht umgehend eine Korrekturmaßnahme ergriffen wird.

  Performance-kritische Ereignisse werden nur auf Grundlage benutzerdefinierter Schwellenwerte gesendet.

- **Fehler**

Die Ereignisquelle funktioniert weiterhin; jedoch ist eine Korrekturmaßnahme erforderlich, um eine Dienstunterbrechung zu vermeiden.

- **Warnung**

  Bei der Ereignisquelle ist ein Ereignis aufgetreten, dessen Sie sich bewusst sein sollten, oder ein Performance-Zähler für ein Clusterobjekt liegt außerhalb des normalen Bereichs und sollte überwacht werden, um sicherzustellen, dass er nicht den kritischen Schweregrad erreicht. Ereignisse dieses Schweregrads führen nicht zu einer Dienstunterbrechung, und sofortige Korrekturmaßnahmen sind möglicherweise nicht erforderlich.

  Performance-Warnereignisse werden von benutzerdefinierten, systemdefinierten oder dynamischen Schwellenwerten gesendet.

- **Informationen**

  Das Ereignis tritt auf, wenn ein neues Objekt erkannt oder eine Benutzeraktion ausgeführt wird. Wenn beispielsweise ein beliebiges Storage Objekt gelöscht wird oder Konfigurationsänderungen vorgenommen werden, wird ein Ereignis mit dem Typ des Schweregrads Information generiert.

  Informationsereignisse werden direkt von ONTAP gesendet, wenn eine Konfigurationsänderung erkannt wird.

Informationen zu den Auswirkungsstufen von Ereignissen in Active IQ Unified Manager

Jedem Ereignis ist ein Auswirkungslevel (Incident, Risiko, Ereignis oder Upgrade) zugeordnet, damit Sie die Ereignisse priorisieren können, die eine sofortige Korrekturmaßnahme erfordern.

- **Incident**

  Ein Incident ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster keine Daten mehr an den Client bereitstellt und nicht mehr genügend Speicherplatz zum Speichern von Daten verfügbar ist. Ereignisse mit einer Auswirkungsstufe vom Level Incident sind am schwerwiegendsten. Um eine Dienstunterbrechung zu vermeiden, sollten umgehend Korrekturmaßnahmen ergriffen werden.

- **Risiko**

  Ein Risiko ist eine Reihe von Ereignissen, die potenziell dazu führen können, dass ein Cluster keine Daten mehr an den Client bereitstellt und der Speicherplatz zum Speichern von Daten knapp wird. Ereignisse mit einer Auswirkungsstufe von Risiko können zu Dienstunterbrechungen führen. Gegebenenfalls sind Korrekturmaßnahmen erforderlich.

- **Ereignis**

  Ein Ereignis ist eine Zustands- oder Statusänderung von Storage Objekten und ihren Attributen. Ereignisse mit einem Auswirkungs-Level von Event dienen der Information und erfordern keine Korrekturmaßnahme.

- **Upgrade**

  Upgrade-Ereignisse sind eine spezielle Art von Ereignissen, die von der Active IQ-Plattform gemeldet werden. Diese Ereignisse kennzeichnen Probleme, deren Behebung ein Upgrade der ONTAP Software, der Node-Firmware oder der Betriebssystemsoftware (aufgrund von Sicherheitshinweisen) erfordert. Bei einigen dieser Probleme ist möglicherweise eine sofortige Korrekturmaßnahme erforderlich, während andere bis zur nächsten planmäßigen Wartung warten können.

Informationen zu Ereignisauswirkungsbereichen in Active IQ Unified Manager

Ereignisse sind in sechs Auswirkungsbereiche (Verfügbarkeit, Kapazität, Konfiguration, Performance, Schutz und Sicherheit) eingeteilt, sodass Sie sich auf die Arten von Ereignissen konzentrieren können, für die Sie verantwortlich sind.

- **Verfügbarkeit**

  Verfügbarkeitsereignisse benachrichtigen Sie, wenn ein Storage-Objekt offline geht, ein Protokolldienst ausfällt, ein Problem mit Storage Failover auftritt oder ein Hardwareproblem auftritt.

- **Kapazität**

  Kapazitätsereignisse benachrichtigen Sie, wenn Ihre Aggregate, Volumes, LUNs oder Namespaces sich einer Größenschwelle nähern oder diese erreicht haben, oder wenn die Wachstumsrate für Ihre Umgebung ungewöhnlich ist.

- **Konfiguration**

  Konfigurationsereignisse informieren Sie über die Erkennung, Löschung, Hinzufügung, Entfernung oder Umbenennung Ihrer Storage Objekte. Konfigurationsereignisse haben ein Auswirkungslevel von Event und den Typ des Schweregrads Information.

- **Leistung**

  Performance-Ereignisse informieren Sie über Ressourcen-, Konfigurations- oder Aktivitätsbedingungen in Ihrem Cluster, die sich negativ auf die Geschwindigkeit der Datenspeicherung oder des Datenabrufs bei Ihren überwachten Storage-Objekten auswirken könnten.

- **Schutz**

  Schutzereignisse benachrichtigen Sie über Incidents oder Risiken im Zusammenhang mit SnapMirror Beziehungen, Probleme mit der Zielkapazität, Probleme mit SnapVault Beziehungen oder Probleme mit Schutzaufträgen. Alle ONTAP Objekte, insbesondere Aggregate, Volumes und SVMs, die sekundäre Volumes und Schutzbeziehungen hosten, zählen zum Schutzauswirkungsbereich.

- **Sicherheit**

  Sicherheitsereignisse informieren Sie darüber, wie sicher Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes auf der Grundlage der in der "NetApp Security Hardening Guide für ONTAP 9" definierten Parameter sind.

  Zusätzlich umfasst dieser Bereich Upgrade-Ereignisse, die von der Active IQ Plattform gemeldet werden.

Wie Active IQ Unified Manager den Objektstatus berechnet

Der Objektstatus wird durch das schwerwiegendste Ereignis bestimmt, das aktuell den Status „Neu“ oder „Bestätigt“ aufweist. Wenn der Objektstatus beispielsweise „Fehler“ lautet, hat eines der Ereignisse des Objekts den Typ des Schweregrads „Fehler“. Sobald eine Korrekturmaßnahme ergriffen wurde, ändert sich der Ereignisstatus zu „Behoben“.

Informationen zu dynamischen Leistungsereignissen in Active IQ Unified Manager

Bei dynamischen Performance-Ereignissen werden im Abschnitt „Systemdiagnose“ auf der Seite mit den Ereignisdetails die wichtigsten Workloads mit der höchsten Latenz oder Auslastung der Clusterkomponente aufgelistet, um die ein Ressourcenkonflikt besteht.

Die Performance Statistiken basieren auf dem Zeitraum von der Erkennung des Performance-Ereignisses bis zur letzten Analyse des Ereignisses. Die Diagramme zeigen außerdem historische Performance Statistiken für die Clusterkomponente, um die ein Konflikt besteht.

Sie können beispielsweise Workloads mit hoher Auslastung einer Komponente identifizieren, um zu bestimmen, welcher Workload auf eine weniger ausgelastete Komponente verschoben werden sollte. Durch das Verschieben des Workloads würde sich die Arbeitslast auf der aktuellen Komponente verringern, wodurch die Komponente möglicherweise nicht mehr um Ressourcen konkurriert. Oben in diesem Abschnitt werden der Uhrzeit- und Datumsbereich angezeigt, in dem ein Ereignis erkannt und zuletzt analysiert wurde. Bei aktiven Ereignissen (neu oder bestätigt) wird der Zeitpunkt der letzten Analyse aktualisiert.

Die Diagramme zu Latenz und Aktivität zeigen die Namen der wichtigsten Workloads an, wenn Sie den Mauszeiger über das Diagramm bewegen. Über das Menü „Workload Type“ rechts neben dem Diagramm können Sie die Workloads nach ihrer Rolle im Ereignis sortieren, darunter „Haie“, „Angreifer“ oder „Opfer“, und Details zu ihrer Latenz sowie zu ihrer Auslastung auf der betroffenen Clusterkomponente anzeigen. Sie können den Istwert mit dem erwarteten Wert vergleichen, um zu erkennen, wann sich der Workload außerhalb seines erwarteten Latenz- oder Auslastungsbereichs befand. Informationen dazu enthält "Von Unified Manager überwachte Workload-Typen".

> Wenn Sie nach der maximalen Latenzabweichung sortieren, werden systemdefinierte Workloads nicht in der Tabelle angezeigt, da die Latenz nur für benutzerdefinierte Workloads gilt. Workloads mit sehr niedrigen Latenzwerten werden nicht in der Tabelle angezeigt.

Weitere Informationen zu den dynamischen Performance-Schwellenwerten finden Sie unter "Analyse von Ereignissen anhand dynamischer Performance-Schwellenwerte".

Informationen darüber, wie Unified Manager die Workloads einstuft und die Sortierreihenfolge bestimmt, finden Sie unter "Wie Unified Manager die Performance-Auswirkungen eines Ereignisses ermittelt".

Die Daten in den Diagrammen zeigen 24 Stunden Performance Statistiken vor dem letzten Zeitpunkt, zu dem das Ereignis analysiert wurde. Die tatsächlichen Werte und erwarteten Werte für jede Arbeitslast basieren auf dem Zeitpunkt, zu dem die Arbeitslast an dem Ereignis beteiligt war. Beispielsweise kann eine Arbeitslast erst nach der Erkennung des Ereignisses an einem Ereignis beteiligt sein, sodass ihre Performance Statistiken möglicherweise nicht mit den Werten zum Zeitpunkt der Ereigniserkennung übereinstimmen. Standardmäßig sind die Arbeitslasten nach der Spitzenabweichung (höchsten Abweichung) bei der Latenz sortiert.

> Da Unified Manager maximal 30 Tage an historischen Performance- und Ereignisdaten im 5-Minuten-Takt speichert, werden keine Performance-Daten angezeigt, wenn das Ereignis älter als 30 Tage ist.

- **Spalte „Arbeitslastsortierung“**
  - **Latenzdiagramm**

    Zeigt die Auswirkungen des Ereignisses auf die Latenz der Arbeitslast während der letzten Analyse an.
  - **Spalte „Komponentenverwendung“**

Zeigt Details zur Auslastung der Clusterkomponente im Konfliktfall an. In den Diagrammen stellt die blaue Linie die tatsächliche Auslastung dar. Ein roter Balken markiert die Ereignisdauer vom Zeitpunkt der Erkennung bis zum Zeitpunkt der letzten Analyse. Weitere Informationen sind unter "Messwerte zur Workload Performance" verfügbar.

Für die Netzwerkkomponente wird diese Spalte nicht angezeigt, da Performance Statistiken aus Aktivitäten außerhalb des Clusters stammen.

- **Komponentenverwendung**

  Zeigt den Nutzungsverlauf in Prozent für die Netzwerk-, Datenverarbeitungs- und Aggregatkomponenten bzw. den Aktivitätsverlauf in Prozent für die QoS-Richtliniengruppenkomponente an. Für die Netzwerk- und Interconnect-Komponenten wird kein Diagramm angezeigt. Durch Zeigen auf die Statistiken können die Nutzungsstatistiken zu einem bestimmten Zeitpunkt angezeigt werden.

- **Verlauf der gesamten Schreibvorgänge in MB/s**

  Nur für die Komponente „MetroCluster Resources“ wird der gesamte Schreibdurchsatz in Megabyte pro Sekunde (MBps) für alle Volume-Workloads angezeigt, die in einer MetroCluster Konfiguration auf den Partner-Cluster gespiegelt werden.

- **Ereignisverlauf**

  Zeigt rot schattierte Linien an, um die historischen Ereignisse der betroffenen Komponente darzustellen. Bei veralteten Ereignissen werden Ereignisse angezeigt, die vor der Erkennung des ausgewählten Ereignisses und nach dessen Behebung stattfanden.

Vom Active IQ Unified Manager erkannte Konfigurationsänderungen

Unified Manager überwacht Ihre Cluster auf Konfigurationsänderungen, um festzustellen, ob eine Änderung ein Performance Ereignis verursacht hat oder dazu beigetragen haben könnte. Die Seiten des Performance Explorer zeigen ein Änderungssymbol ( ) an, das das Datum und die Uhrzeit angibt, zu denen die Änderung erkannt wurde.

Auf den Seiten von Performance Explorer und auf der Seite Workload Analysis können die Performance-Diagramme geprüft werden, um festzustellen, ob sich das Änderungsereignis auf die Performance des ausgewählten Clusterobjekts ausgewirkt hat. Wenn die Änderung gleichzeitig oder ungefähr zur selben Zeit wie ein Performance-Ereignis erkannt wurde, hat sie möglicherweise zu dem Problem beigetragen, das die Ereigniswarnung ausgelöst hat.

Unified Manager kann die folgenden Änderungsereignisse erkennen, die als Informationsereignisse kategorisiert sind:

- Ein Volume bewegt sich zwischen Aggregaten.

  Unified Manager kann erkennen, ob eine Volume Verschiebung ausgeführt wird, abgeschlossen wurde oder fehlgeschlagen ist. Wenn Unified Manager während einer Volume Verschiebung nicht verfügbar ist, erkennt er die Volume Verschiebung nach der Wiederverfügbarkeit und zeigt ein entsprechendes Änderungsereignis an.

- Der Durchsatzgrenzwert (MB/s oder IOPS) einer QoS-Richtliniengruppe, die einen oder mehrere überwachte Workloads enthält, ändert sich.

  Die Änderung eines Grenzwerts einer Richtliniengruppe kann zu vorübergehenden Spitzen bei der Latenz

(Antwortzeit) führen, die wiederum Ereignisse für die Richtliniengruppe auslösen können. Die Latenz normalisiert sich allmählich wieder, und alle durch die Spitzen verursachten Ereignisse verlieren ihre Relevanz.

- Ein Knoten in einem HA-Paar übernimmt den Storage seines Partnerknotens oder gibt ihn zurück.

  Unified Manager kann erkennen, wann eine Übernahme, Teilübernahme oder Rückgabe abgeschlossen wurde. Wenn die Übernahme durch einen ausgefallenen Knoten verursacht wird, erkennt Unified Manager dieses Ereignis nicht.

- Ein ONTAP Upgrade oder ein Revert-Vorgang wird erfolgreich abgeschlossen.

  Die vorherige und die neue Version werden angezeigt.

Liste der Ereignisse und Schweregrade

Informationen zu Aggregatereignissen in Active IQ Unified Manager

Aggregatereignisse liefern Ihnen Informationen über den Status von Aggregaten, sodass Sie potenzielle Probleme überwachen können. Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse umgewandelt wurden.

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Aggregat Offline(ocumEvtAggregateStateOffline)	Vorfall	Aggregat	Kritisch
Aggregat fehlgeschlagen(ocumEvtAggregateStateFailed)	Vorfall	Aggregat	Kritisch
Aggregat eingeschränkt(ocumEvtAggregateStateRestricted)	Risiko	Aggregat	Warnung
Aggregatrekonstruktion(ocumEvtAggregateRaidStateReconstructing)	Risiko	Aggregat	Warnung
Aggregate beeinträchtigt(ocumEvtAggregateRaidStateDegraded)	Risiko	Aggregat	Warnung
Teilweise erreichbare Cloud-Ebene(ocumEventCloudTierPartiallyReachable)	Risiko	Aggregat	Warnung

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Cloud Tier nicht erreichbar(ocumEventCloudTierUnreachable)	Risiko	Aggregat	Fehler
Zugriff auf Cloud Tier für Aggregatverlagerung verweigert *(arlNetraCaCheckFailed)	Risiko	Aggregat	Fehler
Cloud Tier Zugriff für Aggregatverlagerung während Storage Failover verweigert *(gbNetraCaCheckFailed)	Risiko	Aggregat	Fehler
MetroCluster Zurückgelassenes Aggregat (ocumEvtMetroClusterAggregateLeftBehind)	Risiko	Aggregat	Fehler
MetroCluster Aggregate Mirroring beeinträchtigt(ocumEvtMetroClusterAggregateMirrorDegraded)	Risiko	Aggregat	Fehler

Wirkungsbereich: Kapazität

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Aggregatsspeicherplatz nahezu voll(ocumEvtAggregateNearlyFull)	Risiko	Aggregat	Warnung
Aggregat-Speicherplatz voll(ocumEvtAggregateFull)	Risiko	Aggregat	Fehler
Tage, bis das Aggregat voll ist(ocumEvtAggregateDaysUntilFullSoon)	Risiko	Aggregat	Fehler
Aggregate überbelegt(ocumEvtAggregateOvercommitted)	Risiko	Aggregat	Fehler
Aggregat nahezu überbucht(ocumEvtAggregateAlmostOvercommitted)	Risiko	Aggregat	Warnung

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Snapshot Reserve des Aggregats voll(ocumEvtAggregateSnapReserveFull)	Risiko	Aggregat	Warnung
Anomale Aggregatwachstumsrate(ocumEvtAggregateGrowthRateAbnormal)	Risiko	Aggregat	Warnung

Wirkungsbereich: Konfiguration

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Aggregat erkannt(nicht zutreffend)	Ereignis	Aggregat	Informationen
Aggregat umbenannt(Nicht zutreffend)	Ereignis	Aggregat	Informationen
Aggregat gelöscht(Nicht zutreffend)	Ereignis	Node	Informationen

Wirkungsbereich: Performance

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für Aggregat-IOPS überschritten(ocumAggregateIopsIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für Aggregat-IOPS überschritten(ocumAggregateIopsWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für Aggregat MB/s überschritten(ocumAggregateMbpsIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für Aggregat MB/s überschritten(ocumAggregateMbpsWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für die Aggregatlatenz überschritten(ocumAggregateLatencyIncident)	Vorfall	Aggregat	Kritisch

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Warnschwellenwert für die Aggregat-Latenz überschritten(ocumAggregateLatencyWarning)	Risiko	Aggregat	Warnung
Verwendete Aggregat Performance-Kapazität: Kritischer Schwellenwert überschritten(ocumAggregatePerfCapacityUsedIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für die genutzte Aggregat Performance-Kapazität überschritten(ocumAggregatePerfCapacityUsedWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für die Aggregat-Auslastung überschritten (ocumAggregateUtilizationIncident)	Vorfall	Aggregat	Kritisch
Warnschwellenwert für die Auslastung des Aggregats überschritten (ocumAggregateUtilizationWarning)	Risiko	Aggregat	Warnung
Schwellenwert für übermäßige Auslastung von Aggregat-Festplatten überschritten (ocumAggregateDisksOverUtilizedWarning)	Risiko	Aggregat	Warnung
Dynamischer Schwellenwert des Aggregats überschritten (ocumAggregateDynamicEventWarning)	Risiko	Aggregat	Warnung

Informationen zu Clusterereignissen in Active IQ Unified Manager

Clusterereignisse liefern Informationen über den Status von Clustern und ermöglichen so die Überwachung der Cluster auf potenzielle Probleme. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten Ereignisname, Trap-Name, Level, Quelltyp und Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse umgewandelt wurden.

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Cluster verfügt nicht über Ersatzfestplatten(ocumEvtDisksNoSpares)	Risiko	Cluster	Warnung
Cluster nicht erreichbar(ocumEvtClusterUnreachable)	Risiko	Cluster	Fehler
Clusterüberwachung fehlgeschlagen(ocumEvtClusterMonitoringFailed)	Risiko	Cluster	Warnung
Kapazitätsgrenzen der Cluster FabricPool Lizenz überschritten (ocumEvtExternalCapacityTierSpaceFull)	Risiko	Cluster	Warnung
NVMe-oF Kulanzfrist gestartet *(nvmfGracePeriodStart)	Risiko	Cluster	Warnung
NVMe-oF-Kulanzfrist aktiv *(nvmfGracePeriodActive)	Risiko	Cluster	Warnung
NVMe-oF Kulanzfrist abgelaufen *(nvmfGracePeriodExpired)	Risiko	Cluster	Warnung
Objektwartungsfenster gestartet(objectMaintenanceWindowStarted)	Ereignis	Cluster	Kritisch
Objektwartungsfenster beendet(objectMaintenanceWindowEnded)	Ereignis	Cluster	Informationen
MetroCluster Zurückgelassene Ersatzfestplatten(ocumEvtSpareDiskLeftBehind)	Risiko	Cluster	Fehler
MetroCluster Automatische ungeplante Umschaltung deaktiviert(ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Risiko	Cluster	Warnung
Passwort des Cluster-Benutzers geändert *(cluster.passwd.changed)	Ereignis	Cluster	Informationen

Wirkungsbereich: Kapazität

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Schwellenwert für das Ungleichgewicht der Clusterkapazität überschritten(ocumConformanceNodeImbalanceWarning)	Risiko	Cluster	Warnung
Planung der Cluster Cloud Tier (clusterCloudTierPlanningWarning)	Risiko	Cluster	Warnung
FabricPool Spiegelreplikations-Resynchronisierung abgeschlossen *(waflCaResyncComplete)	Ereignis	Cluster	Warnung
FabricPool Platz fast voll *(fabricpoolNearlyFull)	Risiko	Cluster	Fehler

Wirkungsbereich: Konfiguration

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Knoten hinzugefügt(Nicht zutreffend)	Ereignis	Cluster	Informationen
Knoten entfernt(Nicht zutreffend)	Ereignis	Cluster	Informationen
Cluster entfernt(Nicht zutreffend)	Ereignis	Cluster	Informationen
Cluster hinzufügen fehlgeschlagen(Nicht zutreffend)	Ereignis	Cluster	Fehler
Clustername geändert(Nicht zutreffend)	Ereignis	Cluster	Informationen
Notfall-EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Kritisch
Kritische EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Kritisch
Warnmeldung EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Fehler
EMS-Fehler empfangen (Nicht zutreffend)	Ereignis	Cluster	Warnung

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
EMS-Warnung empfangen (Nicht zutreffend)	Ereignis	Cluster	Warnung
Debug EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Warnung
EMS Benachrichtigung erhalten (Nicht zutreffend)	Ereignis	Cluster	Warnung
Informative EMS erhalten (Nicht zutreffend)	Ereignis	Cluster	Warnung

ONTAP EMS Ereignisse werden in drei Unified Manager Ereignisschweregrade kategorisiert.

Schweregrad-Level des Unified Manager Events	ONTAP EMS Level des Ereignis Schweregrads
Kritisch	Notfall Kritisch
Fehler	Alarm
Warnung	Fehler Warnung Debug Hinweis Informationen

Wirkungsbereich: Performance

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Schwellenwert für Cluster-Lastungleichgewicht überschritten()	Risiko	Cluster	Warnung
Kritischer Schwellenwert für Cluster IOPS überschritten(ocumClusterIopsIncident)	Vorfall	Cluster	Kritisch
Cluster-IOPS-Warnschwelle überschritten(ocumClusterIopsWarning)	Risiko	Cluster	Warnung
Kritischer Schwellenwert für Cluster MB/s überschritten(ocumClusterMbpsIncident)	Vorfall	Cluster	Kritisch

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Cluster MB/s Warnschwelle überschritten(ocumClusterMbpsWarning)	Risiko	Cluster	Warnung
Dynamischer Schwellenwert des Clusters überschritten(ocumClusterDynamicEventWarning)	Risiko	Cluster	Warnung

Wirkungsbereich: Sicherheit

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
AutoSupport HTTPS-Transport deaktiviert (ocumClusterASUPHttpsConfiguredDisabled)	Risiko	Cluster	Warnung
Protokollweiterleitung nicht verschlüsselt(ocumClusterAuditLogUnencrypted)	Risiko	Cluster	Warnung
Standardmäßig ist der lokale Administratorbenutzer aktiviert(ocumClusterDefaultAdminEnabled)	Risiko	Cluster	Warnung
FIPS-Modus deaktiviert(ocumClusterFipsDisabled)	Risiko	Cluster	Warnung
Anmeldebanner deaktiviert(ocumClusterLoginBannerDisabled)	Risiko	Cluster	Warnung
Anmeldebanner geändert(ocumClusterLoginBannerChanged)	Risiko	Cluster	Warnung
Protokollweiterleitungsziele geändert(ocumLogForwardDestinationsChanged)	Risiko	Cluster	Warnung
NTP-Servernamen geändert(ocumNtpServerNamesChanged)	Risiko	Cluster	Warnung

Ereignisname(Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Die Anzahl der NTP-Server ist niedrig(securityConfigNTPServerCountLowRisk)	Risiko	Cluster	Warnung
Cluster Peer-Kommunikation nicht verschlüsselt(ocumClusterPeerEncryptionDisabled)	Risiko	Cluster	Warnung
SSH verwendet unsichere Verschlüsselungsalgorithmen(ocumClusterSSHInsecure)	Risiko	Cluster	Warnung
Telnet-Protokoll aktiviert(ocumClusterTelnetEnabled)	Risiko	Cluster	Warnung
Die Passwörter einiger ONTAP Benutzerkonten verwenden die weniger sichere MD5-Hashfunktion(ocumClusterMD5PasswordHashUsed)	Risiko	Cluster	Warnung
Der Cluster verwendet ein selbstsigniertes Zertifikat(ocumClusterSelfSignedCertificate)	Risiko	Cluster	Warnung
Cluster Remote Shell ist aktiviert(ocumClusterRshDisabled)	Risiko	Cluster	Warnung
Das Cluster-Zertifikat läuft demnächst ab(ocumEvtClusterCertificateAboutToExpire)	Risiko	Cluster	Warnung
Clusterzertifikat abgelaufen(ocumEvtClusterCertificateExpired)	Risiko	Cluster	Fehler

Informationen zu Datenträgerereignissen in Active IQ Unified Manager

Datenträgerereignisse liefern Ihnen Informationen über den Status der Datenträger, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungs-Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Flash Disks - Reserveblöcke fast vollständig verbraucht(ocumEvtClusterFlashDiskFewerSpareBlockError)	Risiko	Cluster	Fehler
Flash Disks - Keine Ersatzblöcke(ocumEvtClusterFlashDiskNoSpareBlockCritical)	Vorfall	Cluster	Kritisch
Einige nicht zugewiesene Datenträger(ocumEvtClusterUnassignedDisksSome)	Risiko	Cluster	Warnung
Einige ausgefallene Festplatten(ocumEvtDisksSomeFailed)	Vorfall	Cluster	Kritisch

Informationen zu Gehäuseereignissen in Active IQ Unified Manager

Gehäuseereignisse liefern Ihnen Informationen über den Status von Disk Shelf Gehäusen in Ihrem Datacenter, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Lüfter des Disk Shelf ausgefallen(ocumEvtShelfFanFailed)	Vorfall	Storage Shelf	Kritisch
Netzteile des Disk Shelf ausgefallen(ocumEvtShelfPowerSupplyFailed)	Vorfall	Storage Shelf	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Disk Shelf Multipath nicht konfiguriert(ocumDiskShelfConnectivityNotInMultiPath) Dieses Ereignis gilt nicht für: • Cluster, die sich in einer MetroCluster Konfiguration befinden • Die folgenden Plattformen: FAS2554, FAS2552, FAS2520 und FAS2240	Risiko	Node	Warnung
Shelf-Pfadfehler(ocumDiskShelfConnectivityPathFailure)	Risiko	Storage-Shelf	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Disk Shelf entdeckt(nicht zutreffend)	Ereignis	Node	Informationen
Disk Shelves entfernt(Nicht zutreffend)	Ereignis	Node	Informationen

Informationen zu Lüfterereignissen in Active IQ Unified Manager

Lüfterereignisse liefern Ihnen Informationen zum Status der Lüfter auf den Knoten in Ihrem Datacenter, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Ein oder mehrere defekte Lüfter(ocumEvtFansOneOrMoreFailed)	Vorfall	Node	Kritisch

Informationen zu Flash-Karten-Ereignissen in Active IQ Unified Manager

Flash Kartenereignisse liefern Ihnen Informationen über den Status der auf Knoten in Ihrem Datacenter installierten Flash Karten, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Flash-Karten offline(ocumEvtFlashCardOffline)	Vorfall	Node	Kritisch

Informationen zu Inode-Ereignissen in Active IQ Unified Manager

Inode-Ereignisse liefern Informationen dazu, wann ein Inode voll oder nahezu voll ist, sodass eine Überwachung auf potenzielle Probleme möglich ist. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungs-Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Inodes fast voll(ocumEvtInodesAlmostFull)	Risiko	Volumen	Warnung
Inodes voll (ocumEvtInodesFull)	Risiko	Volumen	Fehler

Netzwerkschnittstellenereignisse in Active IQ Unified Manager

Ereignisse für Netzwerkschnittstellen liefern Informationen über den Status Ihrer Netzwerkschnittstellen (LIFs), sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Netzwerkschnittstellenstatus ausgefallen(ocumEvtLifStatusDown)	Risiko	Schnittstelle	Fehler

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
FC/FCoE Netzwerkschnittstellenstatus ausgefallen(ocumEvtFCLifStatusDown)	Risiko	Schnittstelle	Fehler
Failover der Netzwerkschnittstelle nicht möglich(ocumEvtLifFailoverNotPossible)	Risiko	Schnittstelle	Warnung
Netzwerkschnittstelle nicht am Home Port(ocumEvtLifNotAtHomePort)	Risiko	Schnittstelle	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Netzwerkschnittstellenroute nicht konfiguriert(nicht zutreffend)	Ereignis	Schnittstelle	Informationen

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für Netzwerkschnittstelle MB/s überschritten(ocumNetworkLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
Warnschwelle für Netzwerkschnittstelle MB/s überschritten(ocumNetworkLifMbpsWarning)	Risiko	Schnittstelle	Warnung
Kritischer Schwellenwert für die FC Netzwerkschnittstelle in MB/s überschritten(ocumFcpLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
FC Netzwerkschnittstelle MB/s Warnschwelle überschritten(ocumFcpLifMbpsWarning)	Risiko	Schnittstelle	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
NVMf FC Netzwerkschnittstelle MB/s Kritischer Schwellenwert überschritten(ocumNvmfFcLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
NVMf FC Netzwerkschnittstelle MB/s Warnschwelle überschritten(ocumNvmfFcLifMbpsWarning)	Risiko	Schnittstelle	Warnung

Informationen zu LUN-Ereignissen in Active IQ Unified Manager

LUN-Ereignisse liefern Ihnen Informationen über den Status Ihrer LUNs, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse umgewandelt wurden.

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
LUN offline (ocumEvtLunOffline)	Vorfall	LUN	Kritisch
LUN zerstört *(lunDestroy)	Ereignis	LUN	Informationen
LUN mit nicht unterstütztem Betriebssystem in Initiatorgruppe(igroupUnsupportedOsType)	Vorfall	LUN	Warnung
Einzelner aktiver Pfad zum Zugriff auf LUN(ocumEvtLunSingleActivePath)	Risiko	LUN	Warnung
Keine aktiven Pfade für den Zugriff auf LUN(ocumEvtLunNotReachable)	Vorfall	LUN	Kritisch
Keine optimierten Pfade für den Zugriff auf LUN(ocumEvtLunOptimizedPathInactive)	Risiko	LUN	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Keine Pfade für den Zugriff auf LUN vom HA Partner(ocumEvtLunHaPathInactive)	Risiko	LUN	Warnung
Kein Zugriffspfad auf die LUN von einem Knoten im HA-Paar(ocumEvtLunNodePathStatusDown)	Risiko	LUN	Fehler

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Unzureichender Speicherplatz für LUN-Snapshot-Kopie(ocumEvtLunSnapshotNotPossible)	Risiko	Volumen	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
LUN mit nicht unterstütztem Betriebssystem in Initiatorgruppe(igroupUnsupportedOsType)	Risiko	LUN	Warnung

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für LUN IOPS überschritten(ocumLunIopsIncident)	Vorfall	LUN	Kritisch
LUN IOPS Warnschwelle überschritten(ocumLunIopsWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN MB/s überschritten(ocumLunMbpsIncident)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
LUN MB/s Warnschwelle überschritten(ocumLunMbpsWarning)	Risiko	LUN	Warnung
LUN-Latenz ms/op Kritischer Schwellenwert überschritten(ocumLunLatencyIncident)	Vorfall	LUN	Kritisch
LUN-Latenz ms/op Warnschwelle überschritten(ocumLunLatencyWarning)	Risiko	LUN	Warnung
Kritische Schwellenwerte für LUN-Latenz und IOPS überschritten(ocumLunLatencyIopsIncident)	Vorfall	LUN	Kritisch
LUN-Latenz- und IOPS-Warnschwellenwert überschritten(ocumLunLatencyIopsWarning)	Risiko	LUN	Warnung
LUN-Latenz und kritischer MB/s-Schwellenwert überschritten(ocumLunLatencyMbpsIncident)	Vorfall	LUN	Kritisch
LUN Latenz und MB/s-Warnschwelle überschritten(ocumLunLatencyMbpsWarning)	Risiko	LUN	Warnung
LUN-Latenz und genutzte Aggregate Performance-Kapazität, kritischer Schwellenwert überschritten(ocumLunLatencyAggregatePerfCapacityUsedIncident)	Vorfall	LUN	Kritisch
Warnschwellenwert für LUN Latenz und verwendete Performance-Kapazität des Aggregats überschritten(ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und Aggregatauslastung überschritten(ocumLunLatencyAggregateUtilizationIncident)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Warnschwellenwert für LUN-Latenz und Aggregat-Auslastung überschritten(ocumLunLatencyAggregateUtilizationWarning)	Risiko	LUN	Warnung
LUN-Latenz und verwendete Knoten-Performance-Kapazität, kritischer Schwellenwert überschritten(ocumLunLatencyNodePerfCapacityUsedIncident)	Vorfall	LUN	Kritisch
LUN-Latenz und verwendete Knoten-Performance-Kapazität, Warnschwellenwert überschritten(ocumLunLatencyNodePerfCapacityUsedWarning)	Risiko	LUN	Warnung
Ausgelastete LUN-Latenz und Knotenleistungskapazität, kritischer Schwellenwert für die Übernahme überschritten (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Vorfall	LUN	Kritisch
Verwendete LUN-Latenz und Node Performance Capacity - Schwellenwert für die Takeover-Warnung überschritten(ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und Knotenauslastung überschritten(ocumLunLatencyNodeUtilizationIncident)	Vorfall	LUN	Kritisch
Schwellenwert für LUN-Latenz und Knotenauslastung überschritten(ocumLunLatencyNodeUtilizationWarning)	Risiko	LUN	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
QoS LUN Max IOPS Warnschwelle überschritten(ocumQosLunMaxIopsWarning)	Risiko	LUN	Warnung
QoS LUN Max MB/s Warnschwelle überschritten(ocumQosLunMaxMbpsWarning)	Risiko	LUN	Warnung
Schwellenwert für die Workload LUN Latenz gemäß der Performance Service Level Policy überschritten (ocumConformanceLatencyWarning)	Risiko	LUN	Warnung

Informationen zu Management Stationsereignissen in Active IQ Unified Manager

Die Ereignisse der Managementstation liefern Ihnen Informationen über den Status des Servers, auf dem Unified Manager installiert ist, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Speicherplatz auf dem Management Server fast voll(ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Risiko	Managementstation	Warnung
Speicherplatz auf dem Verwaltungsserver voll(ocumEvtUnifiedManagerDiskSpaceFull)	Vorfall	Managementstation	Kritisch
Management Server mit wenig Arbeitsspeicher(ocumEvtUnifiedManagerMemoryLow)	Risiko	Managementstation	Warnung
Management Server fast ohne freien Speicher(ocumEvtUnifiedManagerMemoryAlmostOut)	Vorfall	Managementstation	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Größe der MySQL-Protokolldatei erhöht; Neustart erforderlich(ocumEvtMysqlLogFileSizeWarning)	Vorfall	Managementstation	Warnung
Die insgesamt zugewiesene Größe des Audit-Protokolls ist fast ausgeschöpft.	Risiko	Managementstation	Warnung
Zertifikat des Syslog-Servers läuft demnächst ab	Risiko	Managementstation	Warnung
Zertifikat des Syslog Server abgelaufen	Risiko	Managementstation	Fehler
Überwachungsprotokolldatei manipuliert	Risiko	Managementstation	Warnung
Audit-Protokolldatei gelöscht	Risiko	Managementstation	Warnung
Verbindungsfehler beim Syslog-Server	Risiko	Managementstation	Fehler
Konfiguration des Syslog-Servers geändert	Ereignis	Managementstation	Warnung

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Die Analyse von Leistungsdaten ist beeinträchtigt(ocumEvtUnifiedManagerDataMissingAnalyze)	Risiko	Managementstation	Warnung
Die Erfassung von Leistungsdaten ist beeinträchtigt(ocumEvtUnifiedManagerDataMissingCollection)	Vorfall	Managementstation	Kritisch

Diese beiden letzten Performance-Ereignisse waren nur für Unified Manager 7.2 verfügbar. Wenn eines dieser Ereignisse den Status „Neu“ aufweist und Sie anschließend auf eine neuere Version der Unified Manager Software aktualisieren, werden die Ereignisse nicht automatisch gelöscht. Sie müssen die Ereignisse manuell in den Status „Gelöst“ verschieben.

Informationen zu MetroCluster Bridge Ereignissen in Active IQ Unified Manager

MetroCluster Bridge-Ereignisse liefern Informationen zum Status der Bridges, sodass Sie

potenzielle Probleme in einer MetroCluster over FC Konfiguration überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, den Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Brücke nicht erreichbar(ocumEvtBridgeUnreachable)	Vorfall	MetroCluster Brücke	Kritisch
Brückentemperatur abnormal(ocumEvtBridgeTemperatureAbnormal)	Vorfall	MetroCluster Brücke	Kritisch

Informationen zu MetroCluster Verbindungsereignissen in Active IQ Unified Manager

Konnektivitätsereignisse liefern Informationen über die Konnektivität zwischen den Komponenten eines Clusters sowie zwischen Clustern in MetroCluster over FC und MetroCluster over IP Konfigurationen, sodass potenzielle Probleme überwacht werden können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten Ereignis- und Trap-Name, Impact Level, Quelltyp und Schweregrad.

In beiden Konfigurationen gemeinsame Ereignisse

Diese Verbindungsereignisse sind sowohl für MetroCluster over FC als auch für MetroCluster over IP Konfigurationen üblich.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Alle Verbindungen zwischen MetroCluster Partnern unterbrochen(ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Vorfall	MetroCluster Beziehung	Kritisch
MetroCluster Partner über Peering-Netzwerk nicht erreichbar (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Vorfall	MetroCluster Beziehung	Kritisch
MetroCluster Disaster Recovery Fähigkeit beeinträchtigt (ocumEvtMetroClusterDRStatusImpacted)	Risiko	MetroCluster Beziehung	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
MetroCluster Konfiguration umgeschaltet (ocumEvtMetroClusterDRStatusImpacted)	Risiko	MetroCluster Beziehung	Warnung

MetroCluster über FC Konfiguration

Diese Ereignisse beziehen sich auf MetroCluster over FC Konfigurationen.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Alle Verbindungen zwischen den Switches ausgefallen(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Vorfall	MetroCluster Verbindung zwischen den Switches	Kritisch
Verbindung der FC-SAS Bridge zum Storage Stack unterbrochen(ocumEvtBridgeSasPortDown)	Vorfall	MetroCluster Bridge-Stack-Verbindung	Kritisch
MetroCluster Konfiguration teilweise umgeschaltet(ocumEvtMetroClusterDRStatusPartiallyImpacted)	Risiko	MetroCluster Beziehung	Fehler
Knoten zu FC Switch: Alle FC-VI-Verbindungslinks ausgefallen(ocumEvtMccNodeSwitchFcviLinksDown)	Vorfall	MetroCluster Node Switch Verbindung	Kritisch
Knoten zu FC Switch: Eine oder mehrere FC-Initiatorverbindungen unterbrochen(ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Risiko	MetroCluster Node Switch Verbindung	Warnung
Knoten zu FC Switch: Alle FC-Initiator-Verbindungen ausgefallen(ocumEvtMccNodeSwitchFcLinksDown)	Vorfall	MetroCluster Node Switch Verbindung	Kritisch
Switch zu FC-SAS-Brücke FC-Verbindung unterbrochen (ocumEvtMccSwitchBridgeFcLinksDown)	Vorfall	MetroCluster Switch Bridge Verbindung	Kritisch

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Inter Node Alle FC VI InterConnect Verbindungen ausgefallen (ocumEvtMccInterNodeLinksDown)	Vorfall	Verbindung zwischen den Knoten	Kritisch
Zwischen Knoten eine oder mehrere FC VI InterConnect Verbindungen ausgefallen (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risiko	Verbindung zwischen den Knoten	Warnung
Verbindung zwischen Knoten und Brücke unterbrochen (ocumEvtMccNodeBridgeLinksDown)	Vorfall	Node-Bridge-Verbindung	Kritisch
Knoten zu Storage Stack: Alle SAS Verbindungen ausgefallen (ocumEvtMccNodeStackLinksDown)	Vorfall	Node-Stack-Verbindung	Kritisch
Knoten zu Storage Stack: Ein oder mehrere SAS-Links ausgefallen (ocumEvtMccNodeStackLinksOneOrMoreDown)	Risiko	Node-Stack-Verbindung	Warnung

MetroCluster over IP Konfiguration

Diese Ereignisse beziehen sich auf MetroCluster over IP Konfigurationen.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
MetroCluster IP-Standort-zu-Standort-Konnektivitätsstatus ist unterbrochen (mccIntersiteconnectivityStatusDown)	Risiko	MetroCluster Beziehung	Kritisch
MetroCluster IP Knoten-zu-Switch-Verbindung offline (mccIpPortStatusOffline)	Risiko	Node	Fehler

Informationen zu MetroCluster Switch-Ereignissen in Active IQ Unified Manager

MetroCluster Switch-Ereignisse für MetroCluster over FC Konfigurationen bieten Informationen zum Status der MetroCluster Switches, um potenzielle Probleme zu überwachen. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten Ereignis- und Trap-Name, Impact Level, Quelltyp und Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Abnormale Switch-Temperatur(ocumEvtSwitchTemperatureAbnormal)	Vorfall	MetroCluster Switch	Kritisch
Switch nicht erreichbar(ocumEvtSwitchUnreachable)	Vorfall	MetroCluster Switch	Kritisch
Lüfter des Switches ausgefallen(ocumEvtSwitchFansOneOrMoreFailed)	Vorfall	MetroCluster Switch	Kritisch
Netzteile des Switches ausgefallen(ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Vorfall	MetroCluster Switch	Kritisch
Temperatursensoren des Switches ausgefallen(ocumEvtSwitchTemperatureSensorFailed) Dieses Ereignis gilt nur für Cisco Switches.	Vorfall	MetroCluster Switch	Kritisch

Informationen zu NVMe Namespace Ereignissen in Active IQ Unified Manager

NVMe Namespace Ereignisse liefern Ihnen Informationen über den Status Ihrer Namespaces, sodass potenzielle Probleme überwacht werden können. Die Ereignisse sind nach Wirkungsbereichen gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse umgewandelt wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
NVMeNS offline *(nvmeNamespaceStatusOffline)	Ereignis	Namensraum	Informationen
NVMeNS online *(nvmeNamespaceStatusOnline)	Ereignis	Namensraum	Informationen
NVMeNS Kein Speicherplatz mehr *(nvmeNamespaceSpaceOutOfSpace)	Risiko	Namensraum	Warnung
NVMeNS löschen *(nvmeNamespaceDestroy)	Ereignis	Namensraum	Informationen

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer IOPS-Schwellenwert für NVMe Namespace überschritten(ocumNvmeNamespaceIopsIncident)	Vorfall	Namensraum	Kritisch
NVMe Namespace IOPS Warnschwelle überschritten(ocumNvmeNamespaceIopsWarning)	Risiko	Namensraum	Warnung
NVMe Namespace MB/s Kritischer Schwellenwert überschritten(ocumNvmeNamespaceMbpsIncident)	Vorfall	Namensraum	Kritisch
NVMe Namespace MB/s Warnschwelle überschritten(ocumNvmeNamespaceMbpsWarning)	Risiko	Namensraum	Warnung
Kritischer Schwellenwert für NVMe Namespace Latenz in ms/op überschritten(ocumNvmeNamespaceLatencyIncident)	Vorfall	Namensraum	Kritisch
NVMe Namespace Latenz Warnschwelle in ms/op überschritten(ocumNvmeNamespaceLatencyWarning)	Risiko	Namensraum	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
NVMe Namespace Latenz und kritischer IOPS-Schwellenwert überschritten(ocumNvmeNamespaceLatencyIopsIncident)	Vorfall	Namensraum	Kritisch
NVMe Namespace Latenz- und IOPS-Warnschwelle überschritten(ocumNvmeNamespaceLatencyIopsWarning)	Risiko	Namensraum	Warnung
Latenz des NVMe Namespace und kritischer MB/s-Schwellenwert überschritten(ocumNvmeNamespaceLatencyMbpsIncident)	Vorfall	Namensraum	Kritisch
NVMe Namespace Latenz und MB/s-Warnschwelle überschritten(ocumNvmeNamespaceLatencyMbpsWarning)	Risiko	Namensraum	Warnung

Informationen zu Knotenereignissen in Active IQ Unified Manager

Knotenereignisse liefern Ihnen Informationen zum Knotenstatus, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, Level, den Quelltyp und Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse umgewandelt wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Speicherplatz des Node Root Volume nahezu voll(ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risiko	Node	Warnung
Cloud AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	Risiko	Node	Fehler

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Cloud AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	Risiko	Node	Fehler
Cloud AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	Risiko	Node	Fehler
Cloud AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	Risiko	Node	Fehler
Cloud AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	Ereignis	Node	Informationen
Cloud AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	Risiko	Node	Fehler
Cloud AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	Risiko	Node	Fehler
Cloud Tier Host nicht auflösbar *(ocumObjstoreHostUnresolvable)	Risiko	Node	Fehler
Cloud Tier Intercluster-Netzwerkschnittstelle ausgefallen *(ocumObjstoreInterClusterLifDown)	Risiko	Node	Fehler
Einer der NFSv4 Pools ist erschöpft *(nbladeNfsv4PoolEXhaust)	Vorfall	Node	Kritisch
Anfrage stimmt nicht mit der Cloud Tier Signatur überein *(oscSignatureMismatch)	Risiko	Node	Fehler

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
QoS Monitor Speicher voll ausgeschöpft *(ocumQosMonitorMemoryMaxed)	Risiko	Node	Fehler
QoS Monitor-Speicher reduziert *(ocumQosMonitorMemoryAbated)	Ereignis	Node	Informationen

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Knoten umbenannt(Nicht zutreffend)	Ereignis	Node	Informationen

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer IOPS-Schwellenwert des Knotens überschritten(ocumNodeIopsIncident)	Vorfall	Node	Kritisch
Knoten-IOPS-Warnschwelle überschritten(ocumNodeIopsWarning)	Risiko	Node	Warnung
Kritischer Schwellenwert für Knoten MB/s überschritten(ocumNodeMbpsIncident)	Vorfall	Node	Kritisch
Knoten-MB/s-Warnschwelle überschritten(ocumNodeMbpsWarning)	Risiko	Node	Warnung
Kritischer Schwellenwert für Knotenlatenz ms/op überschritten(ocumNodeLatencyIncident)	Vorfall	Node	Kritisch
Warnschwelle für Knotenlatenz ms/op überschritten(ocumNodeLatencyWarning)	Risiko	Node	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für die genutzte Knoten-Performance-Kapazität überschritten(ocumNodePerfCapacityUsedIncident)	Vorfall	Node	Kritisch
Warnschwelle für die genutzte Node-Performance-Kapazität überschritten(ocumNodePerfCapacityUsedWarning)	Risiko	Node	Warnung
Genutzte Knoten-Performance-Kapazität - kritischer Schwellenwert für Übernahme überschritten(ocumNodePerfCapacityUsedTakeoverIncident)	Vorfall	Node	Kritisch
Genutzte Knoten-Performancekapazität - Schwellenwert für die Übernahmewarnung überschritten(ocumNodePerfCapacityUsedTakeoverWarning)	Risiko	Node	Warnung
Kritischer Schwellenwert für die Knotenauslastung überschritten (ocumNodeUtilizationIncident)	Vorfall	Node	Kritisch
Schwellenwert für die Knotenauslastungswarnung überschritten (ocumNodeUtilizationWarning)	Risiko	Node	Warnung
Überlastungsschwelle des Knoten-HA-Paares überschritten (ocumNodeHaPairOverUtilizedInformation)	Ereignis	Node	Informationen
Schwellenwert für die Festplattenfragmentierung des Knotens überschritten (ocumNodeDiskFragmentationWarning)	Risiko	Node	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Schwellenwert für die genutzte Performance-Kapazität überschritten (ocumNodeOverUtilizedWarning)	Risiko	Node	Warnung
Dynamischer Schwellenwert des Knotens überschritten (ocumNodeDynamicEventWarning)	Risiko	Node	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Beratungs-ID: NTAP-<*advisory ID*>(ocumx)	Risiko	Node	Kritisch

Informationen zu NVRAM Batterieereignissen in Active IQ Unified Manager

NVRAM Batterieereignisse liefern Ihnen Informationen über den Status Ihrer Batterien, damit Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
NVRAM Batterie schwach(ocumEvtNvramBatteryLow)	Risiko	Node	Warnung
NVRAM Batterie entladen(ocumEvtNvramBatteryDischarged)	Risiko	Node	Fehler
NVRAM Batterie übermäßig geladen(ocumEvtNvramBatteryOverCharged)	Vorfall	Node	Kritisch

Informationen zu Portereignissen in Active IQ Unified Manager

Portereignisse liefern Ihnen Statusinformationen zu Cluster-Ports, sodass Sie Änderungen oder Probleme am Port überwachen können, z. B. ob der Port ausgefallen ist.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Port-Status nicht verfügbar(ocumEvtPortStatusDown)	Vorfall	Node	Kritisch

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für Netzwerkport MB/s überschritten(ocumNetworkPortMbpsIncident)	Vorfall	Port	Kritisch
Warnschwelle für Netzwerkport MB/s überschritten(ocumNetworkPortMbpsWarning)	Risiko	Port	Warnung
Kritischer Schwellenwert für FCP Port MB/s überschritten(ocumFcpPortMbpsIncident)	Vorfall	Port	Kritisch
FCP Port MB/s Warnschwelle überschritten(ocumFcpPortMbpsWarning)	Risiko	Port	Warnung
Kritischer Schwellenwert für die Netzwerkportauslastung überschritten(ocumNetworkPortUtilizationIncident)	Vorfall	Port	Kritisch
Warnschwellenwert für Netzwerkportauslastung überschritten(ocumNetworkPortUtilizationWarning)	Risiko	Port	Warnung
Kritischer Schwellenwert der FCP Port Auslastung überschritten(ocumFcpPortUtilizationIncident)	Vorfall	Port	Kritisch
Warnschwellenwert für FCP Port Auslastung überschritten(ocumFcpPortUtilizationWarning)	Risiko	Port	Warnung

Informationen zu Ereignissen im Zusammenhang mit der Stromversorgung in Active IQ Unified Manager

Ereignisse zu Netzteilen liefern Ihnen Informationen zum Status Ihrer Hardware, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Ein oder mehrere ausgefallene Netzteile(ocumEvtPowerSupplyOneOrMoreFailed)	Vorfall	Node	Kritisch

Informationen zu Schutzereignissen in Active IQ Unified Manager

Schutzereignisse zeigen, ob ein Auftrag fehlgeschlagen oder abgebrochen worden ist, sodass sich Probleme überwachen lassen. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Wirkungsbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Schutzaufgabe fehlgeschlagen(ocumEvtProtectionJobTaskFailed)	Vorfall	Volume oder Storage Service	Kritisch
Schutzauftrag abgebrochen(ocumEvtProtectionJobAborted)	Risiko	Volume oder Storage Service	Warnung

Informationen zu Qtree-Ereignissen in Active IQ Unified Manager

Qtree Ereignisse liefern Ihnen Informationen über die qtree Kapazität sowie über Datei- und Festplattenbeschränkungen, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Qtree-Speicher fast voll(ocumEvtQtreeSpaceNearlyFull)	Risiko	Qtree	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Qtree-Speicherplatz voll (ocumEvtQtreeSpaceFull)	Risiko	Qtree	Fehler
Qtree-Speicherplatz normal (ocumEvtQtreeSpaceThresholdOk)	Ereignis	Qtree	Informationen
Qtree-Dateien: Hartes Limit erreicht(ocumEvtQtreeFilesHardLimitReached)	Vorfall	Qtree	Kritisch
Soft Limit von Qtree Dateien überschritten(ocumEvtQtreeFilesSoftLimitBreached)	Risiko	Qtree	Warnung
Hartes Qtree Speicherplatzlimit erreicht(ocumEvtQtreeSpaceHardLimitReached)	Vorfall	Qtree	Kritisch
Softlimit für den Qtree-Speicherbereich überschritten(ocumEvtQtreeSpaceSoftLimitBreached)	Risiko	Qtree	Warnung

Informationen zu Service Processor Ereignissen in Active IQ Unified Manager

Serviceprozessorereignisse liefern Ihnen Informationen über den Status Ihres Prozessors, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungs-Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Dienstprozessor nicht konfiguriert(ocumEvtServiceProcessorNotConfigured)	Risiko	Node	Warnung
Dienstprozessor offline(ocumEvtServiceProcessorOffline)	Risiko	Node	Fehler

Informationen zu SnapMirror Beziehung Ereignissen in Active IQ Unified Manager

SnapMirror Beziehungsereignisse liefern Ihnen Informationen über den Status Ihrer asynchronen und synchronen SnapMirror Beziehungen, sodass Sie potenzielle Probleme überwachen können. Asynchrone SnapMirror Beziehungsereignisse werden sowohl für Storage VMs als auch für Volumes generiert, synchrone SnapMirror Beziehungsereignisse dagegen nur für Volume Beziehungen. Für einzelne Volumes, die Teil von Disaster-Recovery-Beziehungen von Storage VMs sind, werden keine Ereignisse generiert. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Schutz

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse umgewandelt wurden.

Die SnapMirror Beziehungsereignisse werden für Storage VMs generiert, die durch die Disaster Recovery von Storage VMs geschützt sind, jedoch nicht für Beziehungen zwischen einzelnen Objekten.

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Ungesunde Spiegelreplikation(ocumEvtSnapmirrorRelationshipUnhealthy)	Risiko	SnapMirror Beziehung	Warnung
Spiegelreplikation abgebrochen(ocumEvtSnapmirrorRelationshipStateBrokenoff)	Risiko	SnapMirror Beziehung	Fehler
Initialisierung der Spiegelreplikation fehlgeschlagen(ocumEvtSnapmirrorRelationshipInitializeFailed)	Risiko	SnapMirror Beziehung	Fehler
Aktualisierung der Spiegelreplikation fehlgeschlagen(ocumEvtSnapmirrorRelationshipUpdateFailed)	Risiko	SnapMirror Beziehung	Fehler
Fehler bei der Spiegelreplikationsverzögerung(ocumEvtSnapMirrorRelationshipLagError)	Risiko	SnapMirror Beziehung	Fehler
Warnung vor Verzögerungen bei der Spiegelreplikation(ocumEvtSnapMirrorRelationshipLagWarning)	Risiko	SnapMirror Beziehung	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Resynchronisierung der Spiegelreplikation fehlgeschlagen(ocumEvtSnapmirrorRelationshipResyncFailed)	Risiko	SnapMirror Beziehung	Fehler
Synchrone Replikation nicht synchron *(syncSnapmirrorRelationshipOutofsync)	Risiko	SnapMirror Beziehung	Warnung
Synchrone Replikation wiederhergestellt *(syncSnapmirrorRelationshipInSync)	Ereignis	SnapMirror Beziehung	Informationen
Automatische Resynchronisierung der synchronen Replikation fehlgeschlagen *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Risiko	SnapMirror Beziehung	Fehler
Ontap Mediator wurde dem Cluster hinzugefügt (snapmirrorMediatorAdded)	Ereignis	Cluster	Informationen
Ontap Mediator wird aus dem Cluster entfernt (snapmirrorMediatorRemoved)	Ereignis	Cluster	Informationen
Ontap Mediator ist vom Cluster aus nicht erreichbar (snapmirrorMediatorUnreachable)	Risiko	Mediator	Warnung
Ontap Mediator ist vom Cluster aus nicht erreichbar (snapmirrorMediatorMisconfigured)	Risiko	Mediator	Fehler
Die Ontap Mediator Connectivity wurde wiederhergestellt, ist erneut synchronisiert und bereit für die aktive SnapMirror Synchronisierung (snapmirrorMediatorInQuorum)	Ereignis	Mediator	Informationen

Informationen zu Ereignissen der asynchronen Spiegelung und der Vault Beziehung in Active IQ Unified Manager

Ereignisse für Asynchronous Mirror- und Vault-Beziehungen liefern Ihnen Informationen über den Status Ihrer Asynchronous SnapMirror- und Vault-Beziehungen, sodass Sie potenzielle Probleme überwachen können. Ereignisse für Asynchronous Mirror- und Vault-Beziehungen werden sowohl für Volume- als auch für Storage VM-Schutzbeziehungen unterstützt. Nur Vault-Beziehungen werden für die Storage VM-Notfallwiederherstellung nicht unterstützt. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten Ereignis- und Trap-Name, Auswirkungsstufe, Quelltyp und Schweregrad.

Wirkungsbereich: Schutz

Die Ereignisse für SnapMirror und Vault Beziehungen werden auch für Storage VMs generiert, die durch Storage VM Disaster Recovery geschützt sind, jedoch nicht für Beziehungen zwischen Teilobjekten.

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Asynchrone Spiegelung und Vault fehlerhaft(ocumEvtMirrorVaultRelationshipUnhealthy)	Risiko	SnapMirror Beziehung	Warnung
Asynchroner Mirror und Vault abgebrochen(ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risiko	SnapMirror Beziehung	Fehler
Asynchrone Spiegelung und Vault Initialisierung fehlgeschlagen(ocumEvtMirrorVaultRelationshipInitializeFailed)	Risiko	SnapMirror Beziehung	Fehler
Asynchrone Mirror- und Vault-Aktualisierung fehlgeschlagen(ocumEvtMirrorVaultRelationshipUpdateFailed)	Risiko	SnapMirror Beziehung	Fehler
Asynchroner Spiegelungs- und Vault Verzögerungsfehler(ocumEvtMirrorVaultRelationshipLagError)	Risiko	SnapMirror Beziehung	Fehler

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Warnung vor Verzögerungen bei asynchronem Spiegeln und Vault (ocumEvtMirrorVaultRelationshipLagWarning)	Risiko	SnapMirror Beziehung	Warnung
Asynchrone Spiegelung und Vault-Resynchronisierung fehlgeschlagen(ocumEvtMirrorVaultRelationshipResyncFailed)	Risiko	SnapMirror Beziehung	Fehler

Das Ereignis "SnapMirror update failure" wird vom Active IQ Portal (Config Advisor) ausgelöst.

Informationen zu Snapshot-Ereignissen in Active IQ Unified Manager

Snapshot-Ereignisse liefern Informationen zum Status von Snapshots und ermöglichen so die Überwachung der Snapshots auf potenzielle Probleme. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten Ereignisname, Trap-Name, Impact Level, Quelltyp und Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Automatische Snapshot-Löschung deaktiviert(Nicht zutreffend)	Ereignis	Volumen	Informationen
Automatische Snapshot Löschung aktiviert(Nicht zutreffend)	Ereignis	Volumen	Informationen
Snapshot Auto-delete-Konfiguration geändert(Nicht zutreffend)	Ereignis	Volumen	Informationen

Informationen zu SnapVault Beziehung Ereignissen in Active IQ Unified Manager

SnapVault Beziehungsereignisse liefern Ihnen Informationen über den Status Ihrer SnapVault Beziehungen, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Asynchroner Vault-Fehler(ocumEvtSnapVaultRelationshipUnhealthy)	Risiko	SnapMirror Beziehung	Warnung
Asynchrones Vault unterbrochen(ocumEvtSnapVaultRelationshipStateBrokenoff)	Risiko	SnapMirror Beziehung	Fehler
Asynchrone Vault-Initialisierung fehlgeschlagen(ocumEvtSnapVaultRelationshipInitializeFailed)	Risiko	SnapMirror Beziehung	Fehler
Asynchrone Vault Aktualisierung fehlgeschlagen(ocumEvtSnapVaultRelationshipUpdateFailed)	Risiko	SnapMirror Beziehung	Fehler
Asynchroner Vault-Verzögerungsfehler(ocumEvtSnapVaultRelationshipLagError)	Risiko	SnapMirror Beziehung	Fehler
Warnung vor asynchroner Vault-Verzögerung(ocumEvtSnapVaultRelationshipLagWarning)	Risiko	SnapMirror Beziehung	Warnung
Asynchrone Vault Resynchronisierung fehlgeschlagen(ocumEvtSnapvaultRelationshipResyncFailed)	Risiko	SnapMirror Beziehung	Fehler

Informationen zu Ereignissen bei Storage-Failover-Einstellungen in Active IQ Unified Manager

Ereignisse zu den Storage Failover Einstellungen (SFO) liefern Ihnen Informationen darüber, ob Ihr Storage Failover deaktiviert oder nicht konfiguriert ist, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und umfassen den Ereignis- und Trap-Namen, das Auswirkungs-Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Storage Failover Interconnect: Eine oder mehrere Verbindungen ausgefallen(ocumEvtSfoInterconnectOneOrMoreLinksDown)	Risiko	Node	Warnung
Storage Failover deaktiviert(ocumEvtSfoSettingsDisabled)	Risiko	Node	Fehler
Storage Failover nicht konfiguriert(ocumEvtSfoSettingsNotConfigured)	Risiko	Node	Fehler
Storage Failover Status - Übernahme(ocumEvtSfoStateTakeover)	Risiko	Node	Warnung
Storage Failover Status - Teilweise Rückgabe(ocumEvtSfoStatePartialGiveback)	Risiko	Node	Fehler
Storage Failover Node-Status ausgefallen(ocumEvtSfoNodeStatusDown)	Risiko	Node	Fehler
Storage Failover Übernahme nicht möglich(ocumEvtSfoTakeoverNotPossible)	Risiko	Node	Fehler

Informationen zu Speicherdienstereignissen in Active IQ Unified Manager

Storage Services Ereignisse liefern Ihnen Informationen zur Erstellung und zum Abonnement von Storage Services, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungs-Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Storage Service erstellt(Nicht zutreffend)	Ereignis	Speicherservice	Informationen
Storage Service abonniert(nicht zutreffend)	Ereignis	Speicherservice	Informationen
Storage Service abgemeldet(Nicht zutreffend)	Ereignis	Speicherservice	Informationen

Wirkungsbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Unerwartete Löschung der verwalteten SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion	Risiko	Speicherservice	Warnung
Unerwartete Löschung eines Speicherdienstmitglieds-Volumes(ocumEvtStorageServiceUnexpectedVolumeDeletion)	Vorfall	Speicherservice	Kritisch

Informationen zu Storage Shelf Ereignissen in Active IQ Unified Manager

Storage Shelf Ereignisse zeigen an, ob Ihr Storage Shelf Anomalien aufweist, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Abnormaler Spannungsbereich(ocumEvtShelfVoltageAbnormal)	Risiko	Storage Shelf	Warnung
Abnormaler Strombereich(ocumEvtShelfCurrentAbnormal)	Risiko	Storage Shelf	Warnung
Abnormale Temperatur(ocumEvtShelfTemperatureAbnormal)	Risiko	Storage Shelf	Warnung

Informationen zu Storage VM Ereignissen in Active IQ Unified Manager

Ereignisse für Storage VM (storage virtual machine, auch als SVM bezeichnet) liefern Ihnen Informationen zum Status Ihrer Storage VMs (SVMs), sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel, den Quelltyp und den Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse umgewandelt wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Storage VM CIFS-Service ausgefallen(ocumEvtVserverCifsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM CIFS Service nicht konfiguriert (Nicht zutreffend)	Ereignis	SVM	Informationen
Versuche, eine nicht vorhandene CIFS-Freigabe zu verbinden *(nbladeCifsNoPrivShare)	Vorfall	SVM	Kritisch
CIFS NetBIOS Namenskonflikt *(nbladeCifsNbNameConflict)	Risiko	SVM	Fehler
CIFS Shadow Copy Vorgang fehlgeschlagen *(cifsShadowCopyFailure)	Risiko	SVM	Fehler
Viele CIFS-Verbindungen *(nbladeCifsManyAuths)	Risiko	SVM	Fehler
Maximale Anzahl CIFS-Verbindungen überschritten *(nbladeCifsMaxOpenSameFile)	Risiko	SVM	Fehler
Maximale Anzahl der CIFS-Verbindungen pro Benutzer überschritten *(nbladeCifsMaxSessPerUsrConn)	Risiko	SVM	Fehler
SVM FC/FCoE-Service ausgefallen(ocumEvtVserverFcServiceStatusDown)	Vorfall	SVM	Kritisch
SVM iSCSI Service ausgefallen(ocumEvtVserverIscsiServiceStatusDown)	Vorfall	SVM	Kritisch
NFS-Service der Storage VM ausgefallen(ocumEvtVserverNfsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM FC/FCoE-Service nicht konfiguriert(Nicht zutreffend)	Ereignis	SVM	Informationen

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
SVM iSCSI Service nicht konfiguriert(Nicht zutreffend)	Ereignis	SVM	Informationen
SVM NFS-Dienst nicht konfiguriert(Nicht zutreffend)	Ereignis	SVM	Informationen
Storage VM gestoppt(ocumEvtVserverDown)	Risiko	SVM	Warnung
AV Server ist zu ausgelastet, um neue Scan-Anfragen anzunehmen *(nbladeVscanConnBackPressure)	Risiko	SVM	Fehler
Keine AV-Server-Verbindung für Virenscan *(nbladeVscanNoScannerConn)	Vorfall	SVM	Kritisch
Kein AV-Server registriert *(nbladeVscanNoRegdScanner)	Risiko	SVM	Fehler
Keine reagierende AV-Serververbindung *(nbladeVscanConnInactive)	Ereignis	SVM	Informationen
Unbefugter Benutzerzugriffsversuch auf den AV-Server *(nbladeVscanBadUserPrivAccess)	Risiko	SVM	Fehler
Virus vom AV-Server gefunden *(nbladeVscanVirusDetected)	Risiko	SVM	Fehler

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
SVM gefunden(Nicht zutreffend)	Ereignis	SVM	Informationen
SVM gelöscht(Nicht zutreffend)	Ereignis	Cluster	Informationen
SVM umbenannt(Nicht zutreffend)	Ereignis	SVM	Informationen

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für SVM IOPS überschritten(ocumSvmIopsIncident)	Vorfall	SVM	Kritisch
SVM IOPS-Warnschwelle überschritten(ocumSvmIopsWarning)	Risiko	SVM	Warnung
SVM MB/s Kritischer Schwellenwert überschritten(ocumSvmMbpsIncident)	Vorfall	SVM	Kritisch
SVM MB/s Warnschwelle überschritten(ocumSvmMbpsWarning)	Risiko	SVM	Warnung
Kritischer Schwellenwert für SVM-Latenz überschritten(ocumSvmLatencyIncident)	Vorfall	SVM	Kritisch
SVM Latenzwarnungsschwelle überschritten(ocumSvmLatencyWarning)	Risiko	SVM	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Audit-Protokoll deaktiviert(ocumVserverAuditLogDisabled)	Risiko	SVM	Warnung
Anmeldebanner deaktiviert(ocumVserverLoginBannerDisabled)	Risiko	SVM	Warnung
SSH verwendet unsichere Cipher(ocumVserverSSHInsecure)	Risiko	SVM	Warnung
Anmeldebanner geändert(ocumVserverLoginBannerChanged)	Risiko	SVM	Warnung
Die Anti-Ransomware-Überwachung der Storage VM ist deaktiviert (antiRansomwareSvmStateDisabled)	Risiko	SVM	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Die Überwachung von Storage VMs mit Anti-Ransomware ist aktiviert (Lernmodus) (antiRansomwareSvmStateDryrun)	Ereignis	SVM	Informationen
Storage VM geeignet für die Überwachung von Anti-Ransomware (Lernmodus) (ocumEvtSvmArwCandidate)	Ereignis	SVM	Informationen

Informationen zu Benutzer- und Gruppenkontingentereignissen in Active IQ Unified Manager

Ereignisse zu Benutzer- und Gruppenkontingenten liefern Ihnen Informationen über die Kapazität der Benutzer- und Gruppenkontingente sowie über Datei- und Festplattenlimits, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, das Impact Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Benutzer- oder Gruppenkontingent: Soft-Limit für Speicherplatz überschritten(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risiko	Benutzer- oder Gruppenkontingent	Warnung
Hartes Speicherplatzlimit für Benutzer- oder Gruppenkontingente erreicht(ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingent	Kritisch
Soft-Limit für die Dateianzahl des Benutzer- oder Gruppenkontingents überschritten(ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Risiko	Benutzer- oder Gruppenkontingent	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Hartes Limit der Dateianzahl für Benutzer- oder Gruppenkontingent erreicht(ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingent	Kritisch

Informationen zu Volume-Ereignissen in Active IQ Unified Manager

Volume-Ereignisse liefern Informationen über den Status von Volumes und ermöglichen so die Überwachung potenzieller Probleme. Die Ereignisse sind nach Wirkungsbereich gruppiert und enthalten Ereignisname, Trap-Name, Level, Quelltyp und Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse umgewandelt wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Volume beschränkt(ocumEvtVolumeRestricted)	Risiko	Volumen	Warnung
Volume offline (ocumEvtVolumeOffline)	Vorfall	Volumen	Kritisch
Volume teilweise verfügbar(ocumEvtVolumePartiallyAvailable)	Risiko	Volumen	Fehler
Volume nicht eingehängt(nicht zutreffend)	Ereignis	Volumen	Informationen
Volume gemountet (nicht zutreffend)	Ereignis	Volumen	Informationen
Volume erneut eingehängt(Nicht zutreffend)	Ereignis	Volumen	Informationen
Volumenverbindungspfad inaktiv(ocumEvtVolumeJunctionPathInactive)	Risiko	Volumen	Warnung
Automatische Volumengrößenanpassung aktiviert(Nicht zutreffend)	Ereignis	Volumen	Informationen
Volume Autosize deaktiviert (nicht zutreffend)	Ereignis	Volumen	Informationen

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Maximale Kapazität der automatischen Volume Größenanpassung geändert(Nicht zutreffend)	Ereignis	Volumen	Informationen
Inkrementgröße für Volume Autosize geändert(Nicht zutreffend)	Ereignis	Volumen	Informationen

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Gefährdeter Speicherplatz eines Thin-Provisioned Volume(ocumThinProvisionVolumeSpaceAtRisk)	Risiko	Volumen	Warnung
Fehler bei der Volumeneffizienzoperation(ocumEvtVolumeEfficiencyOperationError)	Risiko	Volumen	Fehler
Volume-Speicher voll(ocumEvtVolumeFull)	Risiko	Volumen	Fehler
Volume Speicherplatz nahezu voll(ocumEvtVolumeNearlyFull)	Risiko	Volumen	Warnung
Logischer Speicherplatz des Volume voll *(volumeLogicalSpaceFull)	Risiko	Volumen	Fehler
Logischer Speicherplatz des Volume nahezu voll *(volumeLogicalSpaceNearlyFull)	Risiko	Volumen	Warnung
Logischer Volume-Speicherplatz normal *(volumeLogicalSpaceAllOK)	Ereignis	Volumen	Informationen
Volume Snapshot Reserve-Speicherplatz voll (ocumEvtSnapshotFull)	Risiko	Volumen	Warnung
Zu viele Snapshot-Kopien(ocumEvtSnapshotTooMany)	Risiko	Volumen	Fehler

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Volume-Qtree-Quota überzeichnet (ocumEvtVolumeQtreeQuotaOvercommitted)	Risiko	Volumen	Fehler
Volume Qtree Quota fast überbelegt(ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Risiko	Volumen	Warnung
Anomale Wachstumsrate des Volumens(ocumEvtVolumeGrowthRateAbnormal)	Risiko	Volumen	Warnung
Volume Tage bis voll(ocumEvtVolumeDaysUntilFullSoon)	Risiko	Volumen	Fehler
Volume Speicherplatzgarantie deaktiviert(nicht anwendbar)	Ereignis	Volumen	Informationen
Speicherplatzgarantie für Volumes aktiviert(nicht zutreffend)	Ereignis	Volumen	Informationen
Volume Space Guarantee geändert(nicht zutreffend)	Ereignis	Volumen	Informationen
Tage bis zur vollständigen Füllung der Volume Snapshot Reserve(ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risiko	Volumen	Fehler
FlexGroup Bestandteile haben Platzprobleme *(flexGroupConstituentsHaveSpaceIssues)	Risiko	Volumen	Fehler
FlexGroup Status des Speicherplatzes aller Bestandteile OK *(flexGroupConstituentsSpaceStatusAllOK)	Ereignis	Volumen	Informationen
FlexGroup Konstituenten haben Inode-Probleme *(flexGroupConstituentsHaveInodesIssues)	Risiko	Volumen	Fehler

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
FlexGroup Konstituenten Inodes Status Alle OK *(flexGroupConstituentsInodesStatusAllOK)	Ereignis	Volumen	Informationen
WAFL Volume AutoSize Fehler *(waflVolAutoSizeFail)	Risiko	Volumen	Fehler
WAFL Volume AutoSize abgeschlossen *(waflVolAutoSizeDone)	Ereignis	Volumen	Informationen
FlexGroup Volume ist zu über 80 % ausgelastet*	Vorfall	Volumen	Fehler
FlexGroup Volume ist zu mehr als 90 % ausgelastet*	Vorfall	Volumen	Kritisch
Anomalie der Storage-Effizienz des Volume (ocumVolumeAbnormalStorageEfficiencyWarning)	Risiko	Volumen	Warnung
Volume Snapshot Reserve Unterauslastung (volumeSnaphotReserveUnderutilizedWarning)	Ereignis	Volumen	Warnung
Unzureichende Auslastung der Volume Snapshot Reserve (volumeSnaphotReserveUnderutilizedCleared)	Ereignis	Volumen	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Volume umbenannt(Nicht zutreffend)	Ereignis	Volumen	Informationen
Volume erkannt(Nicht zutreffend)	Ereignis	Volumen	Informationen
Volume gelöscht(Nicht zutreffend)	Ereignis	Volumen	Informationen

Wirkungsbereich: Performance

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
QoS Volume Max IOPS Warnschwelle überschritten(ocumQosVolumeMaxIopsWarning)	Risiko	Volumen	Warnung
QoS Volume Max MB/s Warnschwelle überschritten(ocumQosVolumeMaxMbpsWarning)	Risiko	Volumen	Warnung
QoS Volume Max IOPS/TB Warnschwelle überschritten(ocumQosVolumeMaxIopsPerTbWarning)	Risiko	Volumen	Warnung
Der in der Performance Service Level Policy definierte Schwellenwert für die Latenz des Workload-Volumes wurde überschritten (ocumConformanceLatencyWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-IOPS überschritten(ocumVolumeIopsIncident)	Vorfall	Volumen	Kritisch
Schwellenwert für die Volume IOPS-Warnung überschritten(ocumVolumeIopsWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Datenvolumen in MB/s überschritten(ocumVolumeMbpsIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume MB/s überschritten(ocumVolumeMbpsWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-Latenz überschritten(ocumVolumeLatencyIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volumenlatenz überschritten(ocumVolumeLatencyWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für die Cache-Miss-Rate des Volumens überschritten(ocumVolumeCacheMissRatioIncident)	Vorfall	Volumen	Kritisch
Schwellenwert für die Warnung zur Volume Cache Miss Ratio überschritten(ocumVolumeCacheMissRatioWarning)	Risiko	Volumen	Warnung
Kritische Schwellenwerte für Volumenlatenz und IOPS überschritten(ocumVolumeLatencyIopsIncident)	Vorfall	Volumen	Kritisch
Warnschwellenwert für Volume-Latenz und IOPS überschritten(ocumVolumeLatencyIopsWarning)	Risiko	Volumen	Warnung
Volume-Latenz und kritischer MB/s-Schwellenwert überschritten(ocumVolumeLatencyMbpsIncident)	Vorfall	Volumen	Kritisch
Warnschwellenwert für Volume-Latenz und MB/s überschritten(ocumVolumeLatencyMbpsWarning)	Risiko	Volumen	Warnung
Volume Latenz und verwendete Aggregate Performance Capacity: Kritischer Schwellenwert überschritten(ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volumenlatenz und genutzte aggregierte Performance-Kapazität überschritten(ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für Volume-Latenz und Aggregatauslastung überschritten(ocumVolumeLatencyAggregateUtilizationIncident)	Vorfall	Volumen	Kritisch
Warnschwellenwert für Volume-Latenz und Aggregatauslastung überschritten (ocumVolumeLatencyAggregateUtilizationWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volumenlatenz und Knotenkapazität für die genutzte Performance überschritten(ocumVolumeLatencyNodePerfCapacityUsedIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume-Latenz und genutzte Node-Performance-Kapazität überschritten(ocumVolumeLatencyNodePerfCapacityUsedWarning)	Risiko	Volumen	Warnung
Volume-Latenz und verwendete Knoten-Performance-Kapazität - kritischer Schwellenwert für Takeover überschritten(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Vorfall	Volumen	Kritisch
Volumenlatenz und genutzte Knoten-Performance-Kapazität - Schwellenwert für die Übernahmewarnung überschritten(ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Kritischer Schwellenwert für Volume-Latenz und Knotenauslastung überschritten(ocumVolumeLatencyNodeUtilizationIncident)	Vorfall	Volumen	Kritisch
Schwellenwert für Volumenlatenz und Knotenauslastung überschritten (ocumVolumeLatencyNodeUtilizationWarning)	Risiko	Volumen	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Die Anti-Ransomware-Überwachung des Volume ist aktiviert (aktiver Modus) (antiRansomwareVolumeStateEnabled)	Ereignis	Volumen	Informationen
Die Überwachung des Volumens mit Anti-Ransomware ist deaktiviert (antiRansomwareVolumeStateDisabled)	Risiko	Volumen	Warnung
Die Anti-Ransomware-Überwachung des Volumes ist aktiviert (Lernmodus) (antiRansomwareVolumeStateDryrun)	Ereignis	Volumen	Informationen
Die Überwachung des Volumens mit Anti-Ransomware ist pausiert (Lernmodus) (antiRansomwareVolumeStateDryrunPaused)	Risiko	Volumen	Warnung
Die Anti-Ransomware-Überwachung des Volumes ist pausiert (Aktiver Modus) (antiRansomwareVolumeStateEnablePaused)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Die Anti-Ransomware-Überwachung des Volumes wird deaktiviert (antiRansomwareVolumeStateDisableInProgress)	Risiko	Volumen	Warnung
Ransomware-Aktivität festgestellt (callHomeRansomwareActivitySeen)	Vorfall	Volumen	Kritisch
Volume geeignet für die Anti-Ransomware-Überwachung (Lernmodus) (ocumEvtVolumeArwCandidate)	Ereignis	Volumen	Informationen
Für die Anti-Ransomware-Überwachung geeignetes Volume (Aktivmodus) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Risiko	Volumen	Warnung
Volume weist übermäßig viele Anti-Ransomware-Warnungen auf (antiRansomwareFeatureNoisyVolume)	Risiko	Volumen	Warnung

Wirkungsbereich: Datenschutz

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Das Volume verfügt über unzureichenden lokalen Snapshot-Schutz (volumeLacksLocalProtectionWarning)	Risiko	Volumen	Warnung
Das Volume verfügt über unzureichenden lokalen Snapshot-Schutz (volumeLacksLocalProtectionCleared)	Risiko	Volumen	Warnung

Informationen zu Statusereignissen bei Volume Moves in Active IQ Unified Manager

Statusereignisse für Volume Verschiebungen informieren Sie über den Status Ihrer Volume Verschiebung, sodass Sie potenzielle Probleme überwachen können. Die Ereignisse sind nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und

Trap-Namen, das Auswirkungs Level, den Quelltyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungs-Level	Quellentyp	Schwere
Status der Volume Verschiebung: In Bearbeitung(Nicht zutreffend)	Ereignis	Volumen	Informationen
Status der Volume-Verschiebung - Fehlgeschlagen(ocumEvtVolumeMoveFailed)	Risiko	Volumen	Fehler
Status der Volumenverschiebung: Abgeschlossen(Nicht zutreffend)	Ereignis	Volumen	Informationen
Volume Move - Umstellung verschoben(ocumEvtVolumeMoveCutoverDeferred)	Risiko	Volumen	Warnung

Beschreibung von Ereignisfenstern und Dialogfeldern

Informationen zur Benachrichtigungsseite in Active IQ Unified Manager

Sie können den Unified Manager Server so konfigurieren, dass er Benachrichtigungen sendet, wenn ein Ereignis generiert oder einem Benutzer zugewiesen wird. Sie können auch die Benachrichtigungsmechanismen konfigurieren. Beispielsweise können Benachrichtigungen als E-Mails oder SNMP-Traps gesendet werden.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

E-Mail

In diesem Bereich ist die Konfiguration der folgenden E-Mail-Einstellungen für Warnungsbenachrichtigungen möglich:

- **Absenderadresse**

  Gibt die E-Mail-Adresse an, von der die Warnungsbenachrichtigung gesendet wird. Dieser Wert wird auch als Absenderadresse für einen Bericht verwendet, wenn dieser freigegeben wird. Wenn die Absenderadresse mit „ActiveIQUnifiedManager@localhost.com“ vorbelegt ist, sollte sie in eine gültige, funktionsfähige E-Mail-Adresse geändert werden, damit alle E-Mail-Benachrichtigungen erfolgreich zugestellt werden.

SMTP-Server

In diesem Bereich können Sie die folgenden SMTP-Servereinstellungen konfigurieren:

- **Hostname oder IP-Adresse**

  Gibt den Hostnamen Ihres SMTP-Hostservers an, mit dem die Warnbenachrichtigung an die angegebenen Empfänger gesendet wird.

- **Benutzername**

  Gibt den SMTP-Benutzernamen an. Der SMTP-Benutzername ist nur erforderlich, wenn SMTPAUTH auf dem SMTP-Server aktiviert ist.

- **Passwort**

  Gibt das SMTP-Passwort an. Der SMTP-Benutzername ist nur erforderlich, wenn SMTPAUTH auf dem SMTP-Server aktiviert ist.

- **Port**

  Gibt den Port an, den der SMTP-Hostserver zum Senden von Warnmeldungen verwendet.

  Der Standardwert ist 25.

- **START/TLS verwenden**

  Durch Aktivieren dieses Kontrollkästchens erfolgt die sichere Kommunikation zwischen dem SMTP-Server und dem Management-Server mithilfe der TLS/SSL-Protokolle (auch bekannt als start_tls und StartTLS).

- **SSL verwenden**

  Wenn dieses Kontrollkästchen aktiviert ist, erfolgt die sichere Kommunikation zwischen dem SMTP-Server und dem Management-Server über das SSL-Protokoll.

SNMP

In diesem Bereich können Sie die folgenden SNMP-Trap-Einstellungen konfigurieren:

- **Version**

  Legt die gewünschte SNMP-Version je nach Sicherheitsanforderung fest. Zur Auswahl stehen Version 1, Version 3, Version 3 mit Authentifizierung und Version 3 mit Authentifizierung und Verschlüsselung. Der Standardwert ist Version 1.

- **Trap-Zielhost**

  Gibt den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) an, die die vom Management-Server gesendeten SNMP-Traps empfängt. Mehrere Trap-Ziele können angegeben werden, indem die einzelnen Hosts durch Kommas getrennt werden.

  > Alle anderen SNMP-Einstellungen, wie z. B. „Version“ und „Outbound Port“, müssen für alle Hosts in der Liste gleich sein.

- **Ausgehender Trap Port**

  Gibt den Port an, über den der SNMP-Server die vom Management-Server gesendeten Traps empfängt.

  Der Standardwert ist 162.

- **Gemeinschaft**

  Die Community-String für den Zugriff auf den Host.

- **Engine-ID**

  Gibt die eindeutige Kennung des SNMP-Agenten an und wird automatisch vom Management-Server generiert. Die Engine-ID ist in SNMP Version 3, SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Benutzername**

  Gibt den SNMP-Benutzernamen an. Der Benutzername ist mit SNMP Version 3, SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Authentifizierungsprotokoll**

  Legt das Protokoll zur Benutzerauthentifizierung fest. Zu den Protokolloptionen gehören MD5 und SHA. MD5 ist der Standardwert. Das Authentifizierungsprotokoll ist in SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Authentifizierungskennwort**

  Gibt das Passwort an, das zur Authentifizierung eines Benutzers verwendet wird. Das Authentifizierungspasswort ist in SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Datenschutzprotokoll**

  Legt das Datenschutzprotokoll für die Verschlüsselung von SNMP-Nachrichten fest. Zu den Protokolloptionen gehören AES 128 und DES. Der Standardwert ist AES 128. Das Datenschutzprotokoll ist mit SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Datenschutzpasswort**

  Gibt das Passwort bei Verwendung des Datenschutzprotokolls an. Das Datenschutzpasswort ist mit SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

Weitere Informationen zu SNMP-Objekten und -Traps können Sie die "Active IQ Unified Manager MIB" von der NetApp Support Site herunterladen.

Informationen zur Inventarseite für die Ereignisverwaltung in Active IQ Unified Manager

Die Bestandsseite von Event Management ermöglicht Ihnen die Anzeige einer Liste der aktuellen Ereignisse und ihrer Eigenschaften. Sie können Aufgaben wie das Bestätigen, Beheben und Zuweisen von Ereignissen ausführen. Außerdem können Sie für bestimmte Ereignisse eine Warnung hinzufügen.

Die Informationen auf dieser Seite aktualisieren sich alle 5 Minuten automatisch, damit die aktuellsten neuen Ereignisse angezeigt werden.

Filterkomponenten

Damit lassen sich die in der Ereignisliste angezeigten Informationen anpassen. Sie können die Liste der angezeigten Ereignisse mithilfe der folgenden Komponenten verfeinern:

- Menü „Ansicht“ zum Auswählen aus einer vordefinierten Liste von Filteroptionen.

  Dies umfasst Elemente wie alle aktiven (neuen und bestätigten) Ereignisse, aktive Performance Ereignisse, mir (dem angemeldeten Benutzer) zugewiesene Ereignisse und alle während sämtlicher Wartungsfenster generierten Ereignisse.

- Suchbereich zum Verfeinern der Ereignisliste durch Eingabe vollständiger oder teilweiser Begriffe.
- Schaltfläche „Filter“, die den Filterbereich öffnet, in dem Sie aus allen verfügbaren Feldern und Feldattributen auswählen können, um die Ereignisliste einzugrenzen.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Zuweisen an**

  Hiermit können Sie den Benutzer auswählen, dem das Ereignis zugewiesen wird. Wenn Sie einem Benutzer ein Ereignis zuweisen, erscheinen der Benutzername und der Zeitpunkt der Zuweisung in der Ereignisliste für die ausgewählten Ereignisse.

  - Mich

    Weist das Ereignis dem aktuell angemeldeten Benutzer zu.

  - Ein anderer Benutzer

    Es wird das Dialogfeld „Besitzer zuweisen“ angezeigt, in dem Sie das Ereignis anderen Benutzern zuweisen oder erneut zuweisen können. Sie können die Zuweisung von Ereignissen auch aufheben, indem Sie das Feld „Besitzer“ leer lassen.

- **Bestätigen**

  Bestätigt die ausgewählten Ereignisse.

  Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und der Zeitpunkt, zu dem Sie das Ereignis bestätigt haben, in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt. Wenn Sie ein Ereignis bestätigen, sind Sie für die Verwaltung dieses Ereignisses verantwortlich.

  Information Ereignisse können nicht quittiert werden.

- **Als gelöst markieren**

  Ermöglicht es Ihnen, den Ereignisstatus in „Gelöst“ zu ändern.

  Wenn Sie ein Ereignis beheben, werden Ihr Benutzername und der Zeitpunkt der Behebung in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie eine Korrekturmaßnahme für das Ereignis ergriffen haben, müssen Sie das Ereignis als behoben markieren.

- **Warnung hinzufügen**

  Das Dialogfeld „Warnung hinzufügen“ wird angezeigt, in dem Sie Warnungen für die ausgewählten Ereignisse hinzufügen können.

- **Berichte**

Ermöglicht den Export von Details der aktuellen Ereignisansicht in eine Datei mit kommagetrennten Werten (.csv) oder ein PDF-Dokument.

- **Spaltenauswahl ein-/ausblenden**

  Ermöglicht die Auswahl der auf der Seite angezeigten Spalten sowie ihrer Anzeigereihenfolge.

Ereignisliste

Zeigt Details aller Ereignisse geordnet nach Auslösezeitpunkt an.

Standardmäßig wird die Ansicht „Alle aktiven Ereignisse“ angezeigt, um die neuen und quittierten Ereignisse der letzten sieben Tage mit dem Impact Level „Vorfall“ oder „Risiko“ anzuzeigen.

- **Auslösezeit**

  Der Zeitpunkt, zu dem das Ereignis ausgelöst wurde.

- **Schweregrad**

  Der Schweregrad des Ereignisses: Kritisch (), Fehler (), Warnung () und Information ().

- **Zustand**

  Der Ereignisstatus: Neu, Bestätigt, Behoben oder Veraltet.

- **Auswirkungslevel**

  Der Auswirkungs-Level des Ereignisses: Vorfall, Risiko, Ereignis oder Upgrade.

- **Auswirkungsbereich**

  Der Wirkungsbereich des Ereignisses: Verfügbarkeit, Kapazität, Performance, Schutz, Konfiguration oder Sicherheit.

- **Name**

  Der Name des Ereignisses. Durch Auswählen des Namens wird die Seite mit den Ereignisdetails für dieses Ereignis angezeigt.

- **Quelle**

  Der Name des Objekts, bei dem das Ereignis aufgetreten ist. Die Auswahl des Namens zeigt die Seite mit den Systemstatus- oder Performance-Details für dieses Objekt an.

  Bei einem Verstoß gegen eine gemeinsame QoS-Richtlinie wird in diesem Feld nur das Workload-Objekt angezeigt, das die meisten IOPS oder MB/s verbraucht. Weitere Workloads, die diese Richtlinie verwenden, werden auf der Seite mit den Ereignisdetails angezeigt.

- **Quellentyp**

  Der Objekttyp (z. B. Storage VM, Volume oder Qtree), dem das Ereignis zugeordnet ist.

- **Zugewiesen an**

  Der Name des Benutzers, dem das Ereignis zugewiesen ist.

- **Ereignisursprung**

  Unabhängig davon, ob das Ereignis vom "Active IQ Portal" oder direkt von "Active IQ Unified Manager" stammt.

- **Anmerkungsname**

  Der Name der Annotation, die dem Storage Objekt zugewiesen ist.

- **Anmerkungen**

  Die Anzahl der für ein Ereignis hinzugefügten Notizen.

- **Ausstehende Tage**

  Die Anzahl der Tage seit der erstmaligen Generierung des Ereignisses.

- **Zugewiesene Zeit**

  Die seit der Zuweisung des Ereignisses an einen Benutzer verstrichene Zeit. Wenn mehr als eine Woche vergangen ist, wird der Zeitstempel angezeigt, zu dem das Ereignis einem Benutzer zugewiesen wurde.

- **Bestätigt von**

  Der Name des Benutzers, der das Ereignis bestätigt hat. Das Feld ist leer, wenn das Ereignis nicht bestätigt wurde.

- **Bestätigte Zeit**

  Die seit der Bestätigung des Ereignisses verstrichene Zeit. Wenn mehr als eine Woche vergangen ist, wird der Zeitstempel angezeigt, zu dem das Ereignis bestätigt wurde.

- **Gelöst durch**

  Der Name des Benutzers, der das Ereignis behoben hat. Das Feld ist leer, wenn das Ereignis nicht behoben ist.

- **Zeitpunkt der Behebung**

  Die seit der Behebung des Ereignisses verstrichene Zeit. Wenn mehr als eine Woche vergangen ist, wird der Zeitstempel angezeigt, zu dem das Ereignis behoben wurde.

- **Zeitpunkt der Außerkraftsetzung**

  Der Zeitpunkt, an dem der Status des Ereignisses zu Obsolete wurde.

Seite mit Ereignisdetails

Informationen zur Seite „Ereignisdetails“ in Active IQ Unified Manager

Auf der Seite mit den Ereignisdetails lassen sich die Details eines ausgewählten Ereignisses anzeigen, z. B. der Schweregrad des Ereignisses, das Auswirkungs-Level, der Auswirkungsbereich und die Ereignisquelle. Außerdem lassen sich zusätzliche Informationen zu möglichen Korrekturmaßnahmen zur Behebung des Problems anzeigen.

- **Ereignisname**

  Der Name des Ereignisses und der Zeitpunkt, zu dem das Ereignis zuletzt beobachtet wurde.

  Bei nicht auf die Performance bezogenen Ereignissen sind die Informationen zum letzten Auftreten nicht bekannt, solange sich das Ereignis im Status „Neu“ oder „Bestätigt“ befindet, und werden daher ausgeblendet.

- **Ereignisbeschreibung**

  Eine kurze Beschreibung des Ereignisses.

  In einigen Fällen enthält die Ereignisbeschreibung einen Grund für das Auslösen des Ereignisses.

- **Komponente in Konflikt**

  Bei dynamischen Performance-Ereignissen werden in diesem Abschnitt Symbole angezeigt, die die logischen und physischen Komponenten des Clusters darstellen. Wenn eine Komponente in einem Konflikt steht, ist ihr Symbol eingekreist und rot hervorgehoben.

  Eine Beschreibung der hier angezeigten Komponenten ist unter *Cluster-Komponenten und warum sie in Konflikt geraten können* verfügbar.

Beschreibungen der Abschnitte Ereignisinformationen, Systemdiagnose und Vorgeschlagene Maßnahmen finden sich in anderen Themen.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Notizen-Symbol**

  Ermöglicht es Ihnen, eine Notiz zum Ereignis hinzuzufügen oder zu aktualisieren sowie alle von anderen Benutzern hinterlassenen Notizen einzusehen.

Aktionsmenü

- **Mir zuweisen**

  Ordnet Ihnen das Ereignis zu.

- **Anderen zuweisen**

  Öffnet das Dialogfeld „Besitzer zuweisen“, über das sich das Ereignis anderen Benutzern zuweisen oder neu zuweisen lässt.

  Wenn Sie einem Benutzer ein Ereignis zuweisen, werden der Name des Benutzers und der Zeitpunkt der Zuweisung in die Ereignisliste für die ausgewählten Ereignisse aufgenommen.

  Die Zuweisung von Ereignissen kann auch aufgehoben werden, indem das Feld „Eigentümer“ leer gelassen wird.

- **Bestätigen**

  Bestätigung der ausgewählten Ereignisse, damit keine wiederholten Alarmbenachrichtigungen mehr eingehen.

Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und der Zeitpunkt der Bestätigung in der Ereignisliste (Bestätigt von) für die ausgewählten Ereignisse angezeigt. Wenn Sie ein Ereignis bestätigen, übernehmen Sie die Verantwortung für dessen Verwaltung.

- **Als gelöst markieren**

  Ermöglicht es Ihnen, den Ereignisstatus in Resolved zu ändern.

  Wenn Sie ein Ereignis beheben, werden Ihr Benutzername und der Zeitpunkt, zu dem Sie das Ereignis behoben haben, in der Ereignisliste (Behoben von) für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie eine Korrekturmaßnahme für das Ereignis ergriffen haben, müssen Sie das Ereignis als behoben markieren.

- **Warnung hinzufügen**

  Das Dialogfeld „Warnung hinzufügen“ wird angezeigt, in dem Sie eine Warnung für das ausgewählte Ereignis hinzufügen können.

Informationen über den Abschnitt „Ereignisinformationen“ in Active IQ Unified Manager

Im Abschnitt „Ereignisinformationen“ auf der Seite „Ereignisdetails“ finden Sie Details zu einem ausgewählten Ereignis, z. B. den Schweregrad, das Auswirkungs-Level, den Auswirkungsbereich und die Ereignisquelle.

Felder, die für den Ereignistyp nicht relevant sind, werden ausgeblendet. Sie können die folgenden Ereignisdetails anzeigen:

- **Zeitpunkt der Ereignisauslösung**

  Der Zeitpunkt, zu dem das Ereignis ausgelöst wurde.

- **Zustand**

  Der Ereignisstatus: Neu, Bestätigt, Behoben oder Veraltet.

- **Veraltete Ursache**

  Die Maßnahmen, die dazu führten, dass das Ereignis als veraltet markiert wurde, beispielsweise die Behebung des Problems.

- **Ereignisdauer**

  Bei aktiven (neuen und bestätigten) Ereignissen ist dies die Zeitspanne zwischen der Erkennung und dem Zeitpunkt, zu dem das Ereignis zuletzt analysiert wurde. Bei veralteten Ereignissen ist dies die Zeitspanne zwischen der Erkennung und dem Zeitpunkt, zu dem das Ereignis gelöst wurde.

  Dieses Feld erscheint bei allen Performance-Ereignissen und bei anderen Ereignistypen erst, nachdem sie behoben wurden oder veraltet sind.

- **Zuletzt gesehen**

  Datum und Uhrzeit, zu der das Ereignis zuletzt als aktiv erkannt wurde.

  Bei Performance Ereignissen kann dieser Wert aktueller sein als der Auslösezeitpunkt des Ereignisses, da dieses Feld nach jeder neuen Erfassung von Performance Daten aktualisiert wird, solange das Ereignis

aktiv ist. Bei anderen Ereignistypen wird dieser Inhalt im Status „Neu“ oder „Bestätigt“ nicht aktualisiert, und das Feld ist daher ausgeblendet.

- **Schweregrad**

  Der Schweregrad des Ereignisses: Kritisch (), Fehler (), Warnung () und Information ().

- **Auswirkungslevel**

  Der Auswirkungs-Level des Ereignisses: Vorfall, Risiko, Ereignis oder Upgrade.

- **Auswirkungsbereich**

  Der Wirkungsbereich des Ereignisses: Verfügbarkeit, Kapazität, Performance, Schutz, Konfiguration oder Sicherheit.

- **Quelle**

  Der Name des Objekts, auf dem das Ereignis stattgefunden hat.

  Bei der Anzeige der Details eines gemeinsam genutzten QoS-Richtlinienereignisses werden in diesem Feld bis zu drei der Workload-Objekte aufgelistet, die die meisten IOPS oder MBps verbrauchen.

  Über den Link mit dem Quellnamen lässt sich die Detailseite zum Systemstatus oder zur Performance dieses Objekts aufrufen.

- **Quellenanmerkungen**

  Zeigt den Namen und den Wert der Annotation für das Objekt an, dem das Ereignis zugeordnet ist.

  Dieses Feld wird nur bei Systemstatusereignissen auf Clustern, SVMs und Volumes angezeigt.

- **Quellgruppen**

  Zeigt die Namen aller Gruppen an, denen das betroffene Objekt angehört.

  Dieses Feld wird nur bei Systemstatusereignissen auf Clustern, SVMs und Volumes angezeigt.

- **Quellentyp**

  Der Objekttyp (z. B. SVM, Volume oder Qtree), dem das Ereignis zugeordnet ist.

- **Im Cluster**

  Der Name des Clusters, auf dem das Ereignis stattfand.

  Sie können auf den Link mit dem Clusternamen klicken, um die Detailseite für den Systemstatus oder die Performance dieses Clusters anzuzeigen.

- **Anzahl der betroffenen Objekte**

  Die Anzahl der von dem Ereignis betroffenen Objekte.

  Über den Objektlink lässt sich die Inventarseite anzeigen, die mit den Objekten gefüllt ist, die aktuell von diesem Ereignis betroffen sind.

Dieses Feld wird nur für Performance-Ereignisse angezeigt.

- **Betroffene Volumina**

  Die Anzahl der von diesem Ereignis betroffenen Bände.

  Dieses Feld wird nur für Performance Ereignisse auf Knoten oder Aggregaten angezeigt.

- **Ausgelöste Richtlinie**

  Der Name der Schwellenwertrichtlinie, die das Ereignis ausgelöst hat.

  Wenn sich der Mauszeiger über dem Richtliniennamen befindet, sind die Details der Schwellenwertrichtlinie zu sehen. Bei adaptiven QoS-Richtlinien werden außerdem die definierte Richtlinie, die Blockgröße und der Zuweisungstyp (zugewiesener oder belegter Speicherplatz) angezeigt.

  Dieses Feld wird nur für Performance-Ereignisse angezeigt.

- **Regel-ID**

  Bei Active IQ Plattformereignissen ist dies die Nummer der Regel, die zum Generieren des Ereignisses ausgelöst wurde.

- **Bestätigt von**

  Name der Person, die das Ereignis bestätigt hat, und Zeitpunkt der Bestätigung.

- **Behoben durch**

  Name der Person, die den Vorfall gelöst hat, und Zeitpunkt der Lösung des Vorfalls.

- **Zugewiesen an**

  Der Name der Person, die mit der Bearbeitung des Ereignisses beauftragt ist.

- **Warnungseinstellungen**

  Die folgenden Informationen zu Warnmeldungen werden angezeigt:

  - Wenn dem ausgewählten Ereignis keine Warnungen zugeordnet sind, wird der Link **Warnung hinzufügen** angezeigt.

    Sie können das Dialogfeld „Warnung hinzufügen“ durch Klicken auf den Link öffnen.

  - Wenn dem ausgewählten Ereignis eine Warnung zugeordnet ist, wird der Name der Warnung angezeigt.

    Sie können das Dialogfeld „Warnung bearbeiten“ öffnen, indem Sie auf den Link klicken.

  - Falls dem ausgewählten Ereignis mehrere Warnmeldungen zugeordnet sind, wird die Anzahl der Warnmeldungen angezeigt.

    Die Seite „Alert Setup“ kann über den Link geöffnet werden, über den weitere Details zu diesen Warnmeldungen angezeigt werden.

  Deaktivierte Warnmeldungen werden nicht angezeigt.

- **Letzte Benachrichtigung gesendet**

  Datum und Uhrzeit, zu der die letzte Warnmeldung versendet wurde.

- **Versand per**

  Der Mechanismus, mit dem die Warnmeldung gesendet wurde: E-Mail oder SNMP-Trap.

- **Vorheriger Skriptlauf**

  Der Name des Skripts, das beim Generieren der Warnung ausgeführt wurde.

Informationen zu empfohlenen Aktionen in Active IQ Unified Manager

Der Abschnitt „Empfohlene Maßnahmen“ auf der Seite mit den Ereignisdetails bietet mögliche Gründe für das Ereignis und schlägt einige Maßnahmen vor, damit das Ereignis selbst behoben werden kann. Die empfohlenen Maßnahmen sind auf die Art des Ereignisses oder auf die Art des Schwellenwerts zugeschnitten, der überschritten wurde.

Dieser Bereich wird nur für bestimmte Ereignistypen angezeigt.

In einigen Fällen enthält die Seite **Hilfe**-Links mit weiterführenden Informationen zu vielen vorgeschlagenen Aktionen, einschließlich Anleitungen zur Durchführung bestimmter Aktionen. Einige dieser Aktionen können die Verwendung von Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI-Befehlen oder einer Kombination dieser Tools erfordern.

Die hier vorgeschlagenen Maßnahmen sollten nur als Orientierungshilfe bei der Behebung dieses Ereignisses betrachtet werden. Die Maßnahmen, die Sie zur Behebung dieses Ereignisses ergreifen, sollten sich nach den Gegebenheiten Ihrer Umgebung richten.

Für eine detailliertere Analyse von Objekt und Ereignis steht die Schaltfläche **Analyze Workload** zur Verfügung, über die die Seite Workload Analysis angezeigt wird.

Bestimmte Ereignisse kann Unified Manager umfassend diagnostizieren und eine einzelne Lösung bereitstellen. Sofern verfügbar, werden diese Lösungen mit einer Schaltfläche **Fix It** angezeigt. Mit dieser Schaltfläche behebt Unified Manager das Problem, das das Ereignis verursacht.

Bei Active IQ Plattformereignissen kann dieser Abschnitt, sofern verfügbar, einen Link zu einem NetApp Knowledgebase-Artikel enthalten, der das Problem und mögliche Lösungen beschreibt. An Standorten ohne externen Netzwerkzugriff wird lokal ein PDF des Knowledgebase-Artikels geöffnet; das PDF ist Teil der Regeldatei, die Sie manuell auf die Unified Manager Instanz herunterladen.

Informationen zur Systemdiagnose in Active IQ Unified Manager

Der Abschnitt „Systemdiagnose“ auf der Seite mit den Ereignisdetails bietet Informationen, die Ihnen bei der Diagnose von Problemen helfen können, die möglicherweise für das Ereignis verantwortlich waren.

Dieser Bereich wird nur bei einigen Ereignissen angezeigt.

Einige Performance Ereignisse liefern Diagramme, die für das jeweils ausgelöste Ereignis relevant sind. Dazu gehören in der Regel ein IOPS- oder MB/s-Diagramm sowie ein Latenzdiagramm für die vorangegangenen zehn Tage. In dieser Anordnung lässt sich erkennen, welche Storage Komponenten die Latenz am stärksten beeinflussen oder von der Latenz betroffen sind, wenn das Ereignis aktiv ist.

Bei dynamischen Performance-Ereignissen werden folgende Diagramme angezeigt:

- Workload-Latenz - Zeigt den Verlauf der Latenz für die wichtigsten Opfer-, Bully- oder Shark-Workloads an der Komponente mit Ressourcenkonflikt an.
- Workload-Aktivität - Zeigt Details zur Workload-Nutzung der Clusterkomponente bei Ressourcenkonflikten an.
- Ressourcenaktivität - Anzeige historischer Performance Statistiken für die Clusterkomponente im Engpass.

Andere Diagramme werden angezeigt, wenn einige Clusterkomponenten um Ressourcen konkurrieren.

Andere Ereignisse liefern eine kurze Beschreibung der Art der Analyse, die das System für das Storage Objekt durchführt. In manchen Fällen gibt es bei systemdefinierten Performance-Richtlinien, die mehrere Performance-Zähler analysieren, eine oder mehrere Zeilen, eine für jede analysierte Komponente. In diesem Szenario zeigt ein grünes oder rotes Symbol neben der Diagnose an, ob in dieser bestimmten Diagnose ein Problem gefunden wurde oder nicht.

Informationen zur Seite „Ereigniseinrichtung“ in Active IQ Unified Manager

Die Seite „Ereigniseinstellungen“ zeigt die Liste der deaktivierten Ereignisse an und bietet Informationen wie den zugehörigen Objekttyp und den Schweregrad des Ereignisses. Sie können auch Aufgaben wie das globale Deaktivieren oder Aktivieren von Ereignissen ausführen.

Auf diese Seite kann nur zugegriffen werden, wenn Sie die Rolle „Application Administrator“ oder „Storage Administrator“ haben.

Befehlsschaltflächen

Mit den Befehlsschaltflächen lassen sich für ausgewählte Ereignisse folgende Aufgaben ausführen:

- **Deaktivieren**

  Öffnet das Dialogfeld „Ereignisse deaktivieren“, mit dem Sie Ereignisse deaktivieren können.

- **Aktivieren**

  Aktiviert ausgewählte Ereignisse, die Sie zuvor deaktiviert hatten.

- **Upload-Regeln**

  Das Dialogfeld „Upload Rules“ wird geöffnet, über das Standorte ohne externen Netzwerkzugriff die Active IQ Regeldatei manuell in Unified Manager hochladen können. Die Regeln werden auf Cluster AutoSupport Meldungen angewendet, um Ereignisse für Systemkonfiguration, Verkabelung, Best Practices und Verfügbarkeit gemäß den Definitionen der Active IQ Plattform zu generieren.

- **EMS-Ereignisse abonnieren**

  Öffnet das Dialogfeld „EMS-Ereignisse abonnieren“, über das Sie bestimmte Ereignisse des Event Management System (EMS) von den Clustern abonnieren können, die Sie überwachen. Das EMS erfasst Informationen über Ereignisse, die im Cluster auftreten. Wenn eine Benachrichtigung für ein abonniertes EMS-Ereignis eingeht, wird ein Unified Manager Ereignis mit dem entsprechenden Schweregrad generiert.

Listenansicht

Die Listenansicht zeigt (in Tabellenform) Informationen zu deaktivierten Ereignissen an. Mithilfe der Spaltenfilter können Sie die angezeigten Daten anpassen.

- **Ereignis**

  Zeigt den Namen des deaktivierten Ereignisses an.

- **Schweregrad**

  Zeigt den Schweregrad des Ereignisses an. Der Schweregrad kann Kritisch, Fehler, Warnung oder Information sein.

- **Quellentyp**

  Zeigt den Quelltyp an, für den das Ereignis generiert wurde.

Das Dialogfeld „Ereignisse“ in Active IQ Unified Manager wird deaktiviert

Im Dialogfeld „Ereignisse deaktivieren“ wird die Liste der Ereignistypen angezeigt, für die Sie Ereignisse deaktivieren können. Sie können Ereignisse für einen Ereignistyp auf Grundlage eines bestimmten Schweregrads oder für eine Gruppe von Ereignissen deaktivieren.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Bereich „Ereigniseigenschaften“

Der Bereich „Ereigniseigenschaften“ enthält die folgenden Ereigniseigenschaften:

- **Ereignisschweregrad**

  Ermöglicht die Auswahl von Ereignissen anhand des Typs des Schweregrads, der Kritisch, Fehler, Warnung oder Information sein kann.

- **Ereignisname enthält**

  Ermöglicht das Filtern von Ereignissen, deren Name die angegebenen Zeichen enthält.

- **Passende Ereignisse**

  Zeigt die Liste der Ereignisse an, die dem von Ihnen angegebenen Typ des Schweregrads des Ereignisses und dem Text-String entsprechen.

- **Ereignisse deaktivieren**

  Zeigt die Liste der Ereignisse an, die Sie zum Deaktivieren ausgewählt haben.

  Der Schweregrad des Ereignisses wird auch zusammen mit dem Ereignisnamen angezeigt.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie für die ausgewählten Ereignisse folgende Aufgaben ausführen:

- **Speichern und schließen**

  Deaktiviert den Ereignistyp und schließt das Dialogfeld.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld.

Benachrichtigungen verwalten

Informationen zu Warnmeldungen in Active IQ Unified Manager

Obwohl Ereignisse kontinuierlich auftreten, generiert der Unified Manager nur dann eine Warnung, wenn ein Ereignis festgelegte Filterkriterien erfüllt. Sie können die Ereignisse auswählen, für die Warnungen generiert werden sollen—beispielsweise, wenn ein Speicherplatzschwellenwert überschritten wird oder ein Objekt offline geht. Sie können eine Warnung auch mit einem Skript verknüpfen, das beim Auslösen einer Warnung ausgeführt wird.

Zu den Filterkriterien gehören Objektklasse, Name oder Ereignisschweregrad.

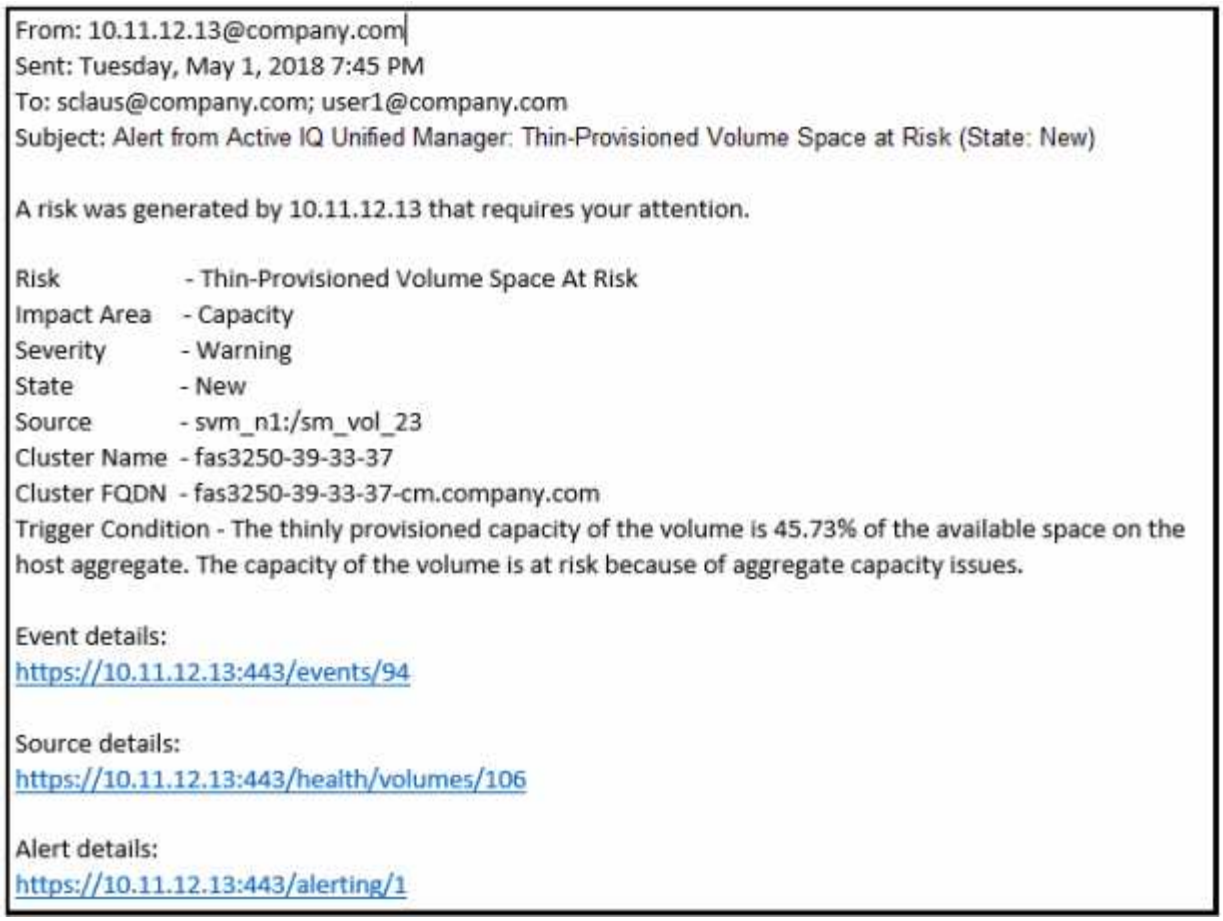
Informationen in einer Active IQ Unified Manager Benachrichtigungs-E-Mail

Unified Manager Benachrichtigungs-E-Mails enthalten den Typ des Ereignisses, den Schweregrad des Ereignisses, den Namen der Richtlinie oder des Schwellenwerts, deren bzw. dessen Überschreitung das Ereignis verursacht hat, sowie eine Beschreibung des Ereignisses. Die E-Mail-Nachricht enthält außerdem für jedes Ereignis einen Hyperlink, über den sich die Detailseite des Ereignisses in der UI anzeigen lässt.

Alle Benutzer, die den Erhalt von Alerts abonniert haben, erhalten Benachrichtigungs-E-Mails.

Wenn sich ein Performance-Zähler oder ein Kapazitätswert während eines Erfassungszeitraums stark ändert, kann dies dazu führen, dass gleichzeitig ein kritisches und ein Warnereignis für dieselbe Schwellenwertrichtlinie ausgelöst werden. In diesem Fall erhalten Sie möglicherweise eine E-Mail für das Warnereignis und eine weitere für das kritische Ereignis. Dies liegt daran, dass Unified Manager es Ihnen ermöglicht, Benachrichtigungen für Warn- und kritische Schwellenwertüberschreitungen separat zu abonnieren.

Nachfolgend ist ein Beispiel für eine Benachrichtigungs-E-Mail dargestellt:


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

Benachrichtigungen hinzufügen

Hinzufügen von Benachrichtigungen in Active IQ Unified Manager

Sie können Warnmeldungen so konfigurieren, dass Sie benachrichtigt werden, wenn ein bestimmtes Ereignis generiert wird. Sie können Warnmeldungen für eine einzelne Ressource, für eine Gruppe von Ressourcen oder für Ereignisse eines bestimmten Typs des Schweregrads konfigurieren. Sie können die Häufigkeit angeben, mit der Sie benachrichtigt werden möchten, und der Warnmeldung ein Skript zuordnen.

Bevor Sie beginnen

- Es müssen Benachrichtigungseinstellungen wie die E-Mail-Adresse des Benutzers, der SMTP-Server und der SNMP-Trap-Host konfiguriert sein, damit der Active IQ Unified Manager Server diese Einstellungen verwenden kann, um Benutzern Benachrichtigungen zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Benachrichtigung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn ein Skript basierend auf dem Ereignis ausgeführt werden soll, muss das Skript zuvor über die Seite „Skripte“ zu Unified Manager hinzugefügt worden sein.
- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Es besteht die Möglichkeit, eine Benachrichtigung direkt auf der Seite „Ereignisdetails“ nach dem Empfang eines Ereignisses zu erstellen, zusätzlich zur Erstellung einer Benachrichtigung über die Seite „Benachrichtigungseinrichtung“, wie hier beschrieben.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Alarmeinstellungen Hinzufügen** auswählen.
3. Im Dialogfeld **Warnung hinzufügen** auf **Name** klicken und einen Namen sowie eine Beschreibung für die Warnung eingeben.
4. **Ressourcen** auswählen und die Ressourcen bestimmen, die in die Benachrichtigung einbezogen oder von ihr ausgeschlossen werden.

   Ein Filter kann festgelegt werden, indem im Feld **Name enthält** ein Text-String angegeben wird, um eine Gruppe von Ressourcen auszuwählen. Basierend auf dem angegebenen Text-String werden in der Liste der verfügbaren Ressourcen nur die Ressourcen angezeigt, die der Filterregel entsprechen. Der angegebene Text-String ist Groß-/Kleinschreibungs-empfindlich.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschluss- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschlussregel, und die Warnung wird für Ereignisse, die sich auf die ausgeschlossene Ressource beziehen, nicht generiert.

5. Auf **Ereignisse** klicken und die Ereignisse anhand des Ereignisnamens oder des Typs des Schweregrads auswählen, für die ein Alarm ausgelöst werden soll.

   Um mehr als ein Ereignis auszuwählen, die Strg-Taste gedrückt halten, während die Auswahl getroffen wird.

6. Auf **Aktionen** klicken, die Benutzer auswählen, die benachrichtigt werden sollen, die Benachrichtigungshäufigkeit festlegen, auswählen, ob ein SNMP-Trap an den Trap-Empfänger gesendet wird, und ein Skript zuweisen, das ausgeführt wird, wenn eine Warnung generiert wird.

   Wenn die für den Benutzer angegebene E-Mail-Adresse geändert und die Benachrichtigung erneut zum Bearbeiten geöffnet wird, bleibt das Namensfeld leer, da die geänderte E-Mail-Adresse nicht mehr dem zuvor ausgewählten Benutzer zugeordnet ist. Auch wenn die E-Mail-Adresse des ausgewählten Benutzers auf der Seite „Benutzer“ geändert wurde, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

   Alternativ ist es möglich, die Benutzer auch über SNMP-Traps zu benachrichtigen.

7. Auf **Speichern** klicken.

Beispiel für das Hinzufügen einer Benachrichtigung

Dieses Beispiel zeigt, wie eine Benachrichtigung erstellt wird, die die folgenden Anforderungen erfüllt:

- Name der Warnung: HealthTest
- Ressourcen: Umfasst alle Volumes, deren Name „abc“ enthält, und schließt alle Volumes aus, deren Name „xyz“ enthält.
- Ereignisse: umfasst alle kritischen Gesundheitsereignisse
- Aktionen: Enthält "sample@domain.com", ein "Test" Skript und der Benutzer muss alle 15 Minuten benachrichtigt werden

Im Dialogfeld „Warnung hinzufügen“ sind die folgenden Schritte auszuführen:

1. Nach Auswahl von **Name** erfolgt die Eingabe von **`HealthTest`** in das Feld **Alert Name**.

2. **Ressourcen** auswählen und im Tab „Einschließen“ **Volumes** aus der Dropdown-Liste wählen.
   a. Die Eingabe von **`abc`** in das Feld **Name enthält** zeigt die Volumes an, deren Name "abc" enthält.
   b. **<<All Volumes whose name contains 'abc'>>** im Bereich „Verfügbare Ressourcen“ auswählen und in den Bereich „Ausgewählte Ressourcen“ verschieben.
   c. Nach Auswahl von **Ausschließen** ist **`xyz`** in das Feld **Name enthält** einzugeben; anschließend ist **Hinzufügen** auszuwählen.
3. Auf **Ereignisse** klicken und im Feld **Ereignisschweregrad Kritisch** auswählen.
4. Im Bereich „Übereinstimmende Ereignisse“ **Alle kritischen Ereignisse** auswählen und in den Bereich „Ausgewählte Ereignisse“ verschieben.
5. Unter **Aktionen** im Feld „Diese Benutzer benachrichtigen“ **`sample@domain.com`** eingeben.
6. **Alle 15 Minuten erinnern** benachrichtigt den Benutzer alle 15 Minuten.

   Sie können eine Benachrichtigung so konfigurieren, dass sie über einen festgelegten Zeitraum wiederholt an die Empfänger gesendet wird. Es sollte der Zeitpunkt festgelegt werden, ab dem die Ereignisbenachrichtigung für die Benachrichtigung aktiv ist.
7. Im Menü „Auszuführendes Skript auswählen“ das Skript **Test** auswählen.
8. Auf **Speichern** klicken.

Richtlinien zum Hinzufügen von Warnmeldungen in Active IQ Unified Manager

Sie können Warnungen basierend auf einer Ressource, z. B. einem Cluster, Knoten, Aggregat oder Volume, sowie auf Ereignissen eines bestimmten Typs des Schweregrads hinzufügen. Es empfiehlt sich, eine Warnung für jedes Ihrer kritischen Objekte hinzuzufügen, nachdem Sie den Cluster hinzugefügt haben, zu dem das Objekt gehört.

Mithilfe der folgenden Richtlinien und Überlegungen lassen sich Warnmeldungen erstellen, um Ihre Systeme effektiv zu managen:

- Alarmbeschreibung

  Sie sollten eine Beschreibung für die Warnmeldung angeben, damit Sie Ihre Warnmeldungen effektiv nachverfolgen können.

- Ressourcen

  Sie sollten entscheiden, für welche physische oder logische Ressource eine Warnung erforderlich ist. Ressourcen können nach Bedarf ein- oder ausgeschlossen werden. Wenn beispielsweise Aggregate durch die Konfiguration einer Warnung genau überwacht werden sollen, müssen die erforderlichen Aggregate aus der Ressourcenliste ausgewählt werden.

  Wenn Sie eine Ressourcenkategorie auswählen, zum Beispiel **<<All User or Group Quotas>>**, dann erhalten Sie Warnmeldungen für alle Objekte in dieser Kategorie.

> Die Auswahl eines Clusters als Ressource wählt die Storage Objekte innerhalb dieses Clusters nicht automatisch aus. Wenn Sie beispielsweise eine Warnung für alle kritischen Ereignisse für alle Cluster erstellen, erhalten Sie nur Warnungen für kritische Cluster-Ereignisse. Sie erhalten keine Warnungen für kritische Ereignisse auf Knoten, Aggregaten usw.

- Schweregrad

  Sie legen fest, ob ein Ereignis eines bestimmten Typs des Schweregrads (Kritisch, Fehler, Warnung) die Warnung auslösen soll und, falls ja, welcher Typ des Schweregrads.

- Ausgewählte Ereignisse

  Wenn Sie eine Warnmeldung basierend auf dem Typ des generierten Ereignisses hinzufügen, sollten Sie entscheiden, welche Ereignisse eine Warnmeldung erfordern.

  Wenn Sie einen Ereignisschweregrad auswählen, aber keine einzelnen Ereignisse auswählen (wenn Sie die Spalte „Ausgewählte Ereignisse“ leer lassen), erhalten Sie Benachrichtigungen für alle Ereignisse in der Kategorie.

- Aktionen

  Sie müssen die Benutzernamen und E-Mail-Adressen der Benutzer angeben, die die Benachrichtigung erhalten. Sie können auch einen SNMP-Trap als Benachrichtigungsmodus festlegen. Sie können Ihre Skripte mit einer Warnung verknüpfen, sodass sie ausgeführt werden, wenn eine Warnung generiert wird.

- Benachrichtigungshäufigkeit

  Sie können einen Alert so konfigurieren, dass für einen festgelegten Zeitraum wiederholt Benachrichtigungen an die Empfänger gesendet werden. Sie sollten den Zeitpunkt festlegen, ab dem die Ereignisbenachrichtigung für den Alert aktiv ist. Wenn die Ereignisbenachrichtigung wiederholt werden soll, bis das Ereignis bestätigt wird, sollten Sie festlegen, wie oft die Benachrichtigung wiederholt werden soll.

- Skript ausführen

  Sie können Ihr Skript mit einer Warnung verknüpfen. Ihr Skript wird ausgeführt, wenn die Warnung generiert wird.

Hinzufügen von Warnmeldungen für Leistungsereignisse in Active IQ Unified Manager

Sie können Benachrichtigungen für einzelne Performance-Ereignisse genauso konfigurieren wie für alle anderen Ereignisse, die von Unified Manager empfangen werden. Wenn Sie außerdem alle Performance-Ereignisse gleich behandeln und E-Mails an dieselbe Person senden möchten, können Sie eine einzelne Benachrichtigung erstellen, die Sie informiert, sobald kritische oder Warnungs-Performance-Ereignisse ausgelöst werden.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Das folgende Beispiel zeigt, wie ein Ereignis für alle kritischen Latenz-, IOPS- und MBps-Ereignisse erstellt wird. Mit derselben Methode können Ereignisse aus allen Performance-Zählern und für alle Warnereignisse ausgewählt werden.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Alarmeinstellungen Hinzufügen** auswählen.

3. Im Dialogfeld **Warnung hinzufügen** auf **Name** klicken und einen Namen sowie eine Beschreibung für die Warnung eingeben.
4. Auf der Seite **Ressourcen** werden keine Ressourcen ausgewählt.

   Da keine Ressourcen ausgewählt sind, gilt die Warnung für alle Cluster, Aggregate, Volumes usw., für die diese Ereignisse empfangen werden.

5. Nach Auswahl von **Events** können die folgenden Aktionen durchgeführt werden:
   a. In der Liste „Ereignisschweregrad“ erfolgt die Auswahl von **Kritisch**.
   b. Im Feld „Ereignisname enthält“ können Sie `latency` eingeben und anschließend auf den Pfeil klicken, um alle übereinstimmenden Ereignisse auszuwählen.
   c. Im Feld „Ereignisname enthält“ `iops` eingeben und anschließend auf den Pfeil klicken, um alle übereinstimmenden Ereignisse auszuwählen.
   d. Im Feld „Ereignisname enthält“ können Sie `mbps` eingeben und dann auf den Pfeil klicken, um alle übereinstimmenden Ereignisse auszuwählen.
6. Unter **Aktionen** folgt im Feld **Diese Benutzer benachrichtigen** die Auswahl des Namens des Benutzers, der die Benachrichtigungs-E-Mail erhalten soll.
7. Auf dieser Seite können Sie alle weiteren Optionen für das Senden von SNMP-Traps und das Ausführen eines Skripts konfigurieren.
8. Auf **Speichern** klicken.

Warnungen in Active IQ Unified Manager testen

Sie können eine Warnung testen, um zu überprüfen, ob Sie sie korrekt konfiguriert haben. Wenn ein Ereignis ausgelöst wird, wird eine Warnung generiert, und eine Warnungs-E-Mail wird an die konfigurierten Empfänger gesendet. Mithilfe der Testwarnung können Sie überprüfen, ob die Benachrichtigung gesendet wird und ob Ihr Skript ausgeführt wird.

Bevor Sie beginnen

- Die Benachrichtigungseinstellungen wie die E-Mail-Adresse der Empfänger, der SMTP-Server und der SNMP-Trap müssen konfiguriert sein.

  Der Unified Manager Server kann diese Einstellungen verwenden, um Benutzern Benachrichtigungen zu senden, wenn ein Ereignis generiert wird.

- Sie müssen ein Skript zugewiesen und dieses so konfiguriert haben, dass es ausgeführt wird, wenn die Warnung generiert wird.
- Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Alert Setup** können Sie den Alert auswählen, der getestet werden soll, und anschließend auf **Test** klicken.

   An die E-Mail-Adressen, die Sie beim Erstellen der Warnung angegeben haben, wird eine Test-E-Mail für Warnungen gesendet.

Benachrichtigungen für gelöste und veraltete Ereignisse in Active IQ Unified Manager deaktivieren

Für alle Ereignisse, für die Sie Benachrichtigungen konfiguriert haben, wird eine Benachrichtigung versendet, wenn diese Ereignisse alle verfügbaren Status durchlaufen: Neu, Erledigt und Veraltet. Wenn Sie keine Benachrichtigungen für Ereignisse erhalten möchten, die in die Status Erledigt und Veraltet wechseln, können Sie eine globale Einstellung konfigurieren, um diese Benachrichtigungen zu unterdrücken.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Standardmäßig werden keine Warnmeldungen für Ereignisse gesendet, wenn diese in den Status „Resolved“ oder „Obsolete“ wechseln.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Benachrichtigungseinstellungen** steht neben dem Element **Benachrichtigungen für behobene und veraltete Ereignisse** ein Schieberegler zur Verfügung, mit dem eine der folgenden Aktionen ausgeführt werden kann:

Zu…	Folgendes ist zu tun…
Benachrichtigungen nicht mehr senden, sobald Ereignisse behoben oder veraltet sind	Den Schieberegler nach links bewegen
Versand von Warnmeldungen, sobald Ereignisse behoben oder obsolet sind	Den Schieberegler nach rechts bewegen

Ausschluss von Ziel-Volumes für die Notfallwiederherstellung von der Generierung von Warnmeldungen in Active IQ Unified Manager

Bei der Konfiguration von Volume-Warnungen können Sie im Warndialogfeld eine Zeichenfolge angeben, die ein Volume oder eine Gruppe von Volumes identifiziert. Wenn Sie jedoch die Notfallwiederherstellung für SVMs konfiguriert haben, haben Quell- und Zielvolume denselben Namen, sodass Sie Warnungen für beide Volumes erhalten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können Warnmeldungen für Disaster-Recovery-Ziel-Volumes deaktivieren, indem Sie Volumes ausschließen, die den Namen der Ziel-SVM tragen. Dies ist möglich, da die Kennung für Volume-Ereignisse sowohl den SVM-Namen als auch den Volume-Namen im Format "<svm_name>:/<volume_name>" enthält.

Das folgende Beispiel zeigt, wie Warnungen für das Volume "vol1" auf der primären SVM "vs1" erstellt werden können, wobei die Generierung der Warnung für ein Volume mit demselben Namen auf der SVM "vs1-dr" ausgeschlossen wird.

Im Dialogfeld „Warnung hinzufügen“ sind die folgenden Schritte auszuführen:

Schritte

1. Unter **Name** lassen sich ein Name und eine Beschreibung für die Warnung eingeben.
2. Nach dem Klick auf **Ressourcen** können Sie die Registerkarte **Einschließen** auswählen.
   a. Nach Auswahl von **Volume** in der Dropdown-Liste ist **`vol1`** in das Feld **Name enthält** einzugeben, damit die Volumes angezeigt werden, deren Name "vol1" enthält.
   b. Sie wählen **<<All Volumes whose name contains 'vol1'>>** im Bereich **Verfügbare Ressourcen** aus und verschieben es in den Bereich **Ausgewählte Ressourcen**.
3. Die Registerkarte **Ausschließen** auswählen, **Volume** auswählen, **`vs1-dr`** in das Feld **Name enthält** eingeben und anschließend auf **Hinzufügen** klicken.

   Dadurch wird verhindert, dass für das Volume "vol1" auf der SVM "vs1-dr" eine Warnung generiert wird.
4. Nach dem Klicken auf **Events** können Sie das Ereignis bzw. die Ereignisse auswählen, das bzw. die Sie auf das Volume bzw. die Volumes anwenden möchten.
5. Unter **Aktionen** folgt im Feld **Diese Benutzer benachrichtigen** die Auswahl des Namens des Benutzers, der die Benachrichtigungs-E-Mail erhalten soll.
6. Auf dieser Seite können alle weiteren Optionen zum Ausgeben von SNMP-Traps und zum Ausführen eines Skripts konfiguriert werden; anschließend kann **Speichern** ausgewählt werden.

Anzeigen von Warnmeldungen in Active IQ Unified Manager

Auf der Seite „Alert Setup“ können Sie die Liste der für verschiedene Ereignisse erstellten Warnmeldungen einsehen. Dort finden Sie auch Eigenschaften der Warnmeldungen wie die Beschreibung, die Benachrichtigungsmethode und -häufigkeit, die Ereignisse, die die Warnmeldung auslösen, die E-Mail-Empfänger der Warnmeldungen sowie betroffene Ressourcen wie Cluster, Aggregate und Volumes.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritt

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.

   Die Liste der Warnmeldungen wird auf der Seite „Benachrichtigungseinrichtung“ angezeigt.

Benachrichtigungen in Active IQ Unified Manager bearbeiten

Sie können Alarmeigenschaften bearbeiten, wie z. B. die Ressource, mit der der Alarm verknüpft ist, Ereignisse, Empfänger, Benachrichtigungsoptionen, Benachrichtigungshäufigkeit und zugehörige Skripte.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Alert Setup** die zu bearbeitende Benachrichtigung auswählen und auf **Edit** klicken.
3. Im Dialogfeld **Warnung bearbeiten** können Sie die Abschnitte Name, Ressourcen, Ereignisse und Aktionen nach Bedarf bearbeiten.

Sie können das mit der Warnung verknüpfte Skript ändern oder entfernen.

4. Auf **Speichern** klicken.

Warnmeldungen in Active IQ Unified Manager löschen

Sie können eine Warnung löschen, wenn sie nicht mehr benötigt wird. Beispielsweise können Sie eine Warnung löschen, die für eine bestimmte Ressource erstellt wurde, wenn diese Ressource nicht mehr von Unified Manager überwacht wird.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Benachrichtigungseinstellungen** die zu löschenden Benachrichtigungen auswählen und auf **Löschen** klicken.
3. Mit **Ja** wird die Löschanfrage bestätigt.

Beschreibung von Warnfenstern und Dialogfeldern

Informationen zur Seite „Warnungseinrichtung“ in Active IQ Unified Manager

Die Seite „Alert Setup“ zeigt eine Liste der Warnmeldungen an und bietet Informationen zum Namen, Status, zur Benachrichtigungsmethode und zur Benachrichtigungshäufigkeit der Warnmeldung. Auf dieser Seite können außerdem Warnmeldungen hinzugefügt, bearbeitet, entfernt, aktiviert oder deaktiviert werden.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Befehlsschaltflächen

- **Hinzufügen**

  Das Dialogfeld „Warnung hinzufügen“ wird angezeigt, in dem neue Warnungen hinzugefügt werden können.

- **Bearbeiten**

  Das Dialogfeld „Warnung bearbeiten“ wird angezeigt, in dem ausgewählte Warnungen bearbeitet werden können.

- **Löschen**

  Ausgewählte Warnmeldungen löschen.

- **Aktivieren**

  Ermöglicht das Versenden von Benachrichtigungen für die ausgewählten Alarme.

- **Deaktivieren**

Deaktiviert die ausgewählten Warnmeldungen, wenn Benachrichtigungen vorübergehend nicht gesendet werden sollen.

- **Test**

  Dient zur Überprüfung der Konfiguration der ausgewählten Warnmeldungen nach dem Hinzufügen oder Bearbeiten.

- **Benachrichtigungen über behobene und veraltete Ereignisse**

  Damit lässt sich festlegen, ob Benachrichtigungen gesendet werden, wenn Ereignisse in die Status „Behoben“ oder „Veraltet“ verschoben werden. Dies kann dazu beitragen, dass Benutzer keine unnötigen Benachrichtigungen erhalten.

Listenansicht

Die Listenansicht zeigt Informationen zu den erstellten Warnmeldungen in tabellarischer Form an. Mithilfe der Spaltenfilter können Sie die angezeigten Daten anpassen. Außerdem können Sie eine Warnmeldung auswählen, um im Detailbereich weitere Informationen dazu anzuzeigen.

- **Status**

  Gibt an, ob eine Warnung aktiviert ( ) oder deaktiviert ( ) ist.

- **Alarm**

  Zeigt den Namen der Warnung an.

- **Beschreibung**

  Zeigt eine Beschreibung der Warnung an.

- **Benachrichtigungsmethode**

  Zeigt die für die Warnung ausgewählte Benachrichtigungsmethode an. Sie können Benutzer per E-Mail oder SNMP-Traps benachrichtigen.

- **Benachrichtigungshäufigkeit**

  Legt die Häufigkeit (in Minuten) fest, mit der der Verwaltungsserver weiterhin Benachrichtigungen sendet, bis das Ereignis bestätigt oder behoben ist oder den Status „Veraltet“ erhält.

Detailbereich

Der Detailbereich enthält weitere Informationen zur ausgewählten Warnung.

- **Alarmname**

  Zeigt den Namen der Warnung an.

- **Warnungsbeschreibung**

  Zeigt eine Beschreibung der Warnung an.

- **Ereignisse**

Zeigt die Ereignisse an, für die Sie eine Benachrichtigung auslösen möchten.

- **Ressourcen**

  Zeigt die Ressourcen an, für die die Warnmeldung ausgelöst werden soll.

- **Beinhaltet**

  Zeigt die Ressourcengruppe an, für die die Warnung ausgelöst werden soll.

- **Ausgenommen**

  Zeigt die Gruppe von Ressourcen an, für die Sie keine Warnung auslösen möchten.

- **Benachrichtigungsmethode**

  Anzeige der Benachrichtigungsmethode für die Warnung.

- **Benachrichtigungshäufigkeit**

  Zeigt an, wie häufig der Managementserver weiterhin Warnmeldungen sendet, bis das Ereignis bestätigt, behoben oder in den Status „Obsolete“ verschoben wird.

- **Skriptname**

  Zeigt den Namen des Skripts an, das mit der ausgewählten Warnung verknüpft ist. Dieses Skript wird ausgeführt, wenn eine Warnung generiert wird.

- **E-Mail-Empfänger**

  Zeigt die E-Mail-Adressen der Benutzer an, die die Warnungsbenachrichtigung erhalten.

Informationen zum Dialogfeld „Warnung hinzufügen“ in Active IQ Unified Manager

Sie können Warnmeldungen erstellen, die Sie benachrichtigen, wenn ein bestimmtes Ereignis generiert wird, sodass Sie das Problem schnell beheben und die Auswirkungen auf Ihre Umgebung minimieren können. Sie können Warnmeldungen für eine einzelne Ressource oder eine Gruppe von Ressourcen sowie für Ereignisse eines bestimmten Typs des Schweregrads erstellen. Außerdem können Sie die Benachrichtigungsmethode und -häufigkeit der Warnmeldungen festlegen.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Name

In diesem Bereich können Sie einen Namen und eine Beschreibung für die Warnmeldung angeben:

- **Alarmname**

  Damit können Sie einen Alert-Namen angeben.

- **Warnungsbeschreibung**

  Ermöglicht Ihnen, eine Beschreibung für die Warnung anzugeben.

Ressourcen

In diesem Bereich können Sie einzelne Ressourcen auswählen oder die Ressourcen anhand einer dynamischen Regel gruppieren, für die eine Warnung ausgelöst werden soll. Eine dynamische Regel ist die Menge an Ressourcen, die anhand des von Ihnen angegebenen Text-Strings gefiltert wird. Sie können nach Ressourcen suchen, indem Sie einen Ressourcentyp aus der Dropdown-Liste auswählen, oder Sie können den genauen Ressourcennamen angeben, um eine bestimmte Ressource anzuzeigen.

Wenn Sie eine Benachrichtigung auf einer der Detailseiten eines Storage Objekts erstellen, wird das Storage Objekt automatisch in die Benachrichtigung aufgenommen.

- **Enthalten**

  Ermöglicht das Einschließen der Ressourcen, für die Warnungen ausgelöst werden sollen. Es kann ein Text-String angegeben werden, um Ressourcen zu gruppieren, die mit diesem String übereinstimmen, und diese Gruppe kann für die Warnung eingeschlossen werden. Beispielsweise können alle Volumes gruppiert werden, deren Name den String „abc“ enthält.

- **Ausschließen**

  Ermöglicht das Ausschließen von Ressourcen, für die keine Warnmeldungen ausgelöst werden sollen. Beispielsweise können Sie alle Volumes ausschließen, deren Name die Zeichenfolge „xyz“ enthält.

  Die Registerkarte „Ausschließen“ wird nur angezeigt, wenn Sie alle Ressourcen eines bestimmten Ressourcentyps auswählen: zum Beispiel <<All Volumes>> oder <<All Volumes whose name contains 'xyz'>>.

  Wenn eine Ressource sowohl den von Ihnen angegebenen Einschluss- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschlussregel, und für das Ereignis wird keine Warnung generiert.

Veranstaltungen

In diesem Bereich können Sie die Ereignisse auswählen, für die Sie die Warnmeldungen erstellen möchten. Sie können Warnmeldungen für Ereignisse auf der Grundlage eines bestimmten Schweregrads oder für eine Reihe von Ereignissen erstellen.

Um mehr als ein Ereignis auszuwählen, sollten Sie während der Auswahl die Strg-Taste gedrückt halten.

- **Ereignisschweregrad**

  Damit können Sie Ereignisse anhand des Typs des Schweregrads auswählen, der Kritisch, Fehler oder Warnung sein kann.

- **Ereignisname enthält**

  Ermöglicht die Auswahl von Ereignissen, deren Name bestimmte Zeichen enthält.

Aktionen

In diesem Bereich können Sie die Benutzer festlegen, die benachrichtigt werden sollen, wenn ein Alarm ausgelöst wird. Außerdem können Sie die Benachrichtigungsmethode und die Benachrichtigungshäufigkeit festlegen.

- **Benachrichtigung dieser Benutzer**

Damit können Sie die E-Mail-Adresse oder den Benutzernamen des Benutzers angeben, der Benachrichtigungen erhalten soll.

Wenn Sie die für den Benutzer hinterlegte E-Mail-Adresse ändern und die Benachrichtigung erneut zum Bearbeiten öffnen, bleibt das Namensfeld leer, da die geänderte E-Mail-Adresse nicht mehr dem zuvor ausgewählten Benutzer zugeordnet ist. Auch wenn Sie die E-Mail-Adresse des ausgewählten Benutzers auf der Seite „Benutzer“ geändert haben, wird die geänderte E-Mail-Adresse für den ausgewählten Benutzer nicht aktualisiert.

- **Benachrichtigungshäufigkeit**

  Ermöglicht es Ihnen, die Häufigkeit festzulegen, mit der der Management-Server Benachrichtigungen sendet, bis das Ereignis bestätigt, behoben oder in den Status „veraltet“ verschoben wird.

  Sie können zwischen folgenden Benachrichtigungsmethoden wählen:

  - Nur einmal benachrichtigen
  - Benachrichtigung mit einer festgelegten Häufigkeit
  - Benachrichtigung mit einer festgelegten Häufigkeit innerhalb des angegebenen Zeitraums

- **SNMP-Trap senden**

  Durch Aktivieren dieses Kontrollkästchens können Sie festlegen, ob SNMP-Traps an den global konfigurierten SNMP-Host gesendet werden sollen.

- **Skript ausführen**

  Ermöglicht das Hinzufügen Ihres benutzerdefinierten Skripts zur Warnung. Dieses Skript wird ausgeführt, wenn eine Warnung generiert wird.

> Wenn diese Funktion in der Benutzeroberfläche nicht verfügbar ist, wurde die Funktionalität von Ihrem Administrator deaktiviert. Bei Bedarf kann diese Funktionalität unter **Storage Management** > **Feature Settings** aktiviert werden.

Befehlsschaltflächen

- **Speichern**

  Erstellt eine Warnung und schließt das Dialogfeld.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld.

Bearbeiten der Alarmeigenschaften in Active IQ Unified Manager

Sie können Alarmeigenschaften wie die Ressource, mit der der Alarm verknüpft ist, Ereignisse, Skripte und Benachrichtigungsoptionen bearbeiten.

Name

In diesem Bereich können Sie den Namen und die Beschreibung der Warnung bearbeiten.

- **Alarmname**

Ermöglicht die Bearbeitung des Alert-Namens.

- **Warnungsbeschreibung**

  Ermöglicht Ihnen, eine Beschreibung für die Warnung anzugeben.

- **Alarmzustand**

  Ermöglicht das Aktivieren oder Deaktivieren der Warnung.

Ressourcen

In diesem Bereich können Sie einzelne Ressourcen auswählen oder die Ressourcen anhand einer dynamischen Regel gruppieren, für die Sie die Warnung auslösen möchten. Sie können nach Ressourcen suchen, indem Sie einen Ressourcentyp aus der Dropdown-Liste auswählen, oder Sie können den genauen Ressourcennamen angeben, um eine bestimmte Ressource anzuzeigen.

- **Enthalten**

  Ermöglicht Ihnen, die Ressourcen einzubeziehen, für die Warnungen ausgelöst werden sollen. Sie können einen Text-String angeben, um Ressourcen zu gruppieren, die mit diesem String übereinstimmen, und diese Gruppe zur Aufnahme in die Warnung auswählen. Beispielsweise können Sie alle Volumes gruppieren, deren Name den String “vol0” enthält.

- **Ausschließen**

  Ermöglicht das Ausschließen von Ressourcen, für die keine Warnmeldungen ausgelöst werden sollen. Beispielsweise können alle Volumes ausgeschlossen werden, deren Name die Zeichenfolge „`xyz`“ enthält.

> Die Registerkarte „Ausschließen“ wird nur angezeigt, wenn Sie alle Ressourcen eines bestimmten Ressourcentyps auswählen, zum Beispiel <<All Volumes>> oder <<All Volumes whose name contains 'xyz'>>.

Veranstaltungen

In diesem Bereich können Sie die Ereignisse auswählen, für die Benachrichtigungen ausgelöst werden sollen. Sie können Benachrichtigungen für Ereignisse basierend auf einem bestimmten Schweregrad oder für eine Gruppe von Ereignissen auslösen.

- **Ereignisschweregrad**

  Damit können Sie Ereignisse anhand des Typs des Schweregrads auswählen, der Kritisch, Fehler oder Warnung sein kann.

- **Ereignisname enthält**

  Ermöglicht die Auswahl von Ereignissen, deren Name die angegebenen Zeichen enthält.

Aktionen

In diesem Bereich können Sie die Benachrichtigungsmethode und die Benachrichtigungshäufigkeit festlegen.

- **Benachrichtigung dieser Benutzer**

  Hier können Sie die E-Mail-Adresse oder den Benutzernamen bearbeiten oder eine neue E-Mail-Adresse

oder einen neuen Benutzernamen angeben, um Benachrichtigungen zu erhalten.

- **Benachrichtigungshäufigkeit**

  Damit lässt sich die Häufigkeit bearbeiten, mit der der Management-Server Benachrichtigungen sendet, bis das Ereignis bestätigt, behoben oder in den Status „Veraltet“ verschoben wird.

  Sie können zwischen folgenden Benachrichtigungsmethoden wählen:

  - Nur einmal benachrichtigen
  - Benachrichtigung mit einer festgelegten Häufigkeit
  - Benachrichtigung mit einer festgelegten Häufigkeit innerhalb des angegebenen Zeitraums

- **SNMP-Trap senden**

  Damit können Sie festlegen, ob SNMP-Traps an den global konfigurierten SNMP-Host gesendet werden sollen.

- **Skript ausführen**

  Ermöglicht es Ihnen, ein Skript mit der Warnung zu verknüpfen. Dieses Skript wird beim Generieren einer Warnung ausgeführt.

Befehlsschaltflächen

- **Speichern**

  Speichert die Änderungen und schließt das Dialogfeld.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld.

Skripte managen

Skripte in Active IQ Unified Manager verwalten

Sie können Skripte verwenden, um mehrere Storage Objekte in Unified Manager automatisch zu ändern oder zu aktualisieren. Das Skript ist mit einer Warnung verknüpft. Wenn ein Ereignis eine Warnung auslöst, führt Unified Manager das Skript aus. Sie können benutzerdefinierte Skripte hochladen und ihre Ausführung beim Erstellen einer Warnung testen.

Das Hochladen und Ausführen von Skripten in Unified Manager ist standardmäßig aktiviert. Falls Ihr Unternehmen diese Funktion aus Sicherheitsgründen nicht zulassen möchte, können Sie sie unter **Speicherverwaltung** > **Funktionseinstellungen** deaktivieren.

Verwandte Informationen

"Aktivieren und Deaktivieren der Möglichkeit zum Hochladen von Skripten"

Wie Skripte mit Warnmeldungen in Active IQ Unified Manager funktionieren

Sie können Ihrem Skript eine Warnung zuordnen, sodass das Skript ausgeführt wird, wenn in Unified Manager für ein Ereignis eine Warnung ausgelöst wird. Mithilfe der Skripte lassen sich Probleme mit Storage Objekten beheben oder die Storage Objekte identifizieren, die die Ereignisse generieren.

Wenn in Unified Manager eine Warnung für ein Ereignis generiert wird, wird eine Benachrichtigungs-E-Mail an die angegebenen Empfänger gesendet. Wenn Sie einer Warnung ein Skript zugeordnet haben, wird das Skript ausgeführt. Die Details der an das Skript übergebenen Argumente sind in der Benachrichtigungs-E-Mail enthalten.

Wenn Sie ein benutzerdefiniertes Skript erstellt und es einer Warnung für einen bestimmten Ereignistyp zugeordnet haben, richten sich die Maßnahmen für diesen Ereignistyp nach Ihrem benutzerdefinierten Skript, und die **Fix it**-Aktionen sind standardmäßig auf der Seite „Management Actions“ oder im Unified Manager Dashboard nicht verfügbar.

Das Skript verwendet für die Ausführung die folgenden Argumente:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Sie können die Argumente in Ihren Skripten verwenden sowie zugehörige Ereignisinformationen erfassen oder Storage Objekte ändern.

Beispiel für das Abrufen von Argumenten aus Skripten

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

Wenn eine Warnmeldung generiert wird, führt das System dieses Skript aus, und die folgende Ausgabe wird angezeigt:

```
-`eventID : 290`
-`eventSourceID : 4138`
```

Skripte in Active IQ Unified Manager hinzufügen

Sie können in Unified Manager Skripte hinzufügen und diese mit Warnmeldungen verknüpfen. Diese Skripte werden automatisch ausgeführt, wenn eine Warnmeldung generiert wird, und ermöglichen es Ihnen, Informationen zu den Storage Objekten abzurufen, für die das Ereignis generiert wird.

Bevor Sie beginnen

- Sie müssen die Skripte, die Sie dem Unified Manager Server hinzufügen möchten, erstellt und gespeichert haben.
- Die unterstützten Dateiformate für Skripte sind Perl, Shell, PowerShell, Python und `.bat`Dateien.

Plattform, auf der Unified Manager installiert ist	Unterstützte Sprachen
VMware	Perl- und Shell-Skripte
Linux	Perl, Python und Shell Skripte
Windows	PowerShell, Perl-, Python- und .bat-Skripte

  - Für Perl Skripte muss Perl auf dem Unified Manager Server installiert sein. Bei VMware Installationen ist Perl 5 standardmäßig installiert, und die Skripte unterstützen nur die von Perl 5 unterstützten Funktionen. Wenn Perl nach Unified Manager installiert wurde, muss der Unified Manager Server neu gestartet werden.
  - Für PowerShell-Skripte muss auf dem Windows-Server die entsprechende PowerShell-Ausführungsrichtlinie festgelegt werden, damit die Skripte ausgeführt werden können.

> Wenn Ihr Skript Protokolldateien erstellt, um den Fortschritt des Alarmskripts zu verfolgen, müssen Sie sicherstellen, dass sich die Protokolldateien nicht irgendwo im Unified Manager Installationsordner befinden.

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können benutzerdefinierte Skripte hochladen und Ereignisdetails zur Warnung erfassen.

> Wenn diese Funktion in der Benutzeroberfläche nicht verfügbar ist, wurde die Funktionalität von Ihrem Administrator deaktiviert. Bei Bedarf kann diese Funktionalität unter **Storage Management** > **Feature Settings** aktiviert werden.

Schritte

1. Im linken Navigationsbereich wird **Storage Management** > **Scripts** ausgewählt.
2. Auf der Seite **Skripte** erfolgt die Auswahl von **Hinzufügen**.
3. Im Dialogfeld **Skript hinzufügen** wird mit **Durchsuchen** die Skriptdatei ausgewählt.
4. Geben Sie für das ausgewählte Skript eine Beschreibung ein.
5. Klicken Sie auf **Add**.

Verwandte Informationen

"Aktivieren und Deaktivieren der Möglichkeit zum Hochladen von Skripten"

Skripte in Active IQ Unified Manager löschen

Sie können ein Skript aus dem Unified Manager löschen, wenn das Skript nicht mehr benötigt wird oder ungültig ist.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Das Skript darf nicht mit einer Warnmeldung verknüpft sein.

Schritte

1. Im linken Navigationsbereich wird **Storage Management** > **Scripts** ausgewählt.
2. Auf der Seite **Skripte** wählen Sie das Skript aus, das Sie löschen möchten, und klicken dann auf **Löschen**.
3. Die Bestätigung der Löschung erfolgt im Dialogfeld **Warning** durch Klicken auf **Yes**.

Ausführung des Testskripts in Active IQ Unified Manager

Sie können überprüfen, ob Ihr Skript korrekt ausgeführt wird, wenn eine Warnung für ein Storage-Objekt generiert wird.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen ein Skript im unterstützten Dateiformat in Unified Manager hochgeladen haben.

Schritte

1. Im linken Navigationsbereich wird **Storage Management** > **Scripts** ausgewählt.
2. Auf der Seite **Skripte** können Sie Ihr Testskript hinzufügen.
3. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
4. Auf der Seite **Alert Setup** können Sie eine der folgenden Aktionen auswählen:

Zu…	Folgendes ist zu tun…
Hinzufügen einer Benachrichtigung	a. Klicken Sie auf **Add**. b. Im Abschnitt „Aktionen“ können Sie die Warnung Ihrem Testskript zuordnen.
Eine Warnmeldung bearbeiten	a. Eine Benachrichtigung auswählen und dann auf **Bearbeiten** klicken. b. Im Abschnitt „Aktionen“ können Sie die Warnung Ihrem Testskript zuordnen.

5. Auf **Speichern** klicken.
6. Auf der Seite **Alert Setup** den hinzugefügten oder geänderten Alarm auswählen und anschließend auf **Test** klicken.

   Das Skript wird mit dem Argument "-test" ausgeführt, und eine Benachrichtigungswarnung wird an die E-Mail-Adressen gesendet, die beim Erstellen der Warnung angegeben wurden.

Informationen zu den unterstützten Active IQ Unified Manager CLI Befehlen

Als Storage Administrator können Sie mithilfe der CLI-Befehle Abfragen für die Storage Objekte ausführen, beispielsweise für Cluster, Aggregate, Volumes, qtrees und LUNs. Sie können die CLI-Befehle auch verwenden, um die interne Datenbank von Unified Manager und die ONTAP Datenbank abzufragen. Darüber hinaus können Sie CLI-Befehle in Skripten verwenden, die zu Beginn oder am Ende eines Vorgangs ausgeführt werden oder wenn eine Warnung ausgelöst wird.

Allen Befehlen müssen der Befehl `um cli login` sowie ein gültiger Benutzername und ein gültiges Passwort für die Authentifizierung vorangestellt werden.

Zum Ausführen des Befehls *um run* benötigt Ihr Konto Zugriff auf die Applikation *console*.

CLI Befehl	Beschreibung	Ausgabe
`um cli login -u <username> [-p <password>]`	Dient zur Anmeldung an der CLI. Aus Sicherheitsgründen sollten Sie nach der Option „-u“ nur den Benutzernamen angeben. Bei dieser Verwendung werden Sie zur Eingabe des Passworts aufgefordert, und das Passwort wird weder im Verlauf noch in der Prozesstabelle erfasst. Die Sitzung läuft drei Stunden nach der Anmeldung ab; danach muss sich der Benutzer erneut anmelden.	Zeigt die entsprechende Meldung an.
`um cli logout`	Meldet den Benutzer von der CLI ab.	Zeigt die entsprechende Meldung an.
`um help`	Zeigt alle Unterbefehle des ersten Levels an.	Zeigt alle Unterbefehle des ersten Levels an.
`um run cmd [ -t <timeout> ] <cluster> <command>`	Die einfachste Methode, einen Befehl auf einem oder mehreren Hosts auszuführen. Wird hauptsächlich für Alarmskripte verwendet, um auf ONTAP einen Vorgang abzurufen oder auszuführen. Das optionale Argument Zeitüberschreitung legt ein maximales Zeitlimit (in Sekunden) fest, innerhalb dessen der Befehl auf dem Client abgeschlossen werden muss. Der Standardwert ist 0 (unbegrenzt warten).	Wie von ONTAP empfangen.

CLI Befehl	Beschreibung	Ausgabe
`um run query <sql command>`	Führt eine SQL-Abfrage aus. Es sind nur Abfragen zulässig, die Daten aus der Datenbank lesen. Aktualisierungs-, Einfüge- oder Löschvorgänge werden nicht unterstützt.	Die Ergebnisse werden in Tabellenform angezeigt. Bei einer leeren Ergebnismenge sowie bei Syntaxfehlern oder fehlerhaften Anfragen wird die entsprechende Fehlermeldung angezeigt.
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Fügt der Liste der verwalteten Storage Systeme eine Datenquelle hinzu. Eine Datenquelle beschreibt, wie Verbindungen zu Storage Systemen hergestellt werden. Beim Hinzufügen einer Datenquelle müssen die Optionen -u (Benutzername) und -P (Passwort) angegeben werden. Die Option -t (Protokoll) gibt das Protokoll an, das für die Kommunikation mit dem Cluster verwendet wird (http oder https). Wird kein Protokoll angegeben, werden beide Protokolle versucht. Die Option -p (Port) gibt den Port an, der für die Kommunikation mit dem Cluster verwendet wird. Wird kein Port angegeben, wird der Standardwert des entsprechenden Protokolls versucht. Dieser Befehl kann nur vom storage admin ausgeführt werden.	Das System fordert den Benutzer auf, das Zertifikat zu akzeptieren, und gibt die entsprechende Meldung aus.
`um datasource list [ <datasource-id>]`	Zeigt die Datenquellen für verwaltete Storage Systeme an.	Zeigt die folgenden Werte in Tabellenform an: `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.`
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	Ändert eine oder mehrere Datenquellenoptionen. Kann nur vom Storage-Administrator ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um datasource remove <datasource-id>`	Entfernt die Datenquelle (Cluster) aus Unified Manager.	Zeigt die entsprechende Meldung an.
`um option list [ <option> .. ]`	Dies ist eine Auflistung aller Optionen, die Sie mit dem Befehl „set“ konfigurieren können.	Zeigt die folgenden Werte in Tabellenform an: `Name, Value, Default Value, and Requires Restart.`

CLI Befehl	Beschreibung	Ausgabe
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	Legt eine oder mehrere Optionen fest. Nur der Storage-Administrator kann den Befehl ausführen.	Zeigt die entsprechende Meldung an.
`um version`	Zeigt die Unified Manager Softwareversion an.	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	Listet die LUNs nach dem Filtern nach dem angegebenen Objekt auf. -q ist für alle Befehle anwendbar, um keine Kopfzeile anzuzeigen. ObjectType kann lun, qtree, cluster, volume, quota oder svm sein. Beispiel: **`um lun list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle LUNs innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform an: `ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	Listet die Storage VMs nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann lun, qtree, cluster, volume, quota oder svm sein. Beispiel: **`um svm list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Storage VMs innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform an: `Name and Cluster ID.`

CLI Befehl	Beschreibung	Ausgabe
`um qtree list [-q] [ -ObjectType <object-id>]`	Listet die Qtrees nach dem Filtern nach dem angegebenen Objekt auf. Die Option `-q` ist für alle Befehle anwendbar, um keine Kopfzeile anzuzeigen. ObjectType kann lun, qtree, cluster, volume, quota oder svm sein. Beispiel: **`um qtree list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Qtrees innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform an: `Qtree ID and Qtree Name.`
`um disk list [-q] [-ObjectType <object-id>]`	Listet die Datenträger nach dem Filtern anhand des angegebenen Objekts auf. ObjectType kann disk, aggr, node oder cluster sein. Beispiel: **`um disk list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Festplatten innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform an `ObjectType and object-id`.
`um cluster list [-q] [-ObjectType <object-id>]`	Listet die Cluster nach dem Filtern anhand des angegebenen Objekts auf. ObjectType kann disk, aggr, node, cluster, lun, qtree, volume, quota oder svm sein. Beispiel: **`um cluster list -aggr 1`** In diesem Beispiel ist "-aggr" der objectType und "1" die objectId. Der Befehl zeigt den Cluster an, zu dem das Aggregat mit der ID 1 gehört.	Zeigt die folgenden Werte in Tabellenform an: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.`

CLI Befehl	Beschreibung	Ausgabe
`um cluster node list [-q] [-ObjectType <object-id>]`	Zeigt die Clusterknoten nach der Filterung auf das angegebene Objekt an. ObjectType kann disk, aggr, node oder cluster sein. Beispiel: **`um cluster node list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Knoten innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform an `Name and Cluster ID`.
`um volume list [-q] [-ObjectType <object-id>]`	Listet die Volumes nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann lun, qtree, cluster, volume, quota, svm oder aggregate sein. Beispiel: **`um volume list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Volumes innerhalb des Clusters mit der ID 1 auf.	Die folgenden Werte werden in Tabellenform angezeigt `Volume ID and Volume Name`.
`um quota user list [-q] [-ObjectType <object-id>]`	Listet die Quota-Benutzer nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann qtree, cluster, volume, quota oder svm sein. Beispiel: **`um quota user list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Kontingentbenutzer innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in Tabellenform `ID, Name, SID and Email`.

CLI Befehl	Beschreibung	Ausgabe
`um aggr list [-q] [-ObjectType <object-id>]`	Listet die Aggregate nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann disk, aggr, node, cluster oder volume sein. Beispiel: **`um aggr list -cluster 1`** In diesem Beispiel ist "-cluster" der objectType und "1" die objectId. Der Befehl listet alle Aggregate innerhalb des Clusters mit der ID 1 auf.	Die folgenden Werte werden in Tabellenform angezeigt `Aggr ID, and Aggr Name`.
`um event ack <event-ids>`	Bestätigt ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event resolve <event-ids>`	Behebt ein oder mehrere Ereignisse.	Zeigt die entsprechende Meldung an.
`um event assign -u <username> <event-id>`	Weist einem Benutzer ein Ereignis zu.	Zeigt die entsprechende Meldung an.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Listet die vom System oder Benutzer generierten Ereignisse auf. Filtert Ereignisse anhand von Quelle, Status und IDs.	Zeigt die folgenden Werte in Tabellenform an `Source, Source type, Name, Severity, State, User and Timestamp`.
`um backup restore -f <backup_file_path_and_name>`	Stellt eine MySQL Datenbanksicherung mithilfe von .7z-Dateien wieder her.	Zeigt die entsprechende Meldung an.

Beschreibung der Skriptfenster und Dialogfelder

Informationen zur Seite „Skripte“ in Active IQ Unified Manager

Die Seite „Skripte“ ermöglicht es Ihnen, Ihre benutzerdefinierten Skripte zu Unified Manager hinzuzufügen. Sie können diese Skripte mit Warnmeldungen verknüpfen, um die automatische Neukonfiguration von Storage Objekten zu ermöglichen.

Auf der Seite „Skripte“ lassen sich Skripte in Unified Manager hinzufügen oder löschen.

Befehlsschaltflächen

- **Hinzufügen**

  Zeigt das Dialogfeld „Skript hinzufügen“ an, in dem Skripte hinzugefügt werden können.

- **Löschen**

  Löscht das ausgewählte Skript.

Listenansicht

Die Listenansicht zeigt die Skripte, die Sie zu Unified Manager hinzugefügt haben, in Tabellenform an.

- **Name**

  Zeigt den Namen des Skripts an.

- **Beschreibung**

  Zeigt die Beschreibung des Skripts an.

Dialogfeld „Skript hinzufügen“ in Active IQ Unified Manager

Im Dialogfeld „Skript hinzufügen“ können Sie Skripte zu Unified Manager hinzufügen. Sie können Warnungen mit Ihren Skripten so konfigurieren, dass Ereignisse, die für Storage Objekte generiert werden, automatisch behoben werden.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

- **Auswahl der Skriptdatei**

  Ermöglicht die Auswahl eines Skripts für die Warnmeldung.

- **Beschreibung**

  Hier können Sie eine Beschreibung für das Skript angeben.

Cluster Performance überwachen und managen

Einführung in die Performance-Überwachung mit Active IQ Unified Manager

Informationen zur Leistungsüberwachung in Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) bietet Funktionen zur Performance-Überwachung und zur Ursachenanalyse von Ereignissen für Systeme, auf denen NetApp ONTAP-Software ausgeführt wird.

Unified Manager hilft Ihnen, Workloads zu identifizieren, die Clusterkomponenten übermäßig beanspruchen und die Performance anderer Workloads im Cluster beeinträchtigen. Durch das Definieren von Performance-Schwellenwertrichtlinien können Sie auch Maximalwerte für bestimmte Performance-Zähler festlegen, sodass Ereignisse generiert werden, wenn der Schwellenwert überschritten wird. Unified Manager benachrichtigt Sie über diese Performance-Ereignisse, damit Sie eine Korrekturmaßnahme ergreifen und die Performance wieder auf ein normales Betriebsniveau bringen können. Sie können Ereignisse in der Unified Manager UI anzeigen und analysieren.

Unified Manager überwacht die Performance von zwei Arten von Arbeitslasten:

- Benutzerdefinierte Arbeitslasten

  Diese Workloads bestehen aus FlexVol Volumes und FlexGroup Volumes, die Sie in Ihrem Cluster erstellt haben.

- Systemdefinierte Workloads

  Diese Arbeitslasten bestehen aus internen Systemaktivitäten.

Die Leistungsüberwachungsfunktionen von Active IQ Unified Manager können erkundet werden.

Unified Manager erfasst und analysiert Performance-Statistiken von Systemen, auf denen ONTAP Software ausgeführt wird. Er verwendet dynamische Performance-Schwellenwerte und benutzerdefinierte Performance-Schwellenwerte, um eine Vielzahl von Performance-Zählern über viele Clusterkomponenten hinweg zu überwachen.

Eine hohe Antwortzeit (Latenz) deutet darauf hin, dass das Storage-Objekt, beispielsweise ein Volume, langsamer als üblich arbeitet. Dies weist außerdem darauf hin, dass sich die Performance von Clientanwendungen verringert hat, die das Volume nutzen. Unified Manager identifiziert die Storage-Komponente, in der das Performance-Problem liegt, und bietet eine Liste mit Handlungsempfehlungen zur Behebung des Performance-Problems.

Unified Manager umfasst folgende Funktionen:

- Überwacht und analysiert Performance Statistiken von Workloads aus einem System, auf dem ONTAP software ausgeführt wird.
- Erfasst Performance-Zähler für Cluster, Knoten, Aggregate, Ports, SVMs, Volumes, LUNs, NVMe-Namespaces und Netzwerkschnittstellen (LIFs).

- Zeigt detaillierte Diagramme an, die die Workload-Aktivität im Zeitverlauf darstellen, einschließlich IOPS (Operationen), MB/s (Durchsatz), Latenz (Antwortzeit), Auslastung, Performance-Kapazität und Cache-Verhältnis.
- Ermöglicht die Erstellung benutzerdefinierter Performance-Schwellenwertrichtlinien, die Ereignisse auslösen und E-Mail-Benachrichtigungen senden, wenn die Schwellenwerte überschritten werden.
- Verwendet systemdefinierte Schwellenwerte und dynamische Performance-Schwellenwerte, die die Aktivität Ihrer Workloads erfassen, um Performance-Probleme zu erkennen und Sie darauf aufmerksam zu machen.
- Kennzeichnet die Quality of Service (QoS)-Richtlinien und Performance Service Level-Richtlinien (PSLs), die auf Ihre Volumes und LUNs angewendet werden.
- Identifiziert eindeutig die Clusterkomponente, um die es zu einem Konflikt kommt.
- Identifiziert Workloads, die Clusterkomponenten übermäßig beanspruchen, und Workloads, deren Performance durch die erhöhte Aktivität beeinträchtigt wird.

Mit Active IQ Unified Manager Schnittstellen lässt sich die Leistung des Speichersystems verwalten.

Diese Abschnitte enthalten Informationen zu den beiden Benutzeroberflächen, die Active IQ Unified Manager zur Fehlerbehebung bei Problemen mit Datenspeicherkapazität, Verfügbarkeit und Schutz bereitstellt. Die beiden Benutzeroberflächen sind die Unified Manager Weboberfläche und die Managementplattform.

Wenn Sie die Schutzfunktionen in Unified Manager nutzen möchten, müssen Sie auch OnCommand Workflow Automation (WFA) installieren und konfigurieren.

Unified Manager Web-Benutzeroberfläche

Die Web-Benutzeroberfläche von Unified Manager ermöglicht es einem Administrator, Clusterprobleme im Zusammenhang mit Storage-Kapazität, Verfügbarkeit und Schutz von Daten zu überwachen und zu beheben.

In diesen Abschnitten werden einige gängige Arbeitsabläufe beschrieben, denen ein Administrator folgen kann, um Probleme mit der Storage-Kapazität, der Datenverfügbarkeit oder dem Schutz zu beheben, die in der Unified Manager Weboberfläche angezeigt werden.

Managementplattform

Die Managementplattform von Unified Manager ermöglicht es Administratoren, Betriebssystemprobleme, Probleme bei Versionsaktualisierungen, Benutzerzugriffsprobleme und Netzwerkprobleme im Zusammenhang mit dem Unified Manager Server zu überwachen, zu diagnostizieren und zu beheben. Wenn die Web-Benutzeroberfläche von Unified Manager nicht verfügbar ist, ist die Managementplattform die einzige Zugriffsmöglichkeit auf Unified Manager.

Mithilfe dieser Informationen können Sie auf die Wartungs-Managementplattform zugreifen und damit Probleme im Zusammenhang mit der Funktionsweise des Unified Manager-Servers beheben.

Clusterkonfiguration und Leistungsdaten in Active IQ Unified Manager anzeigen

Das Erfassungsintervall für Clusterkonfigurationsdaten beträgt 15 Minuten. Nachdem Sie beispielsweise einen Cluster hinzugefügt haben, dauert es 15 Minuten, bis die Clusterdetails in der Unified Manager UI angezeigt werden. Dieses Intervall gilt auch für

Änderungen an einem Cluster.

Wenn beispielsweise zwei neue Volumes zu einer SVM in einem Cluster hinzugefügt werden, sind diese neuen Objekte nach dem nächsten Abfrageintervall in der UI sichtbar, was bis zu 15 Minuten dauern kann.

Unified Manager erfasst aktuelle Performance-Statistiken aller überwachten Cluster alle fünf Minuten. Diese Daten werden analysiert, um Performance-Ereignisse und potenzielle Probleme zu identifizieren. 30 Tage lang werden historische Performance-Daten in Fünf-Minuten-Intervallen und 180 Tage lang historische Performance-Daten in Einstunden-Intervallen aufbewahrt. Dadurch lassen sich für den aktuellen Monat sehr granulare Performance-Details und für bis zu ein Jahr allgemeine Performance-Trends anzeigen.

Die Erfassungsabfragen sind um einige Minuten versetzt, sodass Daten nicht von jedem Cluster gleichzeitig gesendet werden, was die Performance beeinträchtigen könnte.

Die folgende Tabelle beschreibt die vom Unified Manager durchgeführten Datenerfassungsaktivitäten:

Aktivität	Zeitintervall	Beschreibung
Abfrage von Performance Statistiken	Alle 5 Minuten	Erfasst Performance-Daten in Echtzeit aus jedem Cluster.
Statistische Analyse	Alle 5 Minuten	Nach jeder Abfrage der Statistiken vergleicht Unified Manager die erfassten Daten mit benutzerdefinierten, systemdefinierten und dynamischen Schwellenwerten. Wenn Schwellenwerte für die Performance überschritten wurden, generiert Unified Manager Ereignisse und sendet E-Mails an bestimmte Benutzer, sofern dies konfiguriert ist.
Konfigurationsabfrage	Alle 15 Minuten	Erfasst detaillierte Inventarinformationen von jedem Cluster, um alle Storage-Objekte (Knoten, SVMs, Volumes usw.) zu identifizieren.
Zusammenfassung	Stündlich	Fasst die letzten 12 fünfminütigen Performance-Datenerfassungen zu stündlichen Durchschnittswerten zusammen. Die stündlichen Durchschnittswerte werden auf einigen Seiten der Benutzeroberfläche verwendet und 180 Tage lang gespeichert.

Aktivität	Zeitintervall	Beschreibung
Prognoseanalyse und Datenbereinigung	Jeden Tag nach Mitternacht	Analysiert Clusterdaten, um für die nächsten 24 Stunden dynamische Schwellenwerte für Volume-Latenz und IOPS festzulegen. Löscht aus der Datenbank alle Fünf-Minuten-Performance-Daten, die älter als 30 Tage sind.
Datenbereinigung	Jeden Tag nach 2 Uhr morgens	Löscht aus der Datenbank alle Ereignisse, die älter als 180 Tage sind, sowie dynamische Schwellenwerte, die älter als 180 Tage sind.
Datenbereinigung	Jeden Tag nach 3:30 Uhr morgens	Löscht aus der Datenbank alle einstündigen Performance-Daten, die älter als 180 Tage sind.

Informationen zu Datenerfassungszyklen für die Datenkontinuität in Active IQ Unified Manager

Ein Datenkontinuitäts-Erfassungszyklus ruft Performance-Daten außerhalb des Echtzeit-Cluster-Performance-Erfassungszyklus ab, der standardmäßig alle fünf Minuten ausgeführt wird. Datenkontinuitäts-Erfassungen ermöglichen es Unified Manager, Lücken in den Statistiken zu schließen, die entstehen, wenn keine Echtzeitdaten erfasst werden konnten.

Unified Manager führt Erfassungsabfragen zur Datenkontinuität für historische Performance-Daten aus, wenn die folgenden Ereignisse eintreten:

- Ein Cluster wird zunächst zu Unified Manager hinzugefügt.

  Unified Manager erfasst historische Performance-Daten der letzten 15 Tage. Dadurch können Sie bereits wenige Stunden nach dem Hinzufügen eines Clusters historische Performance-Informationen für zwei Wochen einsehen.

  Zusätzlich sind, sofern vorhanden, systemdefinierte Schwellenwertereignisse für den vorherigen Zeitraum aufgeführt.

- Der aktuelle Erfassungszyklus für Performance-Daten schließt nicht rechtzeitig ab.

  Wenn die Echtzeit-Performance-Abfrage über den Erfassungszeitraum von fünf Minuten hinausgeht, wird ein Erfassungszyklus für die Datenkontinuität initiiert, um diese fehlenden Informationen zu sammeln. Ohne die Datenerfassung zur Datenkontinuität wird der nächste Erfassungszeitraum übersprungen.

- Unified Manager war zeitweise nicht erreichbar und ist dann wieder online, wie in den folgenden Situationen:
  - Es wurde neu gestartet.
  - Es wurde während eines Software-Upgrades oder beim Erstellen einer Sicherungsdatei heruntergefahren.

    - Ein Netzwerkausfall wurde behoben.
- Ein Cluster war für eine gewisse Zeit nicht erreichbar und ist dann wieder online, wie in den folgenden Situationen:
    - Ein Netzwerkausfall wurde behoben.
    - Eine langsame Wide Area Network Verbindung verzögerte die normale Erfassung von Performancedaten.

Ein Datenkontinuitäts-Erfassungszyklus kann maximal 24 Stunden an historischen Daten erfassen. Wenn Unified Manager länger als 24 Stunden nicht verfügbar ist, entsteht auf den UI-Seiten eine Lücke in den Performance-Daten.

Ein Datenkontinuitäts-Erfassungszyklus und ein Echtzeit-Datenerfassungszyklus können nicht gleichzeitig ausgeführt werden. Der Datenkontinuitäts-Erfassungszyklus muss abgeschlossen sein, bevor die Echtzeit-Performance-Datenerfassung gestartet wird. Wenn bei der Datenkontinuitäts-Erfassung mehr als eine Stunde an Verlaufsdaten erfasst werden muss, wird oben im Benachrichtigungsbereich für diesen Cluster eine Bannermeldung angezeigt.

Informationen zu Zeitstempeln in erfassten Daten und Ereignissen in Active IQ Unified Manager

Der Zeitstempel, der in den erfassten Systemstatus- und Performance-Daten erscheint oder der als Erkennungszeitpunkt für ein Ereignis angezeigt wird, basiert auf der Clusterzeit von ONTAP, angepasst an die im Webbrowser eingestellte Zeitzone.

Es wird dringend empfohlen, einen Network Time Protocol (NTP)-Server zu verwenden, um die Zeit auf Ihren Unified Manager-Servern, ONTAP-Clustern und Webbrowsern zu synchronisieren.

Wenn Zeitstempel für einen bestimmten Cluster falsch erscheinen, ist möglicherweise zu prüfen, ob die Clusterzeit korrekt eingestellt ist.

Navigation in Performance Workflows in der Unified Manager GUI

Navigation durch Performance-Workflows in der Active IQ Unified Manager GUI

Die Unified Manager Oberfläche bietet zahlreiche Seiten zum Erfassen und Anzeigen von Performance Informationen. Der linke Navigationsbereich dient zum Navigieren zu Seiten in der GUI, und Registerkarten und Links auf den Seiten dienen zum Anzeigen und Konfigurieren von Informationen.

Sie verwenden alle folgenden Seiten zur Überwachung und Fehlerbehebung bei Informationen zur Cluster-Performance:

- Dashboard-Seite
- Storage- und Netzwerkobjektinventarseiten
- Detailseiten für Storage-Objekte (einschließlich des Performance Explorers)
- Konfigurations- und Einrichtungsseiten

- Ereignisseiten

Anmeldung bei der Active IQ Unified Manager UI

Sie können sich über einen unterstützten Webbrowser bei der Unified Manager Benutzeroberfläche anmelden.

Bevor Sie beginnen

- Der Webbrowser muss Mindestanforderungen erfüllen.

  Die vollständige Liste der unterstützten Browserversionen finden Sie in der Interoperabilitätsmatrix unter "mysupport.netapp.com/matrix".

- Sie benötigen die IP-Adresse oder URL des Unified Manager Servers.

Sie werden nach 1 Stunde Inaktivität automatisch abgemeldet. Dieser Zeitraum kann unter **Allgemein** > **Funktionseinstellungen** konfiguriert werden.

Schritte

1. Eingabe der URL in den Webbrowser, wobei URL für die IP-Adresse oder den vollqualifizierten Domainnamen (FQDN) des Unified Manager Servers steht:
   - Für IPv4: `https://URL/`
   - Für IPv6: `https://[URL]/`

Wenn der Server ein selbstsigniertes digitales Zertifikat verwendet, zeigt der Browser möglicherweise eine Warnung an, dass das Zertifikat nicht vertrauenswürdig ist. Sie können entweder das Risiko akzeptieren, um den Zugriff fortzusetzen, oder ein von einer Zertifizierungsstelle (CA) signiertes digitales Zertifikat für die Serverauthentifizierung installieren . Auf dem Anmeldebildschirm erfolgt die Eingabe Ihres Benutzernamens und Passworts.

Wenn die Anmeldung bei der Unified Manager Benutzeroberfläche durch SAML Authentifizierung geschützt ist, geben Sie Ihre Anmeldeinformationen auf der Anmeldeseite des Identitätsanbieters (IdP) statt auf der Unified Manager Anmeldeseite ein.

Die Seite „Dashboard“ erscheint.

Wenn der Unified Manager Server nicht initialisiert ist, wird in einem neuen Browserfenster der Einrichtungsassistent angezeigt. Es ist erforderlich, einen ersten E-Mail-Empfänger anzugeben, an den E-Mail-Benachrichtigungen gesendet werden, den SMTP-Server, der die E-Mail-Kommunikation verarbeitet, sowie, ob AutoSupport aktiviert ist, um Informationen zu Ihrer Unified Manager Installation an den technischen Support zu senden. Nach Abschluss dieser Angaben wird die Unified Manager Benutzeroberfläche angezeigt.

Grafische Benutzeroberfläche und Navigationspfade

Die grafische Benutzeroberfläche und die Navigationspfade in Active IQ Unified Manager

Unified Manager bietet hohe Flexibilität und ermöglicht die Erledigung vielfältiger Aufgaben auf unterschiedliche Weise. Im Laufe Ihrer Arbeit mit Unified Manager identifizieren Sie zahlreiche Navigationspfade. Obwohl hier nicht alle möglichen Navigationskombinationen dargestellt werden können, sollten Sie mit einigen der

gängigsten Szenarien vertraut sein.

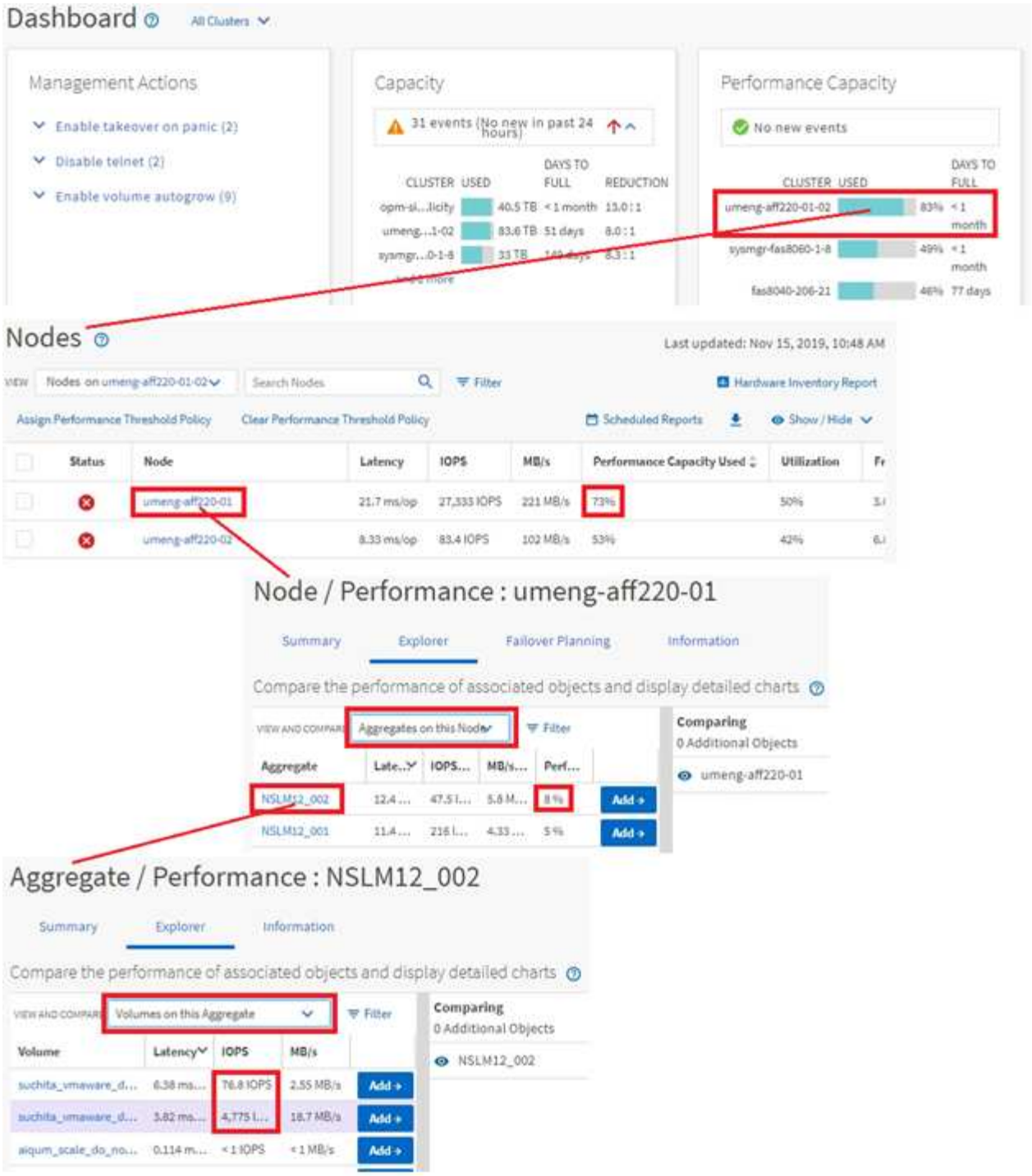
Überwachung der Clusterobjektnavigation in Active IQ Unified Manager

Sie können die Performance aller Objekte in jedem von Unified Manager verwalteten Cluster überwachen. Die Überwachung Ihrer Storage Objekte bietet Ihnen einen Überblick über die Cluster- und Objekt-Performance und umfasst auch die Überwachung von Performance-Ereignissen. Sie können Performance und Ereignisse auf einer hohen Ebene anzeigen oder weitere Details zur Objekt-Performance und zu Performance-Ereignissen untersuchen.

Dies ist ein Beispiel für viele mögliche Navigationen zu Clusterobjekten:

1. Auf der Dashboard-Seite können Sie die Details im Bereich „Performance-Kapazität“ prüfen, um den Cluster zu identifizieren, der die meiste Performance-Kapazität nutzt, und durch Klicken auf das Balkendiagramm zur Liste der Knoten für diesen Cluster navigieren.
2. Der Knoten mit dem höchsten Wert der genutzten Performance-Kapazität ist zu identifizieren und anzuklicken.
3. Auf der Seite „Node / Performance Explorer“ steht im Menü „View and Compare“ die Option **Aggregates on this Node** zur Auswahl.
4. Das Aggregat, das die meiste Performance-Kapazität nutzt, ist zu identifizieren und anzuklicken.
5. Auf der Seite „Aggregate / Performance Explorer“ erfolgt im Menü „View and Compare“ ein Klick auf **Volumes on this Aggregate**.
6. Sie können die Volumes mit den meisten IOPS ermitteln.

Bei diesen Volumes sollte geprüft werden, ob eine QoS-Richtlinie oder eine Performance Service Level Richtlinie angewendet oder die Richtlinieneinstellungen geändert werden sollten, damit diese Volumes nicht einen so großen Prozentsatz der IOPS im Cluster beanspruchen.



Navigation zur Überwachung der Cluster-Performance in Active IQ Unified Manager

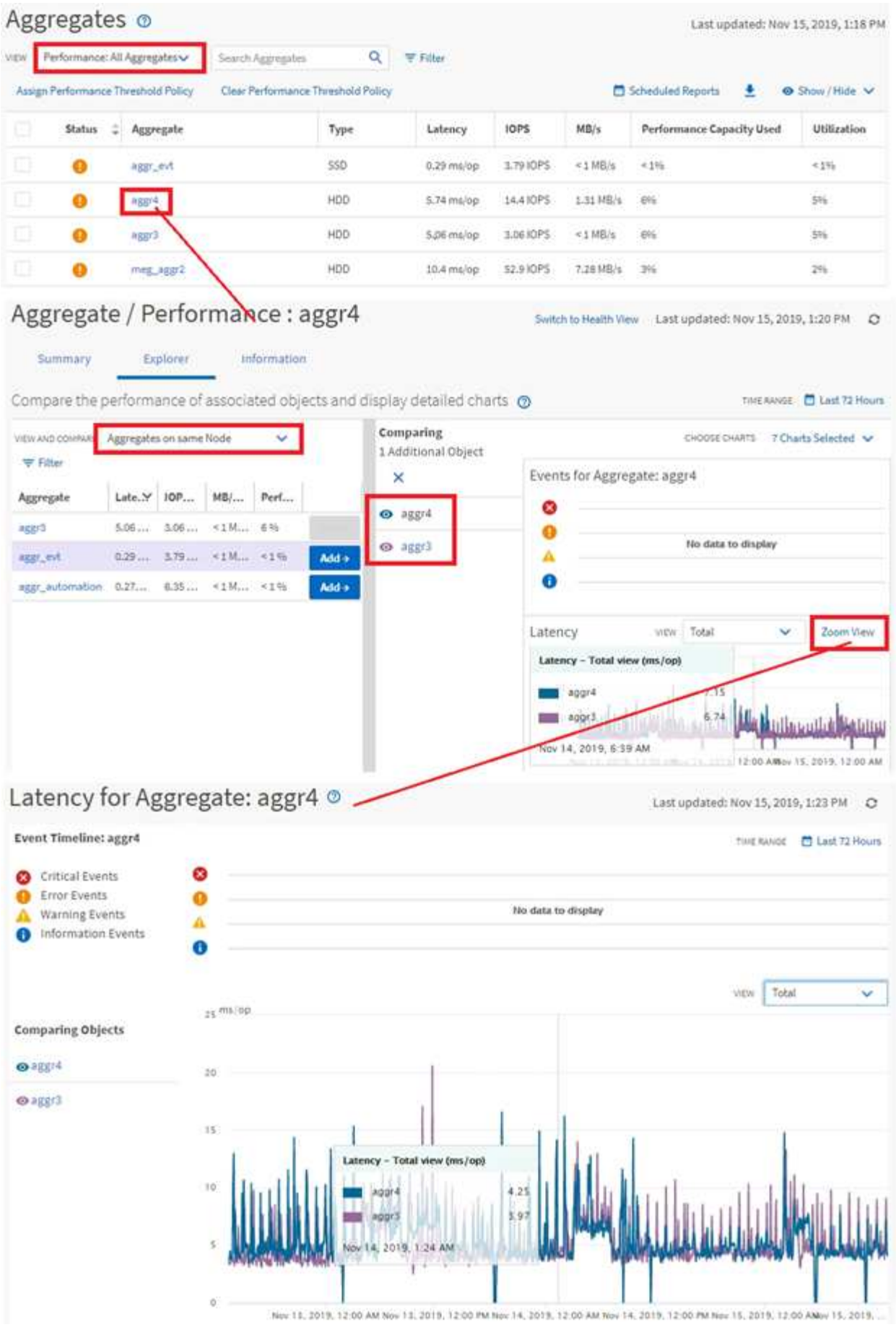
Sie können die Performance aller vom Unified Manager verwalteten Cluster überwachen. Die Überwachung Ihrer Cluster bietet Ihnen einen Überblick über die Cluster- und Objekt-Performance und umfasst die Überwachung von Performance-Ereignissen. Sie können Performance und Ereignisse auf einem allgemeinen Level anzeigen oder Details zur Cluster- und Objekt-Performance sowie zu Performance-Ereignissen genauer untersuchen.

Dies ist ein Beispiel für viele mögliche Navigationspfade für die Cluster-Performance:

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Aggregates**.
2. Informationen zur Performance dieser Aggregate finden Sie in der Ansicht „Performance: All Aggregates“.
3. Zur Navigation zur Seite „Aggregate / Performance Explorer“ ist das zu untersuchende Aggregat auszuwählen und auf dessen Namen zu klicken.
4. Optional können Sie im Menü „Ansicht und Vergleich“ weitere Objekte auswählen, die mit diesem Aggregat verglichen werden sollen, und anschließend eines der Objekte dem Vergleichsbereich hinzufügen.

   Die Statistiken beider Objekte erscheinen zum Vergleich in den Zählerdiagrammen.

5. Im Vergleichsbereich rechts auf der Explorer-Seite lassen sich in einem der Zählerdiagramme über **Zoom View** Details zur Performance Historie für dieses Aggregat anzeigen.


Aggregates
Last updated: Nov 15, 2019, 1:18 PM
VIEW
Performance: All Aggregates
Search Aggregates
Filter
Assign Performance Threshold Policy
Clear Performance Threshold Policy
Scheduled Reports
Show / Hide
Status
Aggregate
Type
Latency
IOPS
MB/s
Performance Capacity Used
Utilization
aggr_evt
SSD
0.29 ms/op
3.79 IOPS
< 1 MB/s
< 1%
aggr4
HDD
5.74 ms/op
14.4 IOPS
1.31 MB/s
6%
5%
aggr3
HDD
5.06 ms/op
3.06 IOPS
< 1 MB/s
6%
5%
meg_aggr2
HDD
10.4 ms/op
52.9 IOPS
7.28 MB/s
3%
2%
Aggregate / Performance : aggr4
Switch to Health View
Last updated: Nov 15, 2019, 1:20 PM
Summary
Explorer
Information
Compare the performance of associated objects and display detailed charts
TIME RANGE
Last 72 Hours
VIEW AND COMPARE
Aggregates on same Node
Filter
Aggregate
Late...
IOP...
MB/...
Perf...
aggr3
5.06 ...
3.06 ...
< 1 M...
6 %
aggr_evt
0.29 ...
3.79 ...
< 1 M...
< 1 %
Add
aggr_automation
0.27...
6.35 ...
< 1 M...
< 1 %
Add
Comparing
1 Additional Object
aggr4
aggr3
CHOOSE CHARTS
7 Charts Selected
Events for Aggregate: aggr4
No data to display
Latency
VIEW
Total
Zoom View
Latency – Total view (ms/op)
aggr4
7.15
aggr3
6.74
Nov 14, 2019, 6:39 AM
12:00 AM
Nov 15, 2019, 12:00 AM
Latency for Aggregate: aggr4
Last updated: Nov 15, 2019, 1:23 PM
Event Timeline: aggr4
TIME RANGE
Last 72 Hours
Critical Events
Error Events
Warning Events
Information Events
No data to display
VIEW
Total
Comparing Objects
aggr4
aggr3
ms/op
25
20
15
10
5
0
Latency – Total view (ms/op)
aggr4
4.25
aggr3
3.97
Nov 14, 2019, 1:24 AM
Nov 13, 2019, 12:00 AM
Nov 13, 2019, 12:00 PM
Nov 14, 2019, 12:00 AM
Nov 14, 2019, 12:00 PM
Nov 15, 2019, 12:00 AM
Nov 15, 2019,

Untersuchung von Leistungsereignissen in Active IQ Unified Manager

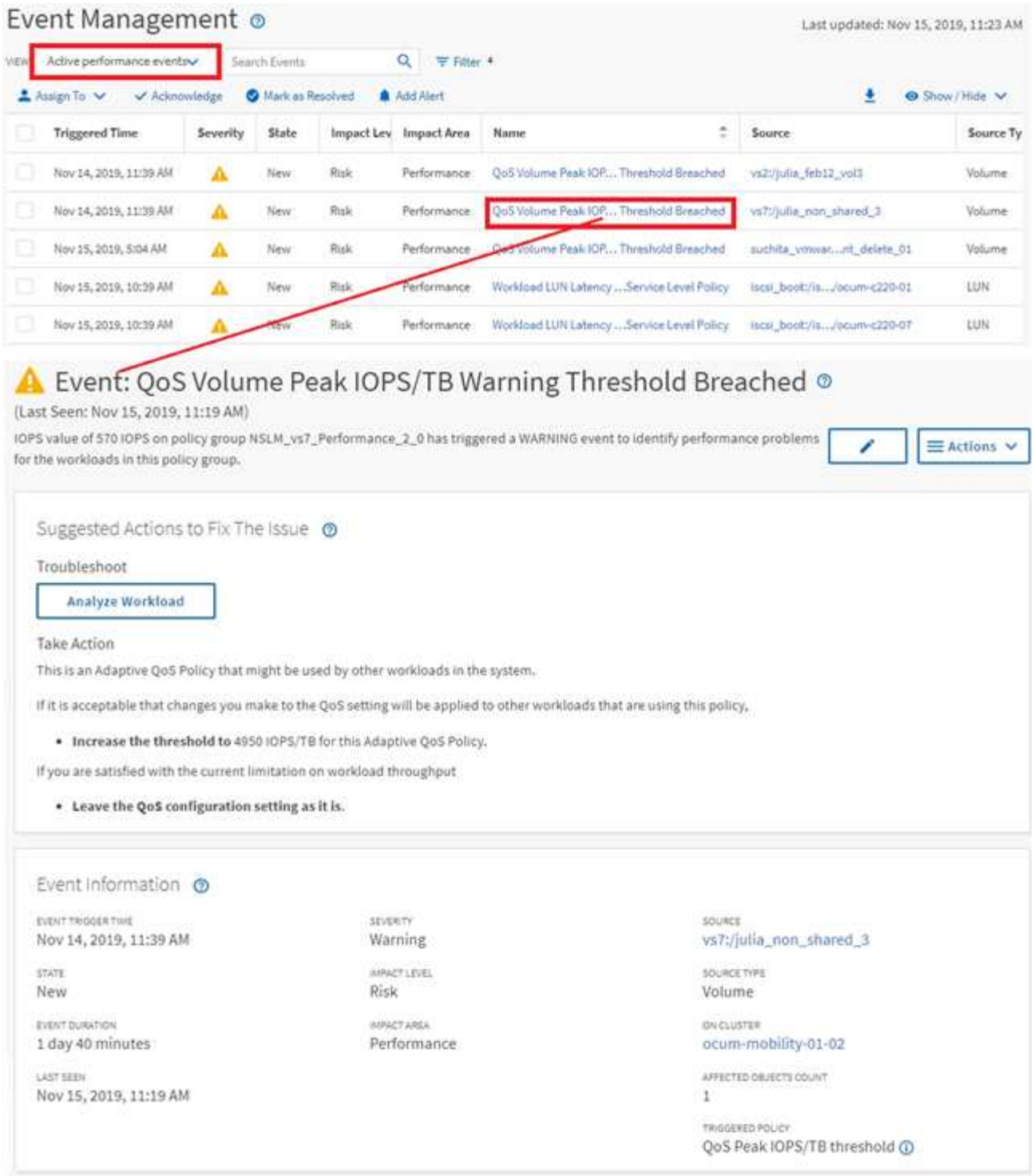
Die Ereignisdetailseiten des Unified Manager bieten Ihnen einen detaillierten Einblick in jedes Performance-Ereignis. Dies ist bei der Untersuchung von Performance-Ereignissen, bei der Fehlerbehebung und bei der Feinabstimmung der System-Performance hilfreich.

Je nach Art des Performance Ereignisses werden Ihnen möglicherweise eine von zwei Arten von Ereignisdetailseiten angezeigt:

- Ereignisdetailseite für benutzerdefinierte und systemdefinierte Schwellenwertrichtlinienereignisse
- Ereignisdetailseite für Ereignisse mit dynamischer Schwellenwertrichtlinie

Dies ist ein Beispiel für die Navigation bei einer Ereignisuntersuchung.

1. Im linken Navigationsbereich auf **Event Management** klicken.
2. Im Menü „Ansicht“ lässt sich **Aktive Performance-Ereignisse** auswählen.
3. Durch Klicken auf den Namen des Ereignisses, das Sie untersuchen möchten, wird die Seite mit den Ereignisdetails angezeigt.
4. In der Description des Ereignisses und in den Suggested Actions (sofern verfügbar) finden sich weitere Details zum Ereignis, die bei der Behebung des Problems hilfreich sein können. Mit der Schaltfläche **Analyze Workload** lassen sich detaillierte Performance-Diagramme anzeigen, um das Problem weiter zu analysieren.



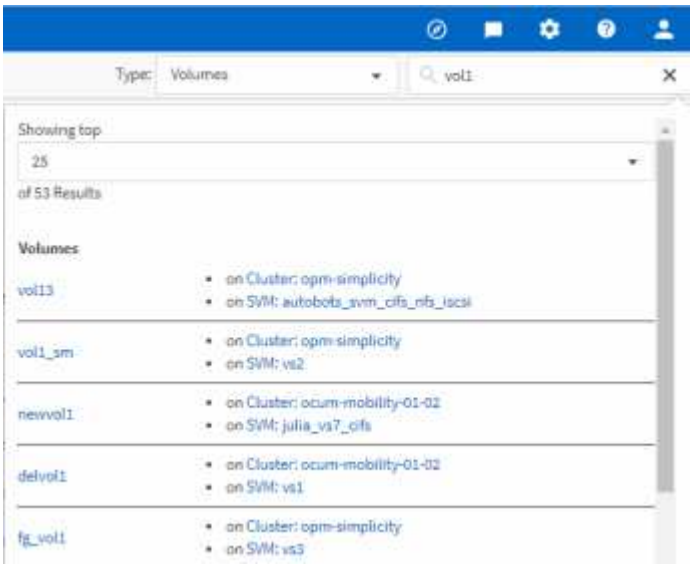
Suche nach Speicherobjekten in Active IQ Unified Manager

Für den schnellen Zugriff auf ein bestimmtes Objekt steht oben in der Menüleiste das Feld **Alle Storage Objekte durchsuchen** zur Verfügung. Diese Methode der globalen Suche über alle Objekte hinweg ermöglicht das schnelle Auffinden bestimmter Objekte nach Typ. Die Suchergebnisse sind nach Storage Objekttyp sortiert und können über das Dropdown-Menü gefiltert werden. Eine gültige Suche muss mindestens drei Zeichen enthalten.

Die globale Suche zeigt die Gesamtzahl der Ergebnisse an, aber nur die ersten 25 Suchergebnisse sind zugänglich. Aus diesem Grund kann die Funktion der globalen Suche als Hilfsmittel zum schnellen Auffinden bestimmter Elemente betrachtet werden, wenn bekannt ist, welche Elemente schnell gefunden werden sollen. Für vollständige Suchergebnisse kann die Suche auf den Objektinventarseiten mit der zugehörigen Filterfunktion verwendet werden.

Sie können auf das Dropdown-Menü klicken und **Alle** auswählen, um gleichzeitig alle Objekte und Ereignisse zu durchsuchen. Alternativ können Sie über das Dropdown-Menü den Objekttyp angeben. Für die Anzeige der Suchergebnisse, z. B.:, werden mindestens drei Zeichen des Objekt- oder Ereignisnamens in das Feld **Alle Storage Objekte durchsuchen** eingegeben und anschließend die **Eingabetaste** gedrückt.

- Cluster: Clusternamen
- Knoten: Knotennamen
- Aggregate: Aggregatnamen
- SVMs: SVM Namen
- Volumes: Volume-Namen
- LUNs: LUN-Pfade



LIFs und Ports sind in der globalen Suchleiste nicht durchsuchbar.

In diesem Beispiel ist im Dropdown-Menü der Objekttyp „Volume“ ausgewählt. Durch Eingabe von “vol” in das Feld **Search all Storage Objects** wird eine Liste aller Volumes angezeigt, deren Namen diese Zeichen enthalten. Bei Objektsuchen gelangen Sie durch Klicken auf ein beliebiges Suchergebnis zur Seite „Performance Explorer“ des entsprechenden Objekts. Bei Ereignissuchen gelangen Sie durch Klicken auf ein Element im Suchergebnis zur Seite „Event Details“.

Inhalte der Inventarseite in Active IQ Unified Manager filtern

Sie können die Daten auf den Inventarseiten im Unified Manager filtern, um schnell Daten anhand bestimmter Kriterien zu finden. Mithilfe der Filterfunktion können Sie die Inhalte der Unified Manager Seiten so einschränken, dass nur die für Sie relevanten Ergebnisse angezeigt werden. Dies ist eine sehr effiziente Methode, um nur die Daten anzuzeigen, die für Sie relevant sind.

Mit **Filterung** lässt sich die Rasteransicht an Ihre Präferenzen anpassen. Die verfügbaren Filteroptionen hängen vom Objekttyp ab, der in der Rasteransicht angezeigt wird. Wenn derzeit Filter angewendet werden, erscheint rechts neben der Schaltfläche „Filter“ deren Anzahl.

Drei Arten von Filterparametern stehen zur Verfügung.

Parameter	Validierung
Zeichenkette (Text)	Die Operatoren sind **enthält**, **beginnt mit**, **endet mit** und **enthält nicht**.
Anzahl	Die Operatoren sind **größer als**, **kleiner als**, **im letzten** und **zwischen**.
Enum (Text)	Die Operatoren sind **is** und **is not**.

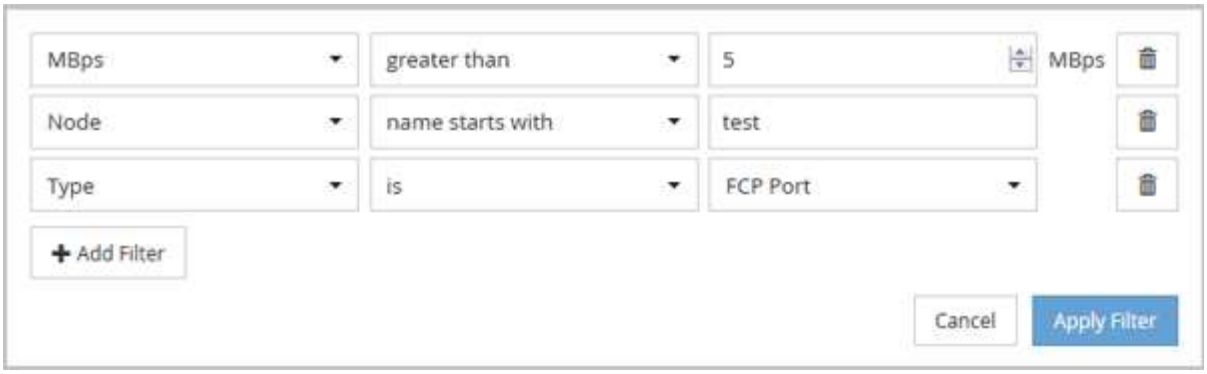
Die Felder „Spalte“, „Operator“ und „Wert“ sind für jeden Filter erforderlich; die verfügbaren Filter entsprechen den filterbaren Spalten auf der aktuellen Seite. Es können maximal vier Filter angewendet werden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten Ihrer gefilterten Suche, nicht nur für die aktuell angezeigte Seite.

Sie können Filter über den Bereich „Filtering“ hinzufügen.

1. Oben auf der Seite wählen Sie die Schaltfläche **Filter** aus. Der Filterbereich wird angezeigt.
2. Über die linke Dropdown-Liste lässt sich ein Objekt auswählen, z. B. *Cluster* oder ein Performance-Zähler.
3. In der mittleren Dropdown-Liste wählen Sie den Operator aus, den Sie verwenden möchten.
4. In der letzten Liste erfolgt die Auswahl oder Eingabe eines Werts, um den Filter für dieses Objekt zu vervollständigen.
5. Zum Hinzufügen eines weiteren Filters klicken Sie auf **+Add Filter**. Ein zusätzliches Filterfeld wird angezeigt. Dieses Filterfeld wird mithilfe des in den vorherigen Schritten beschriebenen Verfahrens ausgefüllt. Es ist zu beachten, dass die Schaltfläche **+Add Filter** nach dem Hinzufügen des vierten Filters nicht mehr angezeigt wird.
6. Zum Anwenden des Filters **Filter anwenden** auswählen. Die Filteroptionen werden auf das Raster angewendet, und die Anzahl der Filter wird rechts neben der Schaltfläche „Filter“ angezeigt.
7. Im Filterbereich können einzelne Filter entfernt werden, indem auf das Papierkorbsymbol rechts neben dem zu entfernenden Filter geklickt wird.
8. Zum Entfernen aller Filter steht unten im Filterbereich **Zurücksetzen** zur Verfügung.

Filterbeispiel

Die Abbildung zeigt das Filterfeld mit drei Filtern. Die Schaltfläche **+Filter hinzufügen** erscheint, wenn weniger als die maximale Anzahl von vier Filtern vorhanden ist.



Nach einem Klick auf **Filter anwenden** schließt sich der Filterbereich, übernimmt Ihre Filter und zeigt die Anzahl der angewendeten Filter an (3).

Überwachung der Cluster-Performance über das Dashboard

Die Clusterleistung lässt sich über das Dashboard in Active IQ Unified Manager überwachen

Das Unified Manager Dashboard stellt einige Bereiche bereit, die den übergeordneten Performance-Status aller Cluster anzeigen, die von dieser Unified Manager Instanz überwacht werden. Damit lässt sich die Gesamt-Performance der verwalteten Cluster beurteilen, und identifizierte Ereignisse können schnell erfasst, lokalisiert oder zur Behebung zugewiesen werden.

Auf dem Active IQ Unified Manager Dashboard stehen Leistungsübersichten zur Verfügung

Das Unified Manager Dashboard bietet mehrere Bereiche, die den allgemeinen Performance-Status aller Cluster in Ihrer Umgebung anzeigen, die überwacht werden. Sie können den Status entweder für alle Cluster oder für einen einzelnen Cluster anzeigen lassen.

Neben Performance Informationen zeigen die meisten Panels auch die Anzahl der aktiven Ereignisse in der jeweiligen Kategorie sowie die Anzahl der in den letzten 24 Stunden neu hinzugekommenen Ereignisse an. Diese Informationen helfen Ihnen bei der Entscheidung, welche Cluster Sie möglicherweise genauer analysieren müssen, um gemeldete Ereignisse zu beheben. Beim Klicken auf die Ereignisse werden die wichtigsten Ereignisse angezeigt, und es wird ein Link zur Event Management Bestandsseite bereitgestellt, die so gefiltert ist, dass die Ereignisse in dieser Kategorie angezeigt werden.

Die folgenden Bereiche geben Auskunft über den Performance-Status.

- **Performance-Kapazitätsbereich**

  In der Übersicht aller Cluster zeigt dieses Panel für jeden Cluster den Wert der Performance Kapazität (gemittelt über die vorherige 1 Stunde) sowie die Anzahl der Tage bis zum Erreichen der oberen Grenze der Performance Kapazität (basierend auf der täglichen Wachstumsrate). Durch Klicken auf das Balkendiagramm gelangt man zur Nodes Inventarseite für diesen Cluster. Zu beachten ist, dass die Nodes Inventarseite die über die vorherigen 72 Stunden gemittelte Performance Kapazität anzeigt, sodass dieser Wert möglicherweise nicht mit dem Dashboard-Wert übereinstimmt.

Bei der Anzeige eines einzelnen Clusters zeigt dieses Panel die Werte für die Cluster Performance Kapazität, die Gesamt-IOPS und den Gesamtdurchsatz an.

- **Workload IOPS Bereich**

  Wenn die aktive Verwaltung von Workloads aktiviert ist und ein einzelner Cluster angezeigt wird, zeigt dieser Bereich die Gesamtzahl der Workloads an, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden.

- **Fensterbereich Workload Performance**

  Wenn das aktive Workload-Management aktiviert ist, zeigt dieses Fenster die Gesamtzahl der konformen und nicht konformen Workloads an, die jedem definierten Performance Service Level zugewiesen sind. Ein Klick auf ein Balkendiagramm führt zu den Workloads, die dieser Richtlinie auf der Seite „Workloads“ zugewiesen sind.

- **Übersichtsfeld zur Nutzung**

  Bei der Anzeige aller Cluster können Sie auswählen, dass Cluster nach den höchsten IOPS oder dem höchsten Durchsatz (MB/s) sortiert angezeigt werden.

  Bei der Anzeige eines einzelnen Clusters können Sie die Workloads auf diesem Cluster nach der höchsten IOPS-Zahl oder dem höchsten Durchsatz (MB/s) sortieren.

Performance-Bannermeldungen in Active IQ Unified Manager interpretieren

Unified Manager kann auf der Benachrichtigungsseite (über die Benachrichtigungsglocke) Bannermeldungen zu Statusproblemen eines bestimmten Clusters anzeigen.

Bannermeldung	Beschreibung	Auflösung
`No performance data is being collected from cluster cluster_name. Restart Unified Manager to correct this issue.`	Der Datenerfassungsdienst von Unified Manager wurde beendet, und es werden keine Performance-Daten mehr von Clustern erfasst.	Ein Neustart von Unified Manager behebt dieses Problem. Falls das Problem dadurch nicht behoben wird, ist der technische Support zu kontaktieren.
`More than x hour(s) of historical data is being collected from cluster cluster_name. Current data collections will start after all historical data is collected.`	Derzeit läuft ein Erfassungszyklus für Datenkontinuität, um Performance-Daten außerhalb des Echtzeit-Cluster-Performance-Erfassungszyklus abzurufen.	Es sind keine Maßnahmen erforderlich. Aktuelle Performance Daten werden nach Abschluss des Datenerfassungszyklus für die Datenkontinuität erfasst. Ein Erfassungszyklus für die Datenkontinuität läuft, wenn ein neuer Cluster hinzugefügt wird oder wenn Unified Manager aus irgendeinem Grund keine aktuellen Leistungsdaten erfassen konnte.

Das Erfassungsintervall für Leistungsstatistiken in Active IQ Unified Manager ändern

Das Standardintervall für die Erfassung von Performance Statistiken beträgt 5 Minuten. Sie können dieses Intervall auf 10 oder 15 Minuten ändern, falls die Erfassung von Daten großer Cluster nicht innerhalb der Standardzeit abgeschlossen wird. Diese Einstellung betrifft die Erfassung von Statistiken aller Cluster, die von dieser Unified Manager Instanz überwacht werden.

Bevor Sie beginnen

Sie müssen über eine Benutzerkennung und ein Passwort verfügen, die für die Anmeldung an der Managementplattform für die Wartung des Unified Manager Servers autorisiert sind.

Auf das Problem, dass die Erfassung von Performance Statistiken nicht rechtzeitig abgeschlossen wird, weisen die Banner-Meldungen `Unable to consistently collect from cluster <cluster_name>` oder `Data collection is taking too long on cluster <cluster_name>` hin.

Das Erfassungsintervall sollte nur dann geändert werden, wenn dies aufgrund eines Problems bei der Erfassung von Statistiken erforderlich ist. Diese Einstellung sollte aus keinem anderen Grund geändert werden.

> Eine Änderung dieses Werts gegenüber der Standardeinstellung von 5 Minuten kann sich auf die Anzahl und Häufigkeit der von Unified Manager gemeldeten Performance-Ereignisse auswirken. Beispielsweise lösen systemdefinierte Performance-Schwellenwerte Ereignisse aus, wenn die Richtlinie 30 Minuten lang überschritten wird. Bei einer Erfassungsdauer von 5 Minuten muss die Richtlinie in sechs aufeinanderfolgenden Erfassungsperioden überschritten werden. Bei einer Erfassungsdauer von 15 Minuten muss die Richtlinie nur in zwei Erfassungsperioden überschritten werden.

Eine Meldung am unteren Rand der Seite „Cluster Setup“ gibt das aktuelle Intervall für die Erfassung statistischer Daten an.

Schritte

1. Sie melden sich per SSH als Wartungsbenutzer am Unified Manager Host an.

   Die Eingabeaufforderungen der Unified Manager Wartungsmanagementplattform werden angezeigt.

2. Die Nummer der Menüoption mit der Bezeichnung **Konfiguration des Performance-Abfrageintervalls** eingeben und anschließend die Eingabetaste drücken.
3. Falls Sie dazu aufgefordert werden, geben Sie das Passwort des Wartungsbenutzers erneut ein.
4. Sie geben die Zahl für das neue Abfrageintervall ein, die Sie festlegen möchten, und drücken anschließend die Eingabetaste.

Wenn Sie das Unified Manager Erfassungsintervall auf 10 oder 15 Minuten geändert haben und derzeit eine Verbindung zu einem externen Datenanbieter (z. B. Graphite) besteht, müssen Sie das Übertragungsintervall des Datenanbieters so ändern, dass es dem Unified Manager Erfassungsintervall entspricht oder größer ist.

Fehlerbehebung bei Workloads mit dem Workload Analyzer

Fehlerbehebung bei Workloads mit dem Workload Analyzer in Active IQ Unified Manager

Der Workload-Analyzer ermöglicht die übersichtliche Darstellung wichtiger Systemstatus- und Performance-Kriterien für einen einzelnen Workload auf einer einzigen Seite und unterstützt so die Fehlerbehebung. Durch die Anzeige aller aktuellen und vergangenen Ereignisse eines Workloads erhalten Sie einen besseren Überblick darüber, warum der Workload derzeit möglicherweise ein Performance- oder Kapazitätsproblem aufweist.

Mithilfe dieses Tools können Sie auch feststellen, ob Storage die Ursache für Performanceprobleme einer Applikation ist oder ob das Problem durch ein Netzwerkproblem oder ein anderes damit zusammenhängendes Problem verursacht wird.

Diese Funktion lässt sich an verschiedenen Stellen in der Benutzeroberfläche starten:

- Über die Option „Arbeitslastanalyse“ im linken Navigationsmenü
- Auf der Seite mit den Ereignisdetails durch Klicken auf die Schaltfläche **Analyze Workload**
- Auf jeder Workload-Inventarseite (Volume, LUN, Workload, NFS-Freigabe oder SMB/CIFS-Freigabe) nach einem Klick auf das Symbol „Mehr“ ⋮ und anschließend auf **Analyze Workload**
- Auf der Seite Virtual Machines durch Klicken auf die Schaltfläche **Analyze Workload** in einem beliebigen Datastore-Objekt

Wenn Sie das Tool über das linke Navigationsmenü starten, können Sie den Namen einer beliebigen Workload eingeben, die Sie analysieren möchten, und den Zeitraum auswählen, für den Sie die Fehlerbehebung durchführen möchten. Wenn Sie das Tool über eine der Inventarseiten für Workloads oder virtuelle Maschinen starten, wird der Name der Workload automatisch eingetragen, und die Daten der Workload werden mit dem standardmäßigen Zeitraum von 2 Stunden angezeigt. Wenn Sie das Tool über die Seite mit den Ereignisdetails starten, wird der Name der Workload automatisch eingetragen, und die Daten von 10 Tagen werden angezeigt.

Workload Analyzer Daten in Active IQ Unified Manager verstehen

Die Seite zur Arbeitslastanalyse zeigt Informationen zu aktuellen Ereignissen an, die sich auf die Arbeitslast auswirken könnten, Empfehlungen zur möglichen Behebung des Problems, das das Ereignis verursacht, sowie Diagramme zur Analyse der Performance- und Kapazitätshistorie.

Oben auf der Seite geben Sie den Namen der zu analysierenden Workload (Volume oder LUN) und den Zeitraum an, für den Statistiken angezeigt werden sollen. Sie können den Zeitraum jederzeit ändern, wenn Sie einen kürzeren oder längeren Zeitraum anzeigen möchten.

In den übrigen Bereichen der Seite werden die Analyseergebnisse sowie die Performance und Kapazitätsdiagramme angezeigt.

ⓘ Workload-Diagramme für LUNs bieten nicht das gleiche Level an Statistiken wie Diagramme für Volumes, daher fallen bei der Analyse dieser beiden Arten von Workloads Unterschiede auf.

- **Ereignisübersichtsbereich**

  Zeigt eine kurze Übersicht über die Anzahl und Art der Ereignisse im angegebenen Zeitraum. Bei Ereignissen aus verschiedenen Wirkungsbereichen (z. B. Performance und Kapazität) werden diese

Informationen angezeigt, sodass Sie Details zum gewünschten Ereignistyp auswählen können. Durch Auswahl des Ereignistyps wird eine Liste der Ereignisnamen angezeigt.

Wenn es im betrachteten Zeitraum nur ein einziges Ereignis gibt, enthält der Eintrag für einige Ereignisse eine Liste mit Empfehlungen zur Behebung des Problems.

- **Zeitleiste der Ereignisse**

  Zeigt alle Ereignisse im angegebenen Zeitraum an. Der jeweilige Ereignisname erscheint, wenn sich der Mauszeiger über einem Ereignis befindet.

  Wenn Sie über die Schaltfläche **Arbeitslast analysieren** von der Seite mit den Ereignisdetails auf diese Seite gelangt sind, wird das Symbol für das ausgewählte Ereignis größer angezeigt, damit Sie das Ereignis leichter erkennen können.

- **Bereich Performance-Diagramme**

  Es werden Diagramme für Latenz, Durchsatz (sowohl IOPS als auch MB/s) und Auslastung (sowohl für den Node als auch für das Aggregat) basierend auf dem von Ihnen ausgewählten Zeitraum angezeigt. Über den Link „View performance details“ kann die Seite „Performance Explorer“ für den Workload angezeigt werden, falls Sie weitere Analysen durchführen möchten.

  - **Latenz** zeigt die Latenz für die Arbeitslast im ausgewählten Zeitraum an. Das Diagramm bietet drei Ansichten, mit denen Folgendes angezeigt werden kann:
    - *Gesamt*latenz
    - **Aufschlüsselung** der Latenz (aufgeschlüsselt nach Lese-, Schreib- und anderen Prozessen)
    - **Cluster Components** Latenz (aufgeschlüsselt nach Clusterkomponente)

Eine Beschreibung der hier angezeigten Clusterkomponenten ist unter "Clusterkomponenten und warum sie um Ressourcen konkurrieren können" zu finden. **Durchsatz zeigt sowohl den IOPS- als auch den MB/s-Durchsatz der Workload im ausgewählten Zeitraum an. Das Diagramm bietet vier Ansichten, in denen Folgendes angezeigt werden kann: * Gesamtdurchsatz * Aufgeschlüsselter Durchsatz (aufgeschlüsselt nach Lese-, Schreib- und anderen Prozessen)** * **Cloud-Durchsatz** (die MB/s, die zum Schreiben von Daten in die Cloud und zum Lesen von Daten aus der Cloud verwendet werden; für Workloads, die Kapazität in die Cloud tieren) *** IOPS mit Prognose (eine Vorhersage der oberen und unteren IOPS-Durchsatzwerte, die für den Zeitraum erwartet wurden) Dieses Diagramm zeigt außerdem die Einstellungen für die maximalen und minimalen Durchsatzschwellenwerte der Quality of Service (QoS) an, sofern diese konfiguriert sind, sodass erkennbar ist, wo das System den Durchsatz möglicherweise absichtlich durch QoS-Richtlinien begrenzt. Auslastung** zeigt die Auslastung sowohl des Aggregats als auch des Knotens an, auf dem die Workload im ausgewählten Zeitraum ausgeführt wird. Hier ist erkennbar, ob Ihr Aggregat oder Knoten überlastet ist und dadurch möglicherweise hohe Latenz verursacht. Bei der Analyse von FlexGroup Volumes werden in den Auslastungsdiagrammen mehrere Knoten und mehrere Aggregate aufgeführt.

- **Kapazitätsdiagrammbereich**

  Diagramme zur Datenkapazität und zur Snapshot-Kapazität der Workload für den vergangenen Monat.

  Bei Volumes können Sie auf den Link „Kapazitätsdetails anzeigen“ klicken, um die Seite „Integritätsdetails“ für den Workload anzuzeigen, falls Sie eine weitere Analyse durchführen möchten. Für LUNs steht dieser Link nicht zur Verfügung, da es für LUNs keine Seite „Integritätsdetails“ gibt.

  - Die **Kapazitätsansicht** zeigt den gesamten für die Arbeitslast zugewiesenen verfügbaren Speicherplatz und den logisch belegten Speicherplatz (nach allen NetApp Optimierungen) an.

- **Snapshot View** zeigt den gesamten für Snapshot Kopien reservierten Speicherplatz sowie den aktuell belegten Speicherplatz an. LUNs stellen keine **Snapshot View** bereit.
- **Cloud Tier View** zeigt, wie viel Kapazität im lokalen Performance-Tier und wie viel im Cloud-Tier verwendet wird. Diese Diagramme enthalten eine Schätzung der verbleibenden Zeit, bis die Kapazität für diese Workload vollständig ausgeschöpft ist. Diese Informationen basieren auf der bisherigen Nutzung und erfordern mindestens 10 Tage an Daten. Wenn weniger als 30 Tage Kapazität verbleiben, kennzeichnet Unified Manager den Storage als “almost full”.

Informationen zur Verwendung des Workload Analyzer in Active IQ Unified Manager

Typischerweise dient der Workload Analyzer dazu, ein von einem Benutzer gemeldetes Latenzproblem zu beheben, ein gemeldetes Ereignis oder eine Warnung eingehender zu analysieren oder eine Workload zu untersuchen, die sich auffällig verhält.

Falls Benutzer Sie kontaktiert haben und mitteilen, dass die von ihnen verwendete Applikation sehr langsam ausgeführt wird, können Sie die Diagramme für Latenz, Durchsatz und Auslastung der Workload überprüfen, auf der die Applikation ausgeführt wird, um festzustellen, ob Storage die Ursache des Performance Problems ist. Sie können auch das Kapazitätsdiagramm verwenden, um festzustellen, ob die Kapazität niedrig ist, da ein ONTAP System mit einer Kapazitätsauslastung von über 85 % Performance Probleme verursachen kann. Diese Diagramme helfen Ihnen dabei festzustellen, ob das Problem durch Storage, das Netzwerk oder einen anderen damit zusammenhängenden Faktor verursacht wird.

Falls Unified Manager ein Performance-Ereignis generiert hat und Sie die Ursache des Problems genauer untersuchen möchten, können Sie den Workload Analyzer auf der Seite mit den Ereignisdetails über die Schaltfläche **Analyze Workload** starten, um einige der Latenz-, Durchsatz- und Kapazitätstrends für die Workload zu untersuchen.

Falls Sie beim Anzeigen einer beliebigen Workload-Inventarseite (Volume, LUN, Workload, NFS-Freigabe oder SMB/CIFS-Freigabe) eine Workload bemerken, die anscheinend nicht normal arbeitet, können Sie auf das Symbol „Mehr“ ⋮ und dann auf „Analyze Workload“ klicken, um die Seite „Workload Analysis“ zu öffnen und die Workload genauer zu untersuchen.

Verwendung des Workload Analyzer in Active IQ Unified Manager

Es gibt viele Möglichkeiten, den Workload Analyzer über die Benutzeroberfläche zu starten. Hier beschreiben wir den Start des Tools über den linken Navigationsbereich.

Schritte

1. Im linken Navigationsbereich auf **Workload Analysis** klicken.

   Die Seite „Workload-Analyse“ wird angezeigt.

2. Wenn der Name der Workload bekannt ist, erfolgt die Eingabe des Namens. Wenn der vollständige Name nicht sicher bekannt ist, sind mindestens 3 Zeichen einzugeben, und das System zeigt eine Liste der Workloads an, die mit der Zeichenfolge übereinstimmen.
3. Wenn Statistiken für einen längeren Zeitraum als die standardmäßigen 2 Stunden angezeigt werden sollen, ist der Zeitraum auszuwählen und anschließend auf **Anwenden** zu klicken.
4. Im Bereich „Zusammenfassung“ können Sie die Ereignisse einsehen, die im angegebenen Zeitraum stattgefunden haben.

5. In den Performance- und Kapazitätsdiagrammen ist erkennbar, wann eine der Kennzahlen außerhalb des Normalbereichs liegt und ob Ereignisse mit dem anomalen Eintrag übereinstimmen.

Sie können die Cluster-Performance auf der Performance Cluster Landing page überwachen.

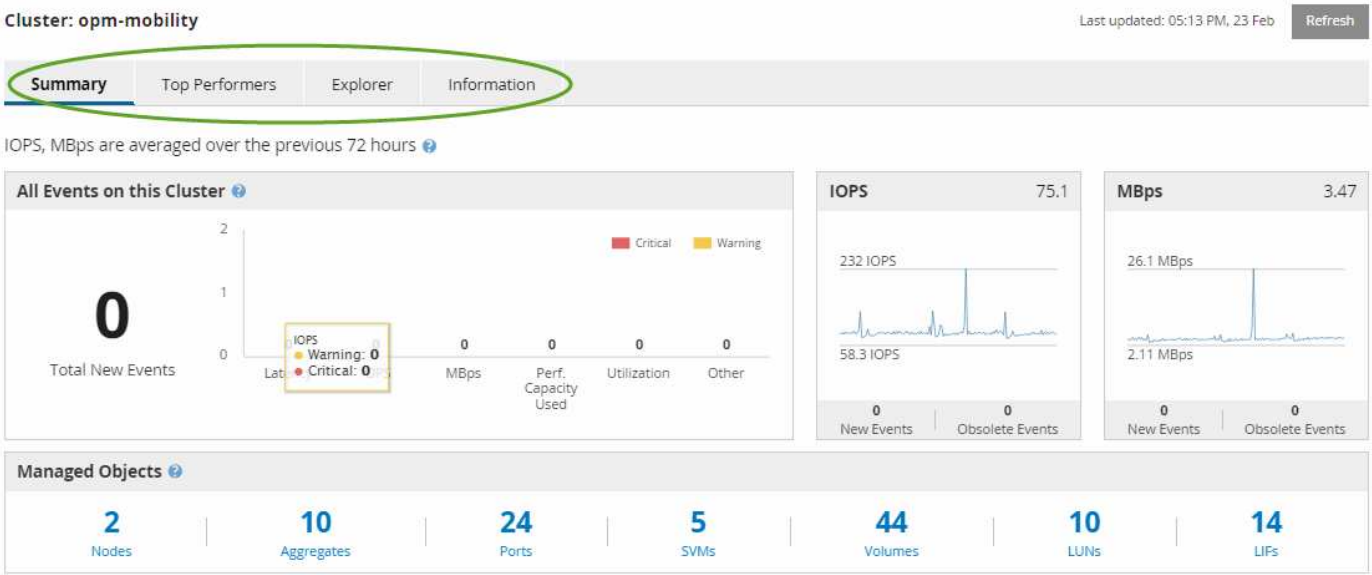
Die Clusterleistung kann auf der Seite „Performance Cluster Landing“ in Active IQ Unified Manager überwacht werden.

Die Landingpage des Performance Clusters zeigt den allgemeinen Performance-Status eines ausgewählten Clusters an, das von einer Unified Manager Instanz überwacht wird. Diese Seite ermöglicht es Ihnen, die Gesamt-Performance eines bestimmten Clusters zu beurteilen und erkannte clusterspezifische Ereignisse schnell zu erfassen, zu lokalisieren oder zur Behebung zuzuweisen.

Die Landingpage des Performance Clusters in Active IQ Unified Manager verstehen

Die Landingpage des Performance Cluster bietet einen allgemeinen Überblick über die Performance eines ausgewählten Clusters, wobei der Schwerpunkt auf dem Performance-Status der Top-10-Objekte innerhalb des Clusters liegt. Performance-Probleme werden oben auf der Seite im Bereich „Alle Ereignisse auf diesem Cluster“ angezeigt.

Die Performance Cluster Landing page bietet einen allgemeinen Überblick über jeden Cluster, der von einer Instanz von Unified Manager gemanagt wird. Diese Seite stellt Informationen zu Ereignissen und Performance bereit und ermöglicht die Überwachung und Fehlerbehebung von Clustern. Die folgende Abbildung zeigt ein Beispiel der Performance Cluster Landing page für den Cluster mit dem Namen opm-mobility:



Die Anzahl der Ereignisse auf der Seite „Clusterübersicht“ stimmt möglicherweise nicht mit der Anzahl der Ereignisse auf der Seite „Leistungsereignisinventar“ überein. Dies liegt daran, dass die Seite „Clusterübersicht“ in den Balken „Latenz“ und „Auslastung“ jeweils ein Ereignis anzeigen kann, wenn kombinierte Schwellenwertrichtlinien überschritten wurden, während die Seite „Leistungsereignisinventar“ nur ein Ereignis

anzeigt, wenn eine kombinierte Richtlinie überschritten wurde.

Wenn ein Cluster aus der Verwaltung durch Unified Manager entfernt wurde, wird der Status **Entfernt** rechts neben dem Clusternamen oben auf der Seite angezeigt.

Landingpage des Performance Cluster

Überprüfung der Landingpage des Performance Clusters in Active IQ Unified Manager

Die Landingpage „Performance Cluster“ zeigt den allgemeinen Performance-Status eines ausgewählten Clusters an. Die Seite ermöglicht den Zugriff auf vollständige Details zu jedem Performance-Zähler für die Storage-Objekte auf dem ausgewählten Cluster.

Die Landingpage des Performance Clusters enthält vier Registerkarten, die die Clusterdetails in vier Informationsbereiche unterteilen:

- Zusammenfassungsseite
  - Bereich „Cluster-Ereignisse“
  - MB/s- und IOPS-Performance-Diagramme
  - Bereich „Verwaltete Objekte“
- Seite „Top Performers“
- Explorer-Seite
- Informationsseite

Zusammenfassungsseite des Performance Clusters

Die Seite „Performance Cluster Summary“ in Active IQ Unified Manager kann überprüft werden.

Die Seite „Performance Cluster Summary“ bietet eine Zusammenfassung der aktiven Ereignisse, der IOPS-Performance und der MB/s-Performance für einen Cluster. Diese Seite enthält außerdem die Gesamtzahl der Storage-Objekte im Cluster.

Eine Überprüfung des Bereichs „Cluster-Leistungsereignisse“ in Active IQ Unified Manager

Der Bereich „Cluster-Performanceereignisse“ zeigt Performance-Statistiken und alle aktiven Ereignisse für den Cluster an. Dies ist besonders hilfreich bei der Überwachung Ihrer Cluster sowie aller clusterbezogenen Performance-Daten und Ereignisse.

Bereich „Alle Ereignisse auf diesem Cluster“

Im Bereich „Alle Ereignisse in diesem Cluster“ werden alle aktiven Cluster Performance-Ereignisse der letzten 72 Stunden angezeigt. Die Gesamtzahl der aktiven Ereignisse wird ganz links angezeigt. Diese Zahl entspricht der Summe aller neuen und bestätigten Ereignisse für alle Storage-Objekte in diesem Cluster. Über den Link „Gesamtzahl der aktiven Ereignisse“ können Sie zur Seite „Ereignisübersicht“ wechseln, die so gefiltert ist, dass diese Ereignisse angezeigt werden.

Das Balkendiagramm „Gesamtzahl aktiver Ereignisse“ für den Cluster zeigt die Gesamtzahl der aktiven kritischen Ereignisse und Warnereignisse an:

- Latenz (gesamt für Knoten, Aggregate, SVMs, Volumes, LUNs und Namespaces)
- IOPS (gesamt für Cluster, Knoten, Aggregate, SVMs, Volumes, LUNs und Namespaces)
- MB/s (gesamt für Cluster, Knoten, Aggregate, SVMs, Volumes, LUNs, Namespaces, Ports und LIFs)
- Genutzte Performance-Kapazität (gesamt für Nodes und Aggregate)
- Auslastung (gesamt für Knoten, Aggregate und Ports)
- Sonstige (Cache-Miss-Verhältnis für Volumes)

Die Liste enthält aktive Performance Ereignisse, die durch benutzerdefinierte Schwellenwertrichtlinien, systemdefinierte Schwellenwertrichtlinien und dynamische Schwellenwerte ausgelöst werden.

Die Diagrammdaten (vertikale Zählerbalken) werden für kritische Ereignisse rot () und für Warnereignisse gelb () angezeigt. Wenn Sie den Mauszeiger über die einzelnen vertikalen Zählerbalken bewegen, werden der tatsächliche Typ und die Anzahl der Ereignisse angezeigt. Durch Klicken auf **Aktualisieren** werden die Daten im Zählerbereich aktualisiert.

Sie können kritische und Warnereignisse im Performance-Diagramm „Total Active Events“ ein- oder ausblenden, indem Sie in der Legende auf die Symbole **Critical** und **Warning** klicken. Wenn Sie bestimmte Ereignistypen ausblenden, werden die Symbole in der Legende grau dargestellt.

Zählerfelder

Die Zählerfelder zeigen die Clusteraktivität und Performance-Ereignisse der vorangegangenen 72 Stunden an und umfassen die folgenden Zähler:

- **IOPS-Zählerfeld**

  IOPS gibt die Betriebsgeschwindigkeit des Clusters als Anzahl der Ein-/Ausgabeoperationen pro Sekunde an. Dieses Zählerfeld bietet einen Überblick über den IOPS-Systemstatus des Clusters für die vorangegangenen 72 Stunden. Durch Positionieren des Mauszeigers über der Trendlinie im Diagramm lässt sich der IOPS-Wert für einen bestimmten Zeitpunkt anzeigen.

- **MB/s-Zählerfeld**

  MB/s zeigt an, wie viele Daten in Megabyte pro Sekunde zum und vom Cluster übertragen wurden. Dieses Zählerfeld bietet eine allgemeine Übersicht über den MB/s Systemstatus des Clusters für den vorangegangenen Zeitraum von 72 Stunden. Durch Positionieren des Mauszeigers über der Trendlinie im Diagramm lässt sich der MB/s-Wert für einen bestimmten Zeitpunkt anzeigen.

Die Zahl oben rechts im Diagramm im grauen Balken ist der Durchschnittswert der letzten 72 Stunden. Die Zahlen unten und oben im Trendliniendiagramm sind die Minimal- und Maximalwerte der letzten 72 Stunden. Der graue Balken unter dem Diagramm enthält die Anzahl aktiver (neuer und bestätigter) Ereignisse und veralteter Ereignisse der letzten 72 Stunden.

Die Zählerfelder enthalten zwei Arten von Ereignissen:

- **Aktiv**

  Zeigt an, dass das Performance-Ereignis derzeit aktiv ist (neu oder bestätigt). Das Problem, das das Ereignis verursacht, hat sich nicht von selbst behoben oder ist noch nicht gelöst. Der Performance-Zähler für das Storage-Objekt bleibt weiterhin über dem Performance-Schwellenwert.

- **Veraltet**

Zeigt an, dass das Ereignis nicht mehr aktiv ist. Das Problem, das das Ereignis verursacht hat, hat sich selbst behoben oder wurde gelöst. Der Performance-Zähler für das Storage-Objekt liegt nicht mehr über dem Performance-Schwellenwert.

Bei **Aktiven Ereignissen** können Sie, wenn nur ein Ereignis vorhanden ist, den Mauszeiger über dem Ereignissymbol positionieren und auf die Ereignisnummer klicken, um zur entsprechenden Seite mit den Ereignisdetails zu gelangen. Wenn mehr als ein Ereignis vorhanden ist, können Sie auf **Alle Ereignisse anzeigen** klicken, um die Seite mit der Ereignisübersicht anzuzeigen, die so gefiltert ist, dass alle Ereignisse für den ausgewählten Objektzählertyp angezeigt werden.

Prüfen des Bereichs „Verwaltete Objekte“ in Active IQ Unified Manager

Der Bereich „Verwaltete Objekte“ auf der Registerkarte „Leistungsübersicht“ bietet einen Überblick auf hoher Ebene über die Storage Objekttypen und deren Anzahl für den Cluster. Dieser Bereich ermöglicht die Verfolgung des Status der Objekte in jedem Cluster.

Die Anzahl der verwalteten Objekte entspricht zeitpunktgenauen Daten aus dem letzten Erfassungszeitraum. Neue Objekte werden in Intervallen von 15 Minuten erkannt.

Durch Klicken auf die verlinkte Nummer für einen beliebigen Objekttyp wird die Objekt-Performance-Inventarseite für diesen Objekttyp angezeigt. Die Objektinventarseite ist so gefiltert, dass nur die Objekte auf diesem Cluster angezeigt werden.

Die verwalteten Objekte sind:

- **Knoten**

  Ein physisches System in einem Cluster.

- **Aggregate**

  Ein Satz aus mehreren Gruppen redundanter Arrays unabhängiger Festplatten (RAID-Gruppen), der als einzelne Einheit für Schutz und Provisionierung verwaltet werden kann.

- **Ports**

  Ein physischer Verbindungspunkt an Knoten, der zur Verbindung mit anderen Geräten in einem Netzwerk dient.

- **Storage-VMs**

  Eine virtuelle Maschine ermöglicht Netzwerkzugriff über eindeutige Netzwerkadressen. Eine SVM kann Daten aus einem separaten Namespace bereitstellen und ist unabhängig vom Rest des Clusters administrierbar.

- **Volumes**

  Eine logische Einheit, die über eines oder mehrere der unterstützten Zugriffsprotokolle zugängliche Benutzerdaten enthält. Die Zählung umfasst sowohl FlexVol Volumes als auch FlexGroup Volumes; FlexGroup Bestandteile werden nicht berücksichtigt.

- **LUNs**

  Die Kennung einer Fibre Channel (FC) logischen Einheit oder einer iSCSI logischen Einheit. Eine logische

Einheit entspricht typischerweise einem Storage-Volume und wird im Betriebssystem eines Computers als Gerät dargestellt.

- **Netzwerkschnittstellen**

  Eine logische Netzwerkschnittstelle, die einen Netzwerkzugriffspunkt für einen Node darstellt. Die Anzahl umfasst alle Schnittstellentypen.

Die Seite „Top-Performer“ in Active IQ Unified Manager

Die Seite „Top Performers“ zeigt die Storage Objekte mit der höchsten oder der niedrigsten Performance an, basierend auf dem Performance Zähler, den Sie auswählen. In der Kategorie Storage VMs können beispielsweise die SVMs mit den höchsten IOPS, der höchsten Latenz oder den niedrigsten MB/s angezeigt werden. Auf dieser Seite wird außerdem angezeigt, ob für eines der Top Performers aktive Performance Ereignisse (New oder Acknowledged) vorliegen.

Auf der Seite „Top Performers“ werden maximal 10 Objekte jedes Typs angezeigt. Zu beachten ist, dass das Objekt „Volume“ sowohl FlexVol Volumes als auch FlexGroup Volumes umfasst.

- **Zeitraum**

  Sie können einen Zeitraum für die Anzeige der leistungsstärksten Objekte auswählen; der ausgewählte Zeitraum gilt für alle Storage Objekte. Verfügbare Zeiträume:

  - Letzte Stunde
  - Letzte 24 Stunden
  - Letzte 72 Stunden (Standard)
  - Letzte 7 Tage

- **Metrik**

  Über das Menü **Metric** lässt sich ein anderer Zähler auswählen. Die Zähleroptionen sind objekttypspezifisch. Beispielsweise stehen für das Objekt **Volumes** die Zähler **Latenz**, **IOPS** und **MB/s** zur Verfügung. Eine Änderung des Zählers lädt die Paneldaten mit den Spitzenreitern auf Basis des ausgewählten Zählers neu.

  Verfügbare Zähler:

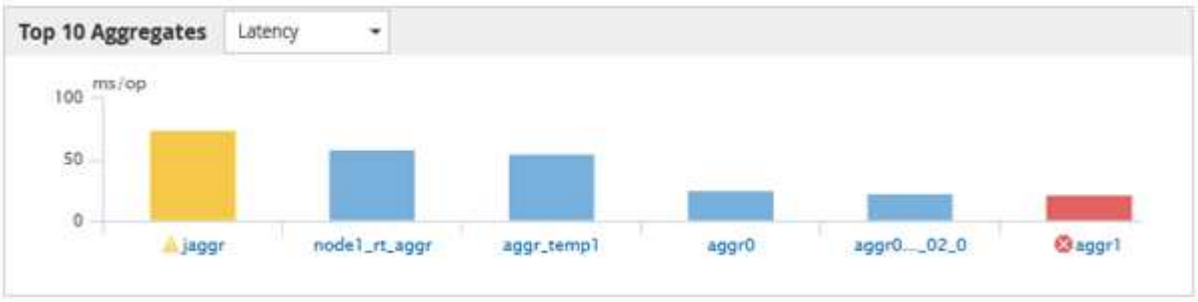
  - Latenz
  - IOPS
  - MB/s
  - Genutzte Performance-Kapazität (für Knoten und Aggregate)
  - Auslastung (für Knoten und Aggregate)

- **Sortieren**

  Im Menü **Sortieren** kann für das ausgewählte Objekt und den ausgewählten Zähler eine aufsteigende oder absteigende Sortierung ausgewählt werden. Die Optionen sind **Höchste zuerst** und **Niedrigste zuerst**. Mit diesen Optionen können die Objekte mit der höchsten oder der niedrigsten Performance angezeigt werden.

- **Zählerleiste**

  Der Zählerbalken im Diagramm zeigt die Performance Statistiken für jedes Objekt an, dargestellt als Balken für das jeweilige Element. Die Balkendiagramme sind farblich gekennzeichnet. Wenn der Zähler keinen Performance Schwellenwert überschreitet, wird der Zählerbalken blau angezeigt. Wenn eine Schwellenwertüberschreitung aktiv ist, also ein neues oder bestätigtes Ereignis vorliegt, wird der Balken in der Farbe des Ereignisses angezeigt: Warnereignisse werden gelb ( ) und kritische Ereignisse rot ( ) dargestellt. Schwellenwertüberschreitungen werden zusätzlich durch Ereignisindikatorsymbole für den Schweregrad von Warnungen und kritischen Ereignissen gekennzeichnet.



  In jedem Diagramm zeigt die X-Achse die Top-Performer für den ausgewählten Objekttyp an. Die Y-Achse zeigt die Einheiten an, die für den ausgewählten Zähler gelten. Ein Klick auf den Link mit dem Objektnamen unter jedem Element des vertikalen Balkendiagramms führt zur Performance Landing page für das ausgewählte Objekt.

- **Ereignisanzeige für Schweregrad**

  Das Symbol für den **Severity Event**-Indikator wird links neben einem Objektnamen für aktive kritische ( ) oder Warnereignisse ( ) in den Top Performer-Diagrammen angezeigt. Durch Klicken auf das Symbol für den **Severity Event**-Indikator wird Folgendes angezeigt:

  - **Ein Ereignis**

    Navigiert zur Detailseite für dieses Ereignis.

  - **Zwei oder mehr Ereignisse**

    Navigiert zur Seite „Ereignisinventar“, die so gefiltert ist, dass alle Ereignisse für das ausgewählte Objekt angezeigt werden.

- **Schaltfläche Export**

  Erstellt eine `.csv` Datei, die die Daten enthält, die in der Zählerleiste angezeigt werden. Sie können wählen, die Datei für den einzelnen Cluster zu erstellen, den Sie anzeigen, oder für alle Cluster im Datacenter.

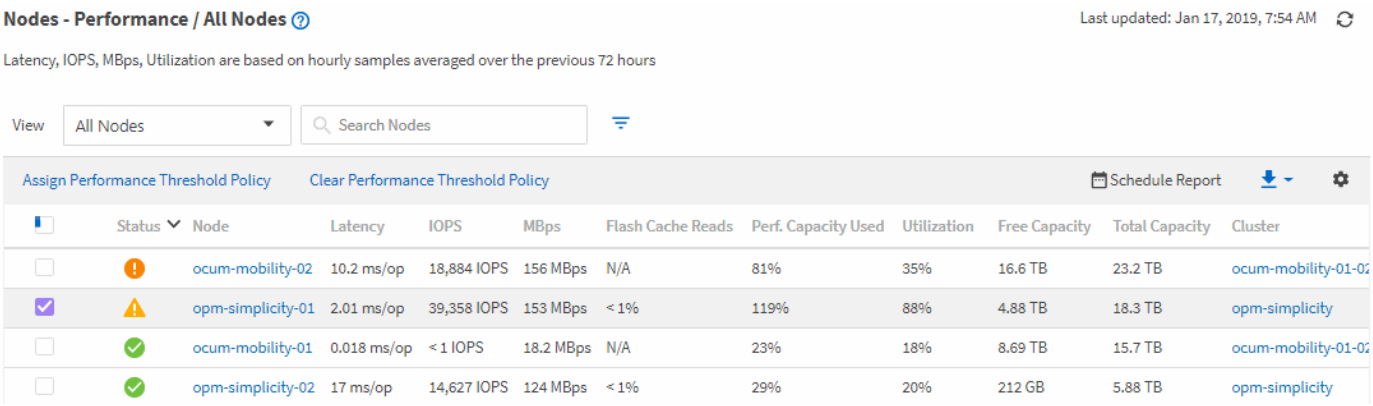
Überwachung der Performance mithilfe der Seiten zur Performance-Inventur

Die Objektleistung kann mithilfe der Performance Inventory Seiten in Active IQ Unified Manager überwacht werden.

Die Objektinventar-Performance-Seiten zeigen Performance-Informationen,

Performance-Ereignisse und den Systemstatus für alle Objekte innerhalb einer Objekttyp-Kategorie an. Dadurch erhalten Sie einen schnellen Überblick über den Performance-Status jedes Objekts innerhalb eines Clusters, beispielsweise für alle Knoten oder alle Volumes.

Objektinventar-Performance-Seiten bieten einen allgemeinen Überblick über den Objektstatus, sodass Sie die Gesamt-Performance aller Objekte beurteilen und die Performance-Daten der Objekte vergleichen können. Sie können den Inhalt von Objektinventar-Seiten durch Suchen, Sortieren und Filtern verfeinern. Dies ist bei der Überwachung und Verwaltung der Objekt-Performance hilfreich, da Sie damit Objekte mit Performance-Problemen schnell finden und mit der Fehlerbehebung beginnen können.



Standardmäßig werden Objekte auf den Performance-Inventarseiten nach der Kritikalität ihrer Objekt-Performance sortiert. Objekte mit neuen kritischen Performance-Ereignissen werden zuerst aufgeführt, Objekte mit Warnereignissen an zweiter Stelle. Dadurch werden Probleme, die behoben werden müssen, sofort sichtbar. Alle Performance-Daten basieren auf einem 72-Stunden-Durchschnitt.

Sie können einfach von der Objektinventar-Performance-Seite zu einer Objektdetailseite navigieren, indem Sie in der Spalte „Objektname“ auf den Objektnamen klicken. Auf der Inventarseite „Performance/All Nodes“ klicken Sie beispielsweise in der Spalte **Nodes** auf ein Knotenobjekt. Die Objektdetailseite bietet ausführliche Informationen und Details zum ausgewählten Objekt, einschließlich eines direkten Vergleichs aktiver Ereignisse.

Leistungsinventarseiten für alle Speicherobjekte in Active IQ Unified Manager

Sie verwenden die Performance-Bestandsseiten, um eine Zusammenfassung der Performance-Informationen zu den verfügbaren Storage Objekten wie Clustern, Aggregaten und Volumes anzuzeigen. Über die Performance-Objektdetailseiten können Sie detaillierte Informationen zu einem bestimmten Objekt anzeigen.

Standardmäßig sind Objekte auf den Ansichtsseiten nach der Kritikalität der Ereignisse sortiert. Objekte mit kritischen Ereignissen werden zuerst aufgeführt, Objekte mit Warnereignissen an zweiter Stelle. Dadurch sind Probleme, die behoben werden müssen, sofort visuell erkennbar.

Sie können Daten von diesen Seiten mithilfe der Schaltfläche **Reports** in eine Datei mit kommagetrennten Werten (`.csv`), eine Microsoft Excel-Datei (`.xlsx`) oder ein Dokument (`.pdf`) exportieren und die exportierten Daten anschließend zum Erstellen von Berichten verwenden. Darüber hinaus können Sie die Seite anpassen und mithilfe der Schaltfläche **Scheduled Reports** die regelmäßige Erstellung und den Versand eines Berichts per E-Mail planen.

Alle Felder auf diesen Seiten können in benutzerdefinierten Ansichten und Berichten verwendet werden.

Einige Felder sind mit verwandten Seiten verknüpft, um eine detailliertere Ansicht zu ermöglichen.

Leistung: Ansicht „Alle Cluster“

Die Ansicht „Performance: All Clusters“ zeigt eine Übersicht über Performance-Ereignisse, Daten und Konfigurationsinformationen für jeden Cluster, der von einer Unified Manager Instanz überwacht wird. Auf dieser Seite können Sie die Performance Ihrer Cluster überwachen sowie Performance-Probleme und Schwellenwertereignisse beheben.

Sie können auf den Objektinventarseiten Performance-Schwellenwertrichtlinien jedem Objekt zuweisen oder Schwellenwertrichtlinien von Objekten entfernen, indem Sie die Schaltflächen **Performance-Schwellenwertrichtlinie zuweisen** und **Performance-Schwellenwertrichtlinie entfernen** verwenden.

Im Folgenden sind einige wichtige Felder in der Ansicht „Performance: Alle Cluster“ aufgeführt.

- Cluster FQDN: Die vollqualifizierte Domain (FQDN) des Clusters.
- IOPS: Die Anzahl der Ein-/Ausgabeoperationen pro Sekunde auf dem Cluster.
- MB/s: Der Durchsatz im Cluster, gemessen in MiB pro Sekunde.
- Kapazitätsfelder: Freie und Gesamtkapazität in GiB.
- Hostname oder IP-Adresse: Der Hostname oder die IP-Adresse (IPv4 oder IPv6) des Cluster-Management-LIF.
- Betriebssystemversion: Die Version der ONTAP Software, die auf dem Cluster installiert ist.

  Wenn auf den Knoten im Cluster unterschiedliche Versionen der ONTAP Software installiert sind, wird die niedrigste Versionsnummer aufgeführt. Die auf den einzelnen Knoten installierte ONTAP Version ist in der Ansicht „Performance: All Nodes“ zu sehen.

- Schwellenwertrichtlinie: Die benutzerdefinierte Performance-Schwellenwertrichtlinie bzw. die benutzerdefinierten Performance-Schwellenwertrichtlinien, die auf diesem Storage Objekt aktiv sind. Bei Richtliniennamen mit Auslassungspunkten (…) zeigt das Positionieren des Cursors den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen an. Die Schaltflächen „Performance-Schwellenwertrichtlinie zuweisen“ und „Performance-Schwellenwertrichtlinie löschen“ bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Performance: Ansicht „Alle Volumes“

Die Ansicht „Performance: Alle Volumes“ zeigt eine Übersicht über die Performance Ereignisse, Zählerdaten und Konfigurationsinformationen für jedes FlexVol Volume und FlexGroup Volume, das von einer Instanz von Unified Manager überwacht wird. Dadurch können Sie die Performance Ihrer Volumes schnell überwachen und Performance Probleme sowie Schwellenwertereignisse beheben.

Wenn die Latenz und der Durchsatz eines bestimmten Objekts analysiert werden sollen, ist die Schaltfläche „Weitere Optionen“ ⋮ und anschließend **Analyze Workload** auszuwählen; auf der Seite „Workload Analysis“ lassen sich dann Performance- und Kapazitätsdiagramme anzeigen. Die Details können in System Manager angezeigt werden, sofern gültige Anmeldeinformationen für System Manager vorliegen.

Für Data Protection (DP) Volumes werden nur Zählerwerte für benutzergenerierten Datenverkehr angezeigt. Root Volumes werden auf dieser Seite nicht angezeigt.

Im Folgenden sind einige wichtige Felder in der Ansicht „Performance: Alle Volumes“ aufgeführt.

- Stil: entweder FlexVol oder FlexGroup.
- Latenz: Bei FlexVol Volumes ist dies die durchschnittliche Antwortzeit des Volumes für alle E/A-Anforderungen, angegeben in Millisekunden pro Operation. Bei FlexGroup Volumes ist dies die durchschnittliche Latenz aller zugehörigen Volumes.
- IOPS/TB: Die Anzahl der pro Sekunde verarbeiteten Ein-/Ausgabeoperationen, bezogen auf den gesamten vom Workload belegten Speicherplatz, angegeben in Terabyte. Dieser Zähler misst, wie viel Performance mit einer bestimmten Storage-Kapazität erzielt werden kann.
- IOPS: Bei FlexVol Volumes ist dies die Anzahl der Ein-/Ausgabeoperationen pro Sekunde für das Volume. Bei FlexGroup Volumes ist dies die Summe der IOPS aller zugehörigen Volumes.
- MB/s: Bei FlexVol Volumes ist dies der Durchsatz auf dem Volume, gemessen in Megabyte pro Sekunde. Bei FlexGroup Volumes ist dies die Summe der MB/s aller Bestandteil-Volumes.
- Kapazitätsfelder: Freie und Gesamtkapazität in GiB.

Weitere Informationen sind unter den folgenden Links verfügbar:

- "Zuweisen von Performance-Schwellenwertrichtlinien zu Storage Objekten"
- "Entfernen von Performance-Schwellenwertrichtlinien aus Storage Objekten"
- "Von Unified Manager überwachte Workload-Typen"
- "Anzeigen der auf bestimmte Volumes oder LUNs angewendeten QoS-Richtliniengruppeneinstellungen"
- "Grundlegendes zu den Empfehlungen von Unified Manager für das Tiering von Daten in die Cloud"
- "Anzeigen von Performance-Diagrammen zum Vergleich von Volumes oder LUNs in derselben QoS-Richtliniengruppe"

Performance: Ansicht „Alle Aggregate“

Die Ansicht „Performance: Alle Aggregate“ zeigt eine Übersicht über die Performance Ereignisse, Daten und Konfigurationsinformationen für jedes Aggregat an, das von einer Instanz von Unified Manager überwacht wird. Diese Seite ermöglicht die Überwachung der Performance Ihrer Aggregate sowie die Fehlerbehebung bei Performance Problemen und Schwellenwertereignissen.

Im Folgenden sind einige wichtige Felder in der Ansicht „Performance: Alle Aggregate“ aufgeführt.

- Typ: Die Art des Aggregats:
  - HDD
  - Hybrid. Kombiniert HDDs und SSDs, Flash Pool wurde jedoch nicht aktiviert.
  - Hybrid (Flash Pool). Kombiniert Festplatten (HDDs) und SSDs, und Flash Pool wurde aktiviert.
  - SSD
  - SSD (FabricPool). Kombiniert SSDs und ein Cloud-Tier
  - HDD (FabricPool). Kombiniert HDDs und ein Cloud-Tier
  - VMDisk (SDS). Virtuelle Festplatten innerhalb einer virtuellen Maschine
  - VMDisk (FabricPool). Kombiniert virtuelle Festplatten und ein Cloud-Tier
  - LUN
- Berichterstattung über inaktive Daten: Gibt an, ob die Funktion zur Berichterstattung über inaktive Daten für dieses Aggregat aktiviert oder deaktiviert ist. Wenn sie aktiviert ist, wird die Menge der kalten Daten in der Ansicht „Performance: Alle Volumes“ für die Volumes dieses Aggregats angezeigt. Der Wert in diesem

Feld ist „N/A“, wenn die Version von ONTAP die Berichterstattung über inaktive Daten nicht unterstützt.

- Schwellenwertrichtlinie: Die benutzerdefinierte Performance-Schwellenwertrichtlinie bzw. die benutzerdefinierten Performance-Schwellenwertrichtlinien, die für dieses Storage-Objekt aktiv sind. Wenn Sie den Mauszeiger über Richtliniennamen mit Auslassungspunkten (…) bewegen, werden der vollständige Richtlinienname oder die Liste der zugewiesenen Richtliniennamen angezeigt. Die Schaltflächen „Performance-Schwellenwertrichtlinie zuweisen“ und „Performance-Schwellenwertrichtlinie löschen“ bleiben deaktiviert, bis Sie ein oder mehrere Objekte durch Klicken auf die Kontrollkästchen ganz links auswählen. Weitere Informationen finden Sie unter den folgenden Links:
- "Zuweisen von Performance-Schwellenwertrichtlinien zu Storage Objekten"
- "Entfernen von Performance-Schwellenwertrichtlinien aus Storage Objekten"

Performance: Ansicht „Alle Knoten“

Die Ansicht „Performance: All Nodes“ bietet eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jeden Knoten, der von einer Unified Manager Instanz überwacht wird. Dies ermöglicht eine schnelle Überwachung der Performance Ihrer Knoten sowie die Behebung von Performance-Problemen und Schwellenwertereignissen.

Flash Cache Reads gibt den Prozentsatz der Lesevorgänge auf dem Knoten an, die durch den Cache bedient werden, anstatt von der Festplatte zurückgegeben zu werden. Flash Cache Daten werden nur für Knoten angezeigt und nur, wenn ein Flash Cache Modul auf dem Knoten installiert ist.

Im Menü **Berichte** ist die Option **Hardwareinventarbericht** verfügbar, wenn Unified Manager und die Cluster, die damit verwaltet werden, an einem Standort ohne externe Netzwerkkonnektivität installiert sind. Diese Schaltfläche generiert eine .csv-Datei mit einer vollständigen Liste der Cluster- und Node-Informationen, z. B. Hardware-Modellnummern und Seriennummern, Festplattentypen und -anzahlen, installierte Lizenzen und mehr. Diese Berichtsfunktion ist für Vertragsverlängerungen in sicheren Umgebungen hilfreich, die nicht mit der NetApp Active IQ Plattform verbunden sind. Sie können Performance-Schwellenwertrichtlinien für beliebige Objekte auf den Objektinventarseiten mit den Schaltflächen **Performance-Schwellenwertrichtlinie zuweisen** und **Performance-Schwellenwertrichtlinie löschen** zuweisen oder entfernen.

Weitere Informationen sind unter den folgenden Links verfügbar:

- "Zuweisen von Performance-Schwellenwertrichtlinien zu Storage Objekten"
- "Entfernen von Performance-Schwellenwertrichtlinien aus Storage Objekten"
- "Erstellung eines Hardware-Inventarberichts für die Vertragsverlängerung"

Performance: Ansicht aller Storage VMs

Die Ansicht „Performance: All Storage VMs“ zeigt eine Übersicht über die Performance Ereignisse, Daten und Konfigurationsinformationen für jede Storage Virtual Machine (SVM) an, die von einer Instanz von Unified Manager überwacht wird. Dadurch ist eine schnelle Überwachung der Performance Ihrer SVMs sowie die Fehlerbehebung bei Performance Problemen und Schwellenwertereignissen möglich. Das Feld „Latency“ auf dieser Seite gibt die durchschnittliche Antwortzeit für alle I/O-Anforderungen in Millisekunden pro Vorgang an.

Die auf dieser Seite aufgeführten SVMs umfassen ausschließlich Daten- und Cluster-SVMs. Unified Manager verwendet oder zeigt keine Admin- oder Node-SVMs an.

Weitere Informationen sind unter den folgenden Links verfügbar:

- "Zuweisen von Performance-Schwellenwertrichtlinien zu Storage Objekten"
- "Entfernen von Performance-Schwellenwertrichtlinien aus Storage Objekten"

Performance: Ansicht aller LUNs

Die Ansicht „Performance: Alle LUNs“ zeigt eine Übersicht über die Performance Ereignisse, Daten und Konfigurationsinformationen für jede LUN an, die von einer Instanz von Unified Manager überwacht wird. Dadurch können die Performance Ihrer LUNs schnell überwacht und Performance Probleme sowie Schwellenwertereignisse behoben werden.

Wenn Sie die Latenz und den Durchsatz eines bestimmten Objekts analysieren möchten, lässt sich über das Symbol „Mehr“ ⋮ und anschließend über **Analyze Workload** die Seite **Workload Analysis** mit Performance- und Kapazitätsdiagrammen öffnen.

Weitere Informationen sind unter den folgenden Links verfügbar:

- "Überwachung von LUNs in einer Konsistenzgruppenbeziehung"
- "Bereitstellung von LUNs"
- "Zuweisen von Performance-Schwellenwertrichtlinien zu Storage Objekten"
- "Entfernen von Performance-Schwellenwertrichtlinien aus Storage Objekten"
- "Anzeigen von Volumes oder LUNs in derselben QoS-Richtliniengruppe".
- "Anzeigen der auf bestimmte Volumes oder LUNs angewendeten QoS-Richtliniengruppeneinstellungen"
- "Bereitstellung von LUNs mithilfe von APIs"

Performance: Ansicht aller NVMe-Namespaces

Die Ansicht „Performance: Alle NVMe Namespaces“ bietet eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jeden NVMe Namespace, der von einer Unified Manager Instanz überwacht wird. So können Sie die Performance und den Systemstatus Ihrer Namespaces schnell überwachen und Probleme sowie Schwellenwertereignisse beheben.

Unter anderem werden folgende Informationen gemeldet: der aktuelle Status des Namespace. * Offline - Lese- oder Schreibzugriff auf den Namespace ist nicht zulässig. * Online - Lese- und Schreibzugriff auf den Namespace ist zulässig. * NVFail - Der Namespace wurde aufgrund eines NVRAM-Fehlers automatisch offline gesetzt. * Space Error - Der Namespace hat keinen freien Speicherplatz mehr.

Weitere Informationen sind unter den folgenden Links verfügbar:

- "Zuweisen von Performance-Schwellenwertrichtlinien zu Storage Objekten"
- "Entfernen von Performance-Schwellenwertrichtlinien aus Storage Objekten"

Performance: Ansicht aller Netzwerkschnittstellen

Die Ansicht „Performance: All Network Interfaces“ zeigt eine Übersicht über die Performance Ereignisse, Daten und Konfigurationsinformationen für jede Netzwerkschnittstelle (LIF), die von dieser Instanz von Unified Manager überwacht wird. Diese Seite ermöglicht eine schnelle Überwachung der Performance Ihrer Schnittstellen sowie die Fehlerbehebung bei Performance Problemen und Schwellenwertereignissen. Im Folgenden sind einige wichtige Felder der Ansicht „Performance: All Network Interfaces“ aufgeführt.

- IOPS: Die Anzahl der Ein-/Ausgabeoperationen pro Sekunde. IOPS gilt nicht für NFS LIFs und CIFS LIFs und wird für diese Typen als „N/A“ angezeigt.

- Latenz: Die durchschnittliche Antwortzeit für alle E/A-Anforderungen, angegeben in Millisekunden pro Operation. Latenz gilt nicht für NFS-LIFs und CIFS-LIFs und wird für diese Typen als N/A angezeigt.
- Home Location: Die Home Location für die Schnittstelle, angezeigt als Node-Name und Portname, getrennt durch einen Doppelpunkt (:). Wenn die Position mit Auslassungspunkten (…) angezeigt wird, können Sie den Mauszeiger über den Positionsnamen bewegen, um die vollständige Position anzuzeigen.
- Aktueller Standort: Der aktuelle Standort der Schnittstelle, angezeigt als Node-Name und Portname, getrennt durch einen Doppelpunkt (:). Wird der Standort mit Auslassungspunkten (…) angezeigt, können Sie den Mauszeiger über den Standortnamen bewegen, um den vollständigen Standort anzuzeigen.
- Rolle: Die Rolle der Schnittstelle: Daten, Cluster, Knotenverwaltung oder Intercluster.

Die auf dieser Seite aufgeführten Schnittstellen umfassen Data LIFs, Cluster LIFs, Node Management LIFs und intercluster LIFs. Unified Manager verwendet oder zeigt keine System LIFs an.

Performance: Ansicht „Alle Ports“

Die Ansicht „Performance: All Ports“ zeigt eine Übersicht über die Performance-Ereignisse, Daten und Konfigurationsinformationen für jeden Port an, der von einer Unified Manager Instanz überwacht wird. Dadurch können Sie die Performance Ihrer Ports schnell überwachen und Probleme mit der Performance sowie Schwellenwertereignisse beheben. Für eine Portrolle wird die Netzwerkportfunktion als Data oder Cluster angezeigt. FCP-Ports können keine Rolle haben, und die Rolle wird als N/A angezeigt.

Performance-Zählerwerte werden nur für physische Ports angezeigt. Zählerwerte werden nicht für VLANs oder Schnittstellengruppen angezeigt.

Weitere Informationen sind unter den folgenden Links verfügbar:

- "Zuweisen von Performance-Schwellenwertrichtlinien zu Storage Objekten"
- "Entfernen von Performance-Schwellenwertrichtlinien aus Storage Objekten"

Performance: Ansicht der QoS-Richtliniengruppen

Die Ansicht „QoS-Richtliniengruppen“ zeigt die QoS-Richtliniengruppen an, die auf den Clustern verfügbar sind, die von Unified Manager überwacht werden. Dazu gehören herkömmliche QoS-Richtlinien, adaptive QoS-Richtlinien und QoS-Richtlinien, die mithilfe von Performance Service Levels zugewiesen sind.

Nachfolgend sind einige wichtige Felder in der Ansicht „Performance: QoS-Richtliniengruppen“ aufgeführt.

- QoS Policy Group: Der Name der QoS Policy Group. Bei NetApp Service Level Manager (NSLM) 1.3-Richtlinien, die in Unified Manager 9.7 oder höher importiert wurden, enthält der hier angezeigte Name den SVM-Namen und weitere Informationen, die nicht im Namen enthalten sind, wenn das Performance Service Level in NSLM definiert wurde. Beispielsweise bedeutet der Name „NSLM_vs6_Performance_2_0“, dass es sich um die systemdefinierte NSLM-PSL-Richtlinie „Performance“ handelt, die auf der SVM „vs6“ mit einer erwarteten Latenz von „2 ms/op“ erstellt wurde.
- SVM: Die Storage VM (SVM), zu der die QoS-Richtliniengruppe gehört. Über den Namen der Storage VM gelangen Sie zur Detailseite dieser Storage VM. Dieses Feld ist leer, wenn die QoS-Richtlinie auf der Admin Storage VM erstellt wurde, da dieser Storage VM-Typ den Cluster repräsentiert.
- Minimaler Durchsatz: Der minimale Durchsatz in IOPS, den die Richtliniengruppe garantiert bereitstellt. Bei adaptiven Richtlinien sind dies die minimal erwarteten IOPS pro TB, die dem Volume oder der LUN basierend auf der zugewiesenen Größe des Storage Objekts zugewiesen werden.

- Maximaler Durchsatz: Der Durchsatz in IOPS und/oder MB/s, den die Richtliniengruppe nicht überschreiten darf. Wenn dieses Feld leer ist, bedeutet dies, dass der in ONTAP definierte maximale Durchsatz unendlich ist. Bei adaptiven Richtlinien ist dies die maximal mögliche Anzahl an IOPS pro TB, die dem Volume oder der LUN zugewiesen werden kann, basierend entweder auf der zugewiesenen Größe des Storage-Objekts oder auf der verwendeten Größe des Storage-Objekts.
- Absolutes Minimum an IOPS: Bei adaptiven Richtlinien ist dies der absolute Mindest-IOPS-Wert, der als Überschreibungswert verwendet wird, wenn die erwarteten IOPS unter diesem Wert liegen.
- Blockgröße: Die für die adaptive QoS-Richtlinie festgelegte Blockgröße.
- Minimale Zuweisung: Gibt an, ob „zugewiesener Speicherplatz“ oder „genutzter Speicherplatz“ zur Bestimmung der maximalen Durchsatz-IOPS (Spitzenwert) verwendet wird.
- Erwartete Latenz: Die erwartete durchschnittliche Latenz für Storage Ein-/Ausgabeoperationen.
- Gemeinsam: Bei traditionellen QoS-Richtlinien, ob die in der Richtliniengruppe definierten Durchsatzwerte von mehreren Objekten gemeinsam genutzt werden.
- Zugeordnete Objekte: Die Anzahl der Workloads, die der QoS-Richtliniengruppe zugewiesen sind. Über die Schaltfläche zum Erweitern ( ) neben dem Namen der QoS-Richtliniengruppe lassen sich weitere Details zur Richtliniengruppe anzeigen.
- Zugewiesene Kapazität: Der Speicherplatz, den die Objekte der QoS-Richtliniengruppe aktuell belegen.
- Zugeordnete Objekte: Die Anzahl der Workloads, die der QoS-Richtliniengruppe zugewiesen sind, unterteilt in Volumes und LUNs. Über die Zahl gelangen Sie zu einer Seite mit weiteren Details zu den ausgewählten Volumes oder LUNs.

Weitere Informationen sind in den Themen unter "Verwalten der Performance mithilfe von Informationen zu QoS-Richtliniengruppen" verfügbar.

Inhalte der Performance-Inventarseite überarbeiten

Verfeinerung des Inhalts der Leistungsinventarseite in Active IQ Unified Manager

Die Inventarseiten für Performance Objekte enthalten Werkzeuge, mit denen Sie den Inhalt der Objektinventardaten verfeinern können, sodass sich bestimmte Daten schnell und einfach finden lassen.

Die auf den Inventarseiten für Performance-Objekte enthaltenen Informationen können sehr umfangreich sein und sich oft über mehrere Seiten erstrecken. Diese umfassenden Daten eignen sich hervorragend zur Überwachung, Nachverfolgung und Verbesserung der Performance; zum schnellen Auffinden bestimmter Daten sind jedoch Werkzeuge erforderlich, mit denen sich die gesuchten Daten rasch lokalisieren lassen. Daher enthalten die Inventarseiten für Performance-Objekte Funktionen zum Suchen, Sortieren und Filtern. Außerdem können Suche und Filterung zusammen verwendet werden, um die Ergebnisse weiter einzugrenzen.

Suche auf den Seiten zur Performance des Objektbestands in Active IQ Unified Manager

Sie können auf den Leistungsseiten des Objektinventars nach Zeichenfolgen suchen. Das Feld **Search** oben rechts auf der Seite ermöglicht das schnelle Auffinden von Daten anhand des Objektnamens oder des Richtliniennamens. Dadurch können bestimmte Objekte und die zugehörigen Daten oder Richtlinien schnell gefunden und die zugehörigen Richtlinienobjektdaten angezeigt werden.

Schritt

1. Abhängig von Ihren Suchanforderungen kommt eine der folgenden Optionen in Frage:

Um dies zu finden…	Folgendes eingeben…
Ein bestimmtes Objekt	Nach Eingabe des Objektnamens in das Feld **Search** und einem Klick auf **Search** werden das gesuchte Objekt und die zugehörigen Daten angezeigt.
Eine benutzerdefinierte Performance-Schwellenwertrichtlinie	Den vollständigen Richtliniennamen oder einen Teil davon in das Feld **Search** eingeben und auf **Search** klicken. Die der gesuchten Richtlinie zugeordneten Objekte werden angezeigt.

Die Daten auf den Seiten zur Objektinventar-Performance in Active IQ Unified Manager können sortiert werden

Sie können alle Daten auf den Performance-Seiten der Objektinventur nach jeder Spalte in aufsteigender oder absteigender Reihenfolge sortieren. Dadurch lassen sich Objektinventardaten schnell auffinden, was bei der Untersuchung der Performance oder beim Beginn eines Fehlerbehebungsprozesses hilfreich ist.

Die zum Sortieren ausgewählte Spalte wird durch den Namen einer hervorgehobenen Spaltenüberschrift und ein Pfeilsymbol rechts neben dem Namen angezeigt, das die Sortierrichtung angibt. Ein Pfeil nach oben weist auf aufsteigende Sortierung hin, ein Pfeil nach unten auf absteigende Sortierung. Die Standardsortierreihenfolge erfolgt nach **Status** (Ereigniskritikalität) in absteigender Reihenfolge, wobei die kritischsten Performance-Ereignisse zuerst aufgeführt werden.

Schritt

1. Durch Klicken auf einen Spaltennamen kann die Sortierreihenfolge der Spalte zwischen aufsteigender und absteigender Reihenfolge umgeschaltet werden.

   Die Inhalte der Seite „Objektinventar-Performance“ sind auf Grundlage der ausgewählten Spalte in aufsteigender oder absteigender Reihenfolge sortiert.

Filtern von Daten auf den Seiten zur Objektinventar-Performance in Active IQ Unified Manager

Sie können Daten auf den Object Inventory Performance pages filtern, um anhand bestimmter Kriterien schnell Daten zu finden. Mithilfe der Filterfunktion können Sie den Inhalt der Object Inventory Performance pages so eingrenzen, dass nur die von Ihnen angegebenen Ergebnisse angezeigt werden. Dies ist eine sehr effiziente Methode, um nur die Performance Daten anzuzeigen, für die Sie sich interessieren.

Im Filterbereich können Sie die Rasteransicht an Ihre Bedürfnisse anpassen. Die verfügbaren Filteroptionen hängen vom angezeigten Objekttyp ab. Wenn derzeit Filter angewendet werden, wird die Anzahl der angewendeten Filter rechts neben der Schaltfläche „Filter“ angezeigt.

Drei Arten von Filterparametern stehen zur Verfügung.

Parameter	Validierung
Zeichenkette (Text)	Die Operatoren sind **enthält**, **beginnt mit**, **endet mit** und **enthält nicht**.

Parameter	Validierung
Anzahl	Die Operatoren sind **größer als**, **kleiner als**, **im letzten** und **zwischen**.
Enum (Text)	Die Operatoren sind **is** und **is not**.

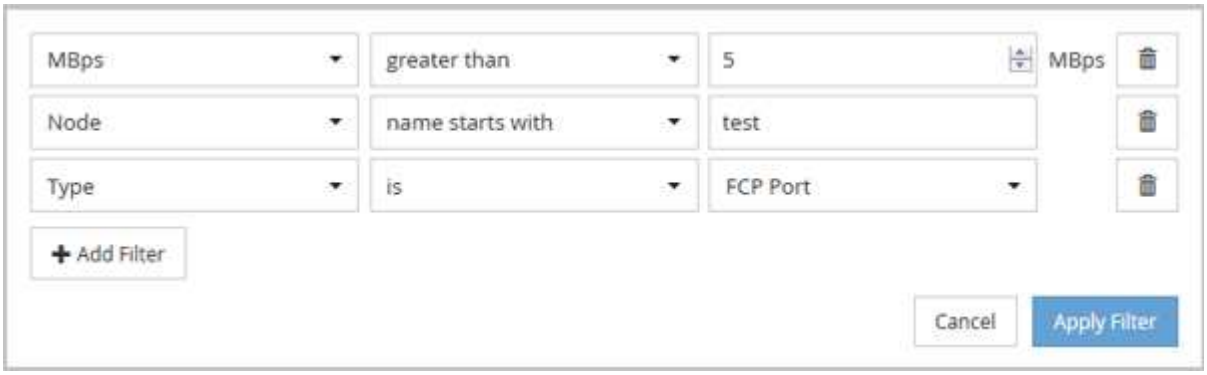
Die Felder „Spalte“, „Operator“ und „Wert“ sind für jeden Filter erforderlich; die verfügbaren Filter entsprechen den filterbaren Spalten auf der aktuellen Seite. Es können maximal vier Filter angewendet werden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten Ihrer gefilterten Suche, nicht nur für die aktuell angezeigte Seite.

Sie können Filter über den Bereich „Filtering“ hinzufügen.

1. Oben auf der Seite wählen Sie die Schaltfläche **Filter** aus. Der Filterbereich wird angezeigt.
2. Über die linke Dropdown-Liste lässt sich ein Objekt auswählen, z. B. *Cluster* oder ein Performance-Zähler.
3. In der mittleren Dropdown-Liste wählen Sie den Operator aus, den Sie verwenden möchten.
4. In der letzten Liste erfolgt die Auswahl oder Eingabe eines Werts, um den Filter für dieses Objekt zu vervollständigen.
5. Zum Hinzufügen eines weiteren Filters klicken Sie auf **+Add Filter**. Ein zusätzliches Filterfeld wird angezeigt. Dieses Filterfeld wird mithilfe des in den vorherigen Schritten beschriebenen Verfahrens ausgefüllt. Es ist zu beachten, dass die Schaltfläche **+Add Filter** nach dem Hinzufügen des vierten Filters nicht mehr angezeigt wird.
6. Zum Anwenden des Filters **Filter anwenden** auswählen. Die Filteroptionen werden auf das Raster angewendet, und die Anzahl der Filter wird rechts neben der Schaltfläche „Filter“ angezeigt.
7. Im Filterbereich können einzelne Filter entfernt werden, indem auf das Papierkorbsymbol rechts neben dem zu entfernenden Filter geklickt wird.
8. Zum Entfernen aller Filter steht unten im Filterbereich **Zurücksetzen** zur Verfügung.

Filterbeispiel

Die Abbildung zeigt das Filterfeld mit drei Filtern. Die Schaltfläche **+Filter hinzufügen** erscheint, wenn weniger als die maximale Anzahl von vier Filtern vorhanden ist.



Nach einem Klick auf **Filter anwenden** schließt sich der Filterbereich, übernimmt Ihre Filter und zeigt die Anzahl der angewendeten Filter an (3).

Die Empfehlungen von Active IQ Unified Manager für das Tiering von Daten in die Cloud können in Active IQ Unified Manager überprüft werden.

Die Ansicht „Performance: Alle Volumes“ zeigt Informationen zur Größe der auf dem Volume gespeicherten inaktiven (kalten) Benutzerdaten an. In manchen Fällen identifiziert Unified Manager bestimmte Volumes, die von einer Tiering der inaktiven Daten auf die Cloud-Ebene (Cloud-Anbieter oder StorageGRID) eines für FabricPool aktivierten Aggregats profitieren würden.

FabricPool wurde in ONTAP 9.2 eingeführt. Wenn Sie also eine Version der ONTAP Software vor 9.2 verwenden, erfordert die Empfehlung von Unified Manager zum Tiering von Daten ein Upgrade Ihrer ONTAP Software. Außerdem wurde die **`auto`** Tiering-Richtlinie in ONTAP 9.4 eingeführt, und die **`all`** Tiering-Richtlinie wurde in ONTAP 9.6 eingeführt. Wenn die Empfehlung also die Verwendung der auto Tiering-Richtlinie vorsieht, müssen Sie ein Upgrade auf ONTAP 9.4 oder höher durchführen.

Die folgenden drei Felder in der Ansicht „Performance: Alle Volumes“ geben Auskunft darüber, ob Sie die Festplattenauslastung Ihres Storage-Systems verbessern und Speicherplatz auf dem Performance-Tier einsparen können, indem Sie inaktive Daten in die Cloud-Ebene verschieben.

- **Tiering-Richtlinie**

  Die Tiering-Richtlinie legt fest, ob die Daten auf dem Volume auf der Performance-Ebene verbleiben oder ob ein Teil der Daten von der Performance-Ebene in die Cloud-Ebene verschoben wird.

  Der Wert in diesem Feld gibt die für das Volume festgelegte Tiering-Richtlinie an, auch wenn sich das Volume aktuell nicht auf einem FabricPool Aggregat befindet. Die Tiering-Richtlinie wird erst wirksam, wenn sich das Volume auf einem FabricPool Aggregat befindet.

- **Kalte Daten**

  Die Anzeige der kalten Daten gibt die Größe der auf dem inaktiven (kalten) Volume gespeicherten Benutzerdaten an.

  Ein Wert wird hier nur bei Verwendung von ONTAP 9.4 oder höher angezeigt, da dies voraussetzt, dass das Aggregat, auf dem das Volume bereitgestellt ist, die **`inactive data reporting parameter`** auf **`enabled`** gesetzt hat und dass die Mindestanzahl an Kühltagen erreicht wurde (für Volumes, die die Tiering-Richtlinie **`snapshot-only`** oder **`auto`** verwenden). Andernfalls wird der Wert als “N/A” aufgeführt.

- **Cloud-Empfehlung**

  Nachdem genügend Informationen über die Datenaktivität auf dem Volume erfasst wurden, kann Unified Manager feststellen, dass keine Maßnahmen erforderlich sind oder dass Sie Speicherplatz auf dem Performance Tier sparen können, indem Sie inaktive Daten auf das Cloud Tier verschieben.

Das Feld „Kalte Daten“ wird alle 15 Minuten aktualisiert, das Feld „Cloud-Empfehlung“ hingegen alle 7 Tage, wenn die Analyse kalter Daten auf dem Volume durchgeführt wird. Daher kann die genaue Menge kalter Daten zwischen den Feldern abweichen. Das Feld „Cloud-Empfehlung“ zeigt das Datum an, an dem die Analyse ausgeführt wurde.

Wenn die Berichterstellung über inaktive Daten aktiviert ist, zeigt das Feld „Kalte Daten“ die genaue Menge an inaktiven Daten an. Ohne die Funktion zur Berichterstellung über inaktive Daten verwendet Unified Manager Performance-Statistiken, um festzustellen, ob Daten auf einem Volume inaktiv sind. Die Menge an inaktiven

Daten wird in diesem Fall nicht im Feld „Kalte Daten“ angezeigt, sondern erst, wenn Sie den Mauszeiger über das Wort „Tier“ bewegen, um die Cloud-Empfehlung anzuzeigen.

Die angezeigten Cloud-Empfehlungen lauten:

- **Lernprozess**. Es wurden noch nicht genügend Daten gesammelt, um eine Empfehlung auszusprechen.
- **Tier**. Die Analyse hat ergeben, dass das Volume inaktive (kalte) Daten enthält und Sie das Volume so konfigurieren sollten, dass diese Daten in das Cloud-Tier verschoben werden. In einigen Fällen kann dies erfordern, dass Sie das Volume zuerst in ein FabricPool fähiges Aggregat verschieben. In anderen Fällen, in denen sich das Volume bereits auf einem FabricPool Aggregat befindet, müssen Sie lediglich die Tiering-Richtlinie ändern.
- **Keine Aktion**. Entweder enthält das Volume nur sehr wenige inaktive Daten, das Volume ist auf einem FabricPool Aggregat bereits auf die Tiering-Richtlinie “auto” gesetzt, oder es handelt sich bei dem Volume um ein Datensicherungs-Volume. Dieser Wert wird auch angezeigt, wenn das Volume offline ist oder in einer MetroCluster Konfiguration verwendet wird.

Zum Verschieben eines Volume oder zum Ändern der Volume-Tiering-Richtlinie oder der Einstellungen für die Berichterstattung über inaktive Aggregatdaten können ONTAP System Manager, die ONTAP CLI-Befehle oder eine Kombination dieser Tools verwendet werden.

Wenn Sie in Unified Manager mit der Rolle **Application Administrator** oder **Storage Administrator** angemeldet sind, ist der Link **Configure Volume** in der Cloud-Empfehlung verfügbar, wenn Sie den Mauszeiger über das Wort **Tier** bewegen. Mit dieser Schaltfläche lässt sich die Seite **Volumes** in System Manager öffnen, um die empfohlene Änderung vorzunehmen.

Überwachung der Performance mithilfe der Performance Explorer Seiten

Die Überwachung der Leistung erfolgt mithilfe der Performance Explorer Seiten in Active IQ Unified Manager

Die Seiten des Performance Explorer zeigen detaillierte Informationen zur Performance jedes Objekts in einem Cluster an. Die Seite bietet eine detaillierte Ansicht der Performance aller Clusterobjekte und ermöglicht es Ihnen, die Performance-Daten bestimmter Objekte über verschiedene Zeiträume hinweg auszuwählen und zu vergleichen.

Sie können auch die Gesamtperformance aller Objekte beurteilen und die Performance-Daten von Objekten in einem nebeneinander angeordneten Format vergleichen.

Stammobjekte werden für die Leistungsüberwachung in Active IQ Unified Manager verwendet

Das Stammobjekt dient als Grundlage, mit der andere Objektvergleiche vorgenommen werden. Dadurch können Sie die Daten anderer Objekte mit dem Stammobjekt anzeigen und vergleichen. So erhalten Sie eine Analyse der Performance-Daten, die Sie bei der Fehlerbehebung und der Verbesserung der Objekt-Performance unterstützt.

Der Name des Stammobjekts wird oben im Vergleichsbereich angezeigt. Weitere Objekte werden unterhalb des Stammobjekts angezeigt. Sie können dem Vergleichsbereich zwar beliebig viele weitere Objekte

hinzufügen, es ist jedoch nur ein Stammobjekt zulässig. Die Daten des Stammobjekts werden automatisch in den Diagrammen im Bereich „Zählerdiagramme“ angezeigt.

Das Stammobjekt kann nicht geändert werden; es ist immer auf die aktuell angezeigte Objektseite festgelegt. Wenn Sie beispielsweise die Seite „Volume Performance Explorer“ von Volume1 öffnen, ist Volume1 das Stammobjekt und kann nicht geändert werden. Für einen Vergleich mit einem anderen Stammobjekt ist der Link zu einem Objekt auszuwählen und dessen Startseite zu öffnen.

Ereignisse und Schwellenwerte werden nur für Root-Objekte angezeigt.

Korrelierte Objekte im Active IQ Unified Manager Raster filtern

Durch Filtern können Sie eine kleinere, besser definierte Teilmenge von Objekten im Raster anzeigen. Wenn Sie beispielsweise 25 Volumes im Raster haben, können Sie durch Filtern nur diejenigen Volumes anzeigen lassen, deren Durchsatz unter 90 MBps liegt oder deren Latenz über 1 ms/op liegt.

Zeitbereich für korrelierte Objekte festlegen

Ein Zeitbereich für korrelierte Objekte in Active IQ Unified Manager wird angegeben

Die Zeitbereichsauswahl auf der Seite „Performance Explorer“ ermöglicht es Ihnen, den Zeitbereich für den Vergleich von Objektdaten festzulegen. Die Angabe eines Zeitbereichs grenzt den Inhalt der Seiten „Performance Explorer“ so ein, dass nur die Objektdaten innerhalb des von Ihnen angegebenen Zeitbereichs angezeigt werden.

Die Eingrenzung des Zeitraums bietet eine effiziente Methode, nur die Performance-Daten anzuzeigen, die für Sie von Interesse sind. Sie können einen vordefinierten Zeitraum auswählen oder einen benutzerdefinierten Zeitraum festlegen. Der Standardzeitraum umfasst die vorangegangenen 72 Stunden.

Auswahl eines vordefinierten Zeitbereichs in Active IQ Unified Manager

Die Auswahl eines vordefinierten Zeitraums ist eine schnelle und effiziente Möglichkeit, die Datenausgabe bei der Anzeige von Performance-Daten zu Cluster-Objekten anzupassen und gezielt darauf zu fokussieren. Bei Auswahl eines vordefinierten Zeitraums stehen Daten für bis zu 13 Monate zur Verfügung.

Schritte

1. Oben rechts auf der Seite **Performance Explorer** lässt sich **Time Range** auswählen.
2. Auf der rechten Seite des Bereichs **Zeitbereichsauswahl** wird ein vordefinierter Zeitbereich ausgewählt.
3. **Bereich anwenden** auswählen.

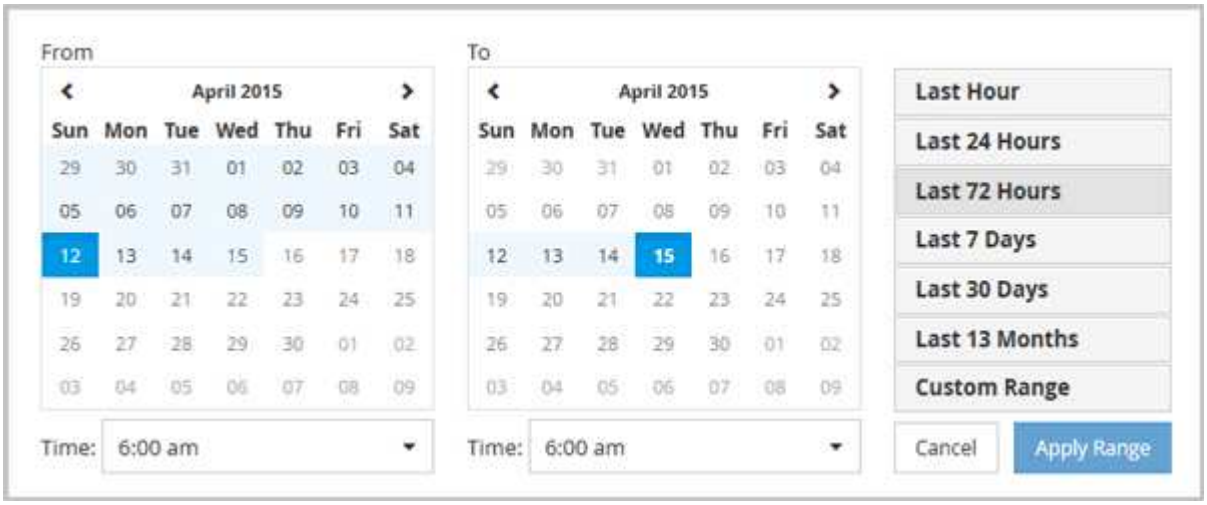
Angeben eines benutzerdefinierten Zeitbereichs in Active IQ Unified Manager

Die Seite „Performance Explorer“ ermöglicht es Ihnen, den Datums- und Zeitbereich für Ihre Performance-Daten festzulegen. Die Angabe eines benutzerdefinierten Zeitraums bietet mehr Flexibilität als die Verwendung vordefinierter Zeitbereiche bei der Verfeinerung von Clusterobjektdaten.

Sie können einen Zeitraum zwischen einer Stunde und 390 Tagen auswählen. 13 Monate entsprechen 390 Tagen, da jeder Monat mit 30 Tagen gezählt wird. Die Angabe eines Datums- und Zeitbereichs liefert detailliertere Informationen und ermöglicht es Ihnen, bestimmte Performance-Ereignisse oder Ereignisreihen genauer zu betrachten. Die Angabe eines Zeitraums erleichtert auch die Fehlerbehebung bei potenziellen Performance-Problemen, da bei der Angabe eines Datums- und Zeitbereichs Daten rund um das Performance-Ereignis detaillierter angezeigt werden. Mit der Option **Zeitbereich** lassen sich vordefinierte Datums- und Zeitbereiche auswählen oder ein eigener benutzerdefinierter Datums- und Zeitbereich von bis zu 390 Tagen angeben. Die Schaltflächen für vordefinierte Zeitbereiche reichen von der **Letzten Stunde** bis zu den **Letzten 13 Monaten**.

Wenn Sie die Option **Letzte 13 Monate** auswählen oder einen benutzerdefinierten Datumsbereich von mehr als 30 Tagen angeben, wird ein Dialogfeld angezeigt, das darauf hinweist, dass für Performance-Daten, die für einen Zeitraum von mehr als 30 Tagen angezeigt werden, stündliche Durchschnittswerte und keine 5-Minuten-Datenabfrage verwendet werden. Daher kann es zu einem Verlust der visuellen Granularität der Zeitachse kommen. Wenn Sie im Dialogfeld auf die Option **Nicht mehr anzeigen** klicken, wird die Meldung nicht angezeigt, wenn Sie die Option **Letzte 13 Monate** auswählen oder einen benutzerdefinierten Datumsbereich von mehr als 30 Tagen angeben. Zusammenfassende Daten gelten auch für einen kleineren Zeitbereich, wenn der Zeitbereich eine Uhrzeit/ein Datum umfasst, die bzw. das mehr als 30 Tage vom heutigen Tag entfernt ist.

Bei der Auswahl eines Zeitraums (benutzerdefiniert oder vordefiniert) basieren Zeiträume von 30 Tagen oder weniger auf Datenstichproben im 5-Minuten-Intervall. Zeiträume von mehr als 30 Tagen basieren auf Datenstichproben im einstündigen Intervall.



1. Nach einem Klick auf das Dropdown-Feld **Zeitbereich** erscheint der Bereich „Zeitbereich“.
2. Für die Auswahl eines vordefinierten Zeitraums ist rechts neben dem Bereich **Time Range** eine der Schaltflächen **Last…** anzuklicken. Bei Auswahl eines vordefinierten Zeitraums stehen Daten für bis zu 13 Monate zur Verfügung. Die ausgewählte Schaltfläche für den vordefinierten Zeitraum wird hervorgehoben, und die entsprechenden Tage und Uhrzeiten werden in den Kalendern und in den Zeitauswahlfeldern angezeigt.
3. Zum Auswählen eines benutzerdefinierten Datumsbereichs wird im Kalender **Von** auf der linken Seite auf das Startdatum geklickt. Zum Vorwärts- oder Rückwärtsnavigieren im Kalender wird auf **<** or **>** geklickt. Zum Festlegen des Enddatums wird im Kalender **Bis** auf der rechten Seite auf ein Datum geklickt. Das Standard-Enddatum ist das aktuelle Datum, sofern kein anderes Enddatum angegeben wird. Die Schaltfläche **Custom Range** rechts im Zeitbereich-Bedienfeld ist hervorgehoben und zeigt damit an, dass ein benutzerdefinierter Datumsbereich ausgewählt wurde.
4. Ein benutzerdefinierter Zeitraum wird über das Steuerelement **Time** unter dem Kalender **From** ausgewählt; dort wird die Startzeit festgelegt. Für die Festlegung der Endzeit dient rechts unter dem Kalender **To** das Steuerelement **Time**; dort wird die Endzeit ausgewählt. Die Schaltfläche **Custom Range** rechts im

Bedienfeld Time Range ist hervorgehoben und zeigt damit an, dass ein benutzerdefinierter Zeitraum ausgewählt wurde.

5. Optional können Sie beim Auswählen eines vordefinierten Datumsbereichs Start- und Endzeitpunkt festlegen. Die Auswahl erfolgt wie zuvor beschrieben zunächst für den vordefinierten Datumsbereich und anschließend für den Start- und Endzeitpunkt. Die ausgewählten Daten werden in den Kalendern hervorgehoben, die von Ihnen festgelegten Start- und Endzeitpunkte werden in den **Time**-Steuerelementen angezeigt, und die Schaltfläche **Custom Range** wird hervorgehoben.
6. Nach Auswahl des Datums- und Zeitbereichs ist **Apply Range** auszuwählen. Die Performance-Statistiken für diesen Zeitraum sind in den Diagrammen und in der Ereigniszeitleiste zu sehen.

Korrelierte Objekte für die grafische Darstellung von Vergleichen im Active IQ Unified Manager definieren

Im Bereich „Zählerdiagramm“ können Sie eine Liste korrelierter Objekte für Daten- und Performance-Vergleiche definieren. Wenn beispielsweise Ihre Storage Virtual Machine (SVM) ein Performance-Problem aufweist, können Sie alle Volumes in der SVM vergleichen, um das Volume zu identifizieren, das das Problem möglicherweise verursacht.

Sie können beliebige Objekte aus dem Raster der korrelierten Objekte in die Bereiche „Vergleichsdiagramm“ und „Zählerdiagramm“ einfügen. Dadurch können Sie Daten mehrerer Objekte sowie des Stammobjekts anzeigen und vergleichen. Objekte lassen sich dem Raster der korrelierten Objekte hinzufügen und daraus entfernen; das Stammobjekt im Vergleichsbereich kann jedoch nicht entfernt werden.

> Das Hinzufügen vieler Objekte zum Vergleichsbereich kann sich negativ auf die Performance auswirken. Zur Aufrechterhaltung der Performance empfiehlt sich die Auswahl einer begrenzten Anzahl von Diagrammen für den Datenvergleich.

Schritte

1. Im Objektraster ist das Objekt zu suchen, das hinzugefügt werden soll, und anschließend die Schaltfläche **Hinzufügen** auszuwählen.

   Die Schaltfläche „Hinzufügen“ wird grau, und das Objekt wird zur Liste der zusätzlichen Objekte im Vergleichsbereich hinzugefügt. Die Daten des Objekts werden den Diagrammen in den Bereichen „Counter Charts“ hinzugefügt. Die Farbe des Augensymbols des Objekts ( ) entspricht der Farbe der Trendlinie der Objektdaten in den Diagrammen.

2. **Optional:** Daten für ausgewählte Objekte ein- oder ausblenden:

Dazu …	Diese Maßnahme durchführen…
Ein ausgewähltes Objekt ausblenden	Im Vergleichsbereich kann auf das Augensymbol ( ) des ausgewählten Objekts geklickt werden. Die Daten des Objekts sind dann ausgeblendet, und das Augensymbol für dieses Objekt wird grau.

Dazu …	Diese Maßnahme durchführen…
Ausgeblendetes Objekt anzeigen	Im Vergleichsbereich auf das graue Augensymbol des ausgewählten Objekts klicken. Das Augensymbol nimmt wieder seine ursprüngliche Farbe an, und die Diagramme im Bereich „Zählerdiagramme“ enthalten wieder die Objektdaten.

3. **Optional:** Ausgewählte Objekte aus dem Bereich **Comparing** entfernen:

Dazu …	Diese Maßnahme durchführen…
Ein ausgewähltes Objekt entfernen	Über dem Namen des ausgewählten Objekts im Vergleichsbereich erscheint die Schaltfläche „Objekt entfernen“ (**X**), sobald sich der Mauszeiger darüber befindet; anschließend kann die Schaltfläche angeklickt werden. Dadurch wird das Objekt aus dem Vergleichsbereich entfernt, und seine Daten werden aus den Zählerdiagrammen gelöscht.
Alle ausgewählten Objekte entfernen	Oben im Vergleichsbereich befindet sich die Schaltfläche „Alle Objekte entfernen“ (**X**). Alle ausgewählten Objekte und ihre Daten werden entfernt, sodass nur das Stammobjekt übrig bleibt.

Zählerdiagramme in Active IQ Unified Manager verstehen

Mit den Diagrammen im Bereich „Zählerdiagramme“ lassen sich Performancedaten für das Stammobjekt und für Objekte anzeigen und vergleichen, die Sie aus der Tabelle „Korrelierte Objekte“ hinzugefügt haben. Dies kann dabei helfen, Performance-Trends zu verstehen sowie Performance-Probleme zu isolieren und zu beheben.

Standardmäßig angezeigte Zählerdiagramme sind Ereignisse, Latenz, IOPS und MBps. Optional anzeigbare Diagramme sind Auslastung, genutzte Performance-Kapazität, verfügbare IOPS, IOPS/TB und Cache-Miss-Verhältnis. Zusätzlich können Sie für die Diagramme Latenz, IOPS, MBps und genutzte Performance-Kapazität Gesamtwerte oder aufgeschlüsselte Werte anzeigen.

Der Performance Explorer zeigt standardmäßig bestimmte Zählerdiagramme an, unabhängig davon, ob das Storage-Objekt sie alle unterstützt oder nicht. Wenn ein Zähler nicht unterstützt wird, ist das Zählerdiagramm leer, und die Meldung `Not applicable for <object>` wird angezeigt.

Die Diagramme zeigen Performance-Trends für das Stammobjekt und für alle im Vergleichsbereich ausgewählten Objekte. Die Daten in den einzelnen Diagrammen sind wie folgt angeordnet:

- **X-Achse**

  Zeigt den angegebenen Zeitraum an. Wenn Sie keinen Zeitraum angegeben haben, wird standardmäßig der vorhergehende 72-Stunden-Zeitraum angezeigt.

- **Y-Achse**

  Zeigt die für das/die ausgewählte(n) Objekt(e) spezifischen Zählereinheiten an.

Die Farben der Trendlinien entsprechen der Farbe des Objektnamens, wie sie im Bereich „Vergleichen“ angezeigt wird. Sie können den Mauszeiger über einen Punkt auf einer beliebigen Trendlinie positionieren, um Details zur Zeit und zum Wert dieses Punkts anzuzeigen.

Wenn Sie einen bestimmten Zeitraum innerhalb eines Diagramms untersuchen möchten, können Sie eine der folgenden Methoden verwenden:

- Mit der Schaltfläche **<** lässt sich der Bereich „Zählerdiagramme“ auf die gesamte Seitenbreite erweitern.
- Mit dem Cursor (wenn er sich in eine Lupe verwandelt) lässt sich ein Teil des Zeitraums im Diagramm auswählen, um den Fokus darauf zu legen und diesen Bereich zu vergrößern. Mit „Reset Chart Zoom“ kehrt das Diagramm zum Standardzeitraum zurück.
- Über die Schaltfläche **Zoom View** lässt sich ein großes Einzelzählerdiagramm mit erweiterten Details und Schwellenwertindikatoren anzeigen.

Gelegentlich treten Lücken in den Trendlinien auf. Diese Lücken bedeuten, dass Unified Manager entweder keine Performance-Daten vom Storage-System erfasst hat oder möglicherweise nicht verfügbar war.

Informationen zu den verschiedenen Typen von Leistungsindikator-Diagrammen in Active IQ Unified Manager

Es gibt Standard Performance-Diagramme, die die Zählerwerte für das ausgewählte Storage-Objekt anzeigen. Jedes der Zählerdiagramme zur Aufschlüsselung zeigt die Gesamtwerte aufgeschlüsselt nach Lese-, Schreib- und anderen Kategorien an. Darüber hinaus zeigen einige Zählerdiagramme zur Aufschlüsselung zusätzliche Details an, wenn das Diagramm in der Zoom-Ansicht angezeigt wird.

Die folgende Tabelle zeigt die verfügbaren Performance-Zählerdiagramme.

Verfügbare Diagramme	Diagrammbeschreibung
Veranstaltungen	Zeigt kritische Ereignisse, Fehler, Warnungen und Informationsereignisse in Korrelation mit den statistischen Diagrammen für das Stammobjekt an. Zusätzlich zu Performance Ereignissen werden Integritätsereignisse angezeigt, um ein vollständiges Bild der Gründe zu liefern, aus denen die Performance beeinträchtigt sein kann.
Latenz - Gesamt	Anzahl der Millisekunden, die zur Beantwortung von Anfragen der Applikation erforderlich sind. Die durchschnittlichen Latenzwerte sind E/A-gewichtet.
Latenz - Aufschlüsselung	Dieselben Informationen wie unter „Latenz insgesamt“, jedoch mit in Lese-, Schreib- und sonstige Latenz aufgeteilten Performance-Daten. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt eine SVM, ein Knoten, ein Aggregat, ein Volume, eine LUN oder ein Namespace ist.

Verfügbare Diagramme	Diagrammbeschreibung
Latenz - Clusterkomponenten	Dieselben Informationen wie unter „Latenz gesamt“, jedoch mit nach Clusterkomponenten aufgeschlüsselten Performance Daten zur Latenz. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volume ist.
IOPS - Gesamt	Anzahl der pro Sekunde verarbeiteten Ein-/Ausgabeoperationen. Bei der Anzeige für einen Knoten zeigt die Auswahl von “Total” die IOPS für Daten an, die über diesen Knoten übertragen werden und sich auf dem lokalen oder dem Remote-Knoten befinden können, und die Auswahl von “Total (Local)” zeigt die IOPS für Daten an, die sich nur auf dem aktuellen Knoten befinden.
IOPS - Aufschlüsselung	Dieselben Informationen wie in „IOPS Gesamt“, jedoch mit den Performance Daten getrennt nach Lese-, Schreib- und sonstigen IOPS. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt eine SVM, ein Knoten, ein Aggregat, ein Volume, eine LUN oder ein Namespace ist. In der Zoom-Ansicht zeigt das Volumendiagramm die minimalen und maximalen QoS-Durchsatzwerte an, sofern diese in ONTAP konfiguriert sind. Bei der Anzeige für einen Knoten zeigt die Auswahl von „`Breakdown`“ die IOPS-Aufschlüsselung für Daten an, die sich durch diesen Knoten bewegen und sich auf dem lokalen oder dem Remote-Knoten befinden können; die Auswahl von „`Breakdown (Local)`“ zeigt die IOPS-Aufschlüsselung für Daten an, die sich nur auf dem aktuellen Knoten befinden.
IOPS - Protokolle	Dieselben Informationen werden in „IOPS Total“ angezeigt, jedoch sind die Performance-Daten in separate Diagramme für CIFS-, NFS-, FCP-, NVMe- und iSCSI-Protokolldatenverkehr unterteilt. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt eine SVM ist.
IOPS/TB - Gesamt	Anzahl der pro Sekunde verarbeiteten Ein-/Ausgabeoperationen, basierend auf dem gesamten vom Workload belegten Speicherplatz, in Terabyte. Auch als E/A-Dichte bezeichnet, misst dieser Zähler, wie viel Performance mit einer bestimmten Storage Kapazität bereitgestellt werden kann. Bei der Anzeige in der Zoom-Ansicht zeigt das Volume-Diagramm die Werte für den erwarteten QoS-Durchsatz und den Spitzendurchsatz an, sofern diese in ONTAP konfiguriert sind. Diese Diagrammoption gilt nur, wenn es sich bei dem ausgewählten Objekt um ein Volume handelt.

Verfügbare Diagramme	Diagrammbeschreibung
MB/s - Gesamt	Anzahl der Megabyte an Daten, die pro Sekunde zum und vom Objekt übertragen werden.
MB/s - Aufschlüsselung	Die gleichen Informationen wie im MB/s-Diagramm, jedoch mit den Durchsatzdaten, getrennt nach Festplattenlesevorgängen, Flash Cache-Lesevorgängen, Schreibvorgängen und Sonstigem. In der Zoom-Ansicht zeigt das Volume-Diagramm die maximalen QoS-Durchsatzwerte an, sofern diese in ONTAP konfiguriert sind. Diese Diagrammoption gilt nur, wenn es sich bei dem ausgewählten Objekt um eine SVM, einen Knoten, ein Aggregat, ein Volume, eine LUN oder einen Namespace handelt. Flash Cache Daten werden nur für Knoten angezeigt, und nur dann, wenn ein Flash Cache Modul auf dem Knoten installiert ist.
Genutzte Performance-Kapazität - Gesamt	Prozentsatz der Performance-Kapazität, den der Knoten oder das Aggregat verbraucht.
Verwendete Performance Kapazität - Aufschlüsselung	Daten zur genutzten Performance-Kapazität, getrennt nach Benutzerprotokollen und Systemhintergrundprozessen. Zusätzlich wird die freie Performance-Kapazität angezeigt.
Verfügbare IOPS - Gesamt	Anzahl der aktuell für dieses Objekt verfügbaren (freien) Ein-/Ausgabeoperationen pro Sekunde. Dieser Wert ergibt sich aus der Differenz zwischen den aktuell genutzten IOPS und den gesamten IOPS, die Unified Manager für das Objekt berechnet. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Knoten oder Aggregat ist.
Auslastung - Gesamt	Prozentualer Anteil der verfügbaren Ressourcen des Objekts, der verwendet wird. Die Auslastung gibt die Knotenauslastung bei Knoten, die Festplattenauslastung bei Aggregaten und die Bandbreitenauslastung bei Ports an. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Knoten, ein Aggregat oder ein Port ist.
Cache-Fehlerrate - Gesamt	Prozentsatz der Leseanfragen von Client-Applikationen, die von der Festplatte statt aus dem Cache beantwortet werden. Diese Diagrammoption gilt nur, wenn es sich bei dem ausgewählten Objekt um ein Volume handelt.

Auswahl der Leistungsdiagramme zur Anzeige in Active IQ Unified Manager

Über die Dropdown-Liste „Diagramme auswählen“ lassen sich die Typen von

Performance-Zählerdiagrammen auswählen, die im Bereich „Zählerdiagramme“ angezeigt werden. Dadurch lassen sich spezifische Daten und Zähler entsprechend Ihren Performance-Anforderungen anzeigen.

Schritte

1. Im Bereich **Zählerdiagramme** erfolgt die Auswahl über die Dropdown-Liste **Diagramme auswählen**.
2. Diagramme hinzufügen oder entfernen:

Zu…	Folgendes ist zu tun…
Einzelne Diagramme hinzufügen oder entfernen	Die Kontrollkästchen neben den Diagrammen dienen zum Ein- oder Ausblenden der gewünschten Diagramme.
Alle Diagramme hinzufügen	Auf **Alle auswählen** klicken
Alle Diagramme entfernen	Auf **Alle abwählen** klicken

Ihre Diagrammauswahl wird im Bereich „Zählerdiagramme“ angezeigt. Beim Hinzufügen von Diagrammen werden neue Diagramme im Bereich „Zählerdiagramme“ so eingefügt, dass sie der Reihenfolge der in der Dropdown-Liste „Diagramme auswählen“ aufgeführten Diagramme entsprechen. Bei der Auswahl weiterer Diagramme ist möglicherweise zusätzliches Scrollen nötig.

Der Bereich „Zählerdiagramme“ in Active IQ Unified Manager kann erweitert werden

Sie können den Bereich „Zählerdiagramme“ erweitern, sodass die Diagramme größer und besser lesbar sind.

Nachdem Sie die Vergleichsobjekte und den Zeitbereich für Zähler definiert haben, können Sie einen größeren Bereich „Counter Charts“ anzeigen. Die Schaltfläche **<** in der Mitte des Performance Explorer Fensters dient zum Erweitern des Bereichs.

Schritt

1. Erweitern oder Verkleinern des Bereichs **Zählerdiagramme**.

Zu…	Folgendes ist zu tun…
Erweiterung des Bereichs „Zählerdiagramme“ auf die Breite der Seite	Die Schaltfläche **<** auswählen
Verkleinern des Bereichs „Zählerdiagramme“ auf die rechte Seitenhälfte	Auf die Schaltfläche **>** klicken

Der Fokus der Zählerdiagramme in Active IQ Unified Manager wird auf einen kürzeren Zeitraum geändert

Sie können mithilfe der Maus den Zeitbereich verkleinern, um sich im Bereich des Zählerdiagramms oder im Fenster der Zoom Ansicht der Zählerdiagramme auf einen bestimmten Zeitraum zu konzentrieren. Dadurch erhalten Sie eine feinkörnigere Ansicht bis auf Mikroebene von beliebigen Teilen der Zeitleiste mit Performance Daten, Ereignissen und Schwellenwerten.

Bevor Sie beginnen

Der Cursor muss sich in eine Lupe geändert haben, was anzeigt, dass diese Funktion aktiv ist.

> Bei Verwendung dieser Funktion, die die Zeitleiste so ändert, dass Werte angezeigt werden, die der feiner granulierten Darstellung entsprechen, ändert sich der Zeit- und Datumsbereich im Auswahlfeld **Time Range** nicht gegenüber den ursprünglichen Werten des Diagramms.

Schritte

1. Zum Vergrößern eines bestimmten Zeitraums wird mit der Lupe geklickt und der Mauszeiger gezogen, um den Bereich hervorzuheben, der im Detail angezeigt werden soll.

   Die Zählerwerte für den von Ihnen ausgewählten Zeitraum füllen das Zählerdiagramm.

2. Für die Rückkehr zum ursprünglichen Zeitraum gemäß Auswahlfeld **Zeitbereich** steht die Schaltfläche **Diagrammzoom zurücksetzen** zur Verfügung.

   Das Zählerdiagramm erscheint in seinem Originalzustand.

Ereignisdetails in der Ereigniszeitleiste von Active IQ Unified Manager anzeigen

Im Bereich „Events Timeline“ des Performance Explorer können Sie alle Ereignisse und die zugehörigen Details anzeigen. Dies ist eine schnelle und effiziente Methode zum Anzeigen aller Systemstatus- und Performance-Ereignisse, die auf dem Stammobjekt innerhalb eines bestimmten Zeitraums aufgetreten sind, was bei der Fehlerbehebung von Performance-Problemen hilfreich sein kann.

Der Bereich „Ereigniszeitleiste“ zeigt kritische, Fehler-, Warn- und Informationsereignisse an, die im ausgewählten Zeitraum für das Stammobjekt aufgetreten sind. Jeder Schweregrad hat eine eigene Zeitleiste. Einzelne und mehrere Ereignisse werden durch einen Ereignispunkt auf der Zeitleiste dargestellt. Die Ereignisdetails sind sichtbar, wenn sich der Mauszeiger über einem Ereignispunkt befindet. Um die visuelle Granularität mehrerer Ereignisse zu erhöhen, kann der Zeitraum verkleinert werden. Dadurch werden mehrere Ereignisse auf einzelne Ereignisse verteilt, sodass jedes Ereignis separat angezeigt und untersucht werden kann.

Jeder Performance-Ereignispunkt auf der Ereigniszeitleiste entspricht vertikal einem entsprechenden Ausschlag in den Trendlinien der Zählerdiagramme, die unterhalb der Ereigniszeitleiste angezeigt werden. Dies stellt einen direkten visuellen Zusammenhang zwischen Ereignissen und der allgemeinen Performance her. Systemstatusereignisse werden ebenfalls auf der Zeitleiste angezeigt, diese Ereignistypen entsprechen jedoch nicht zwangsläufig einem Ausschlag in einem der Performance-Diagramme.

Schritte

1. Im Bereich **Ereigniszeitleiste** wird beim Positionieren des Cursors über einem Ereignispunkt auf der Zeitleiste eine Zusammenfassung des Ereignisses oder der Ereignisse an diesem Ereignispunkt angezeigt.

   Ein Pop-up-Dialog zeigt Informationen zu den Ereignistypen, zu Datum und Uhrzeit des Auftretens der Ereignisse, zum Status und zur Ereignisdauer an.

2. Vollständige Details für ein oder mehrere Ereignisse anzeigen:

Dazu …	Durch Klicken hier…
Details zu einem einzelnen Ereignis anzeigen	**Ereignisdetails anzeigen** im Popup-Dialogfeld.

Dazu …	Durch Klicken hier…
Details für mehrere Ereignisse	**Ereignisdetails anzeigen** im Popup-Dialog. Wenn Sie im Dialogfeld „Mehrere Ereignisse“ auf ein einzelnes Ereignis klicken, wird die entsprechende Seite mit Ereignisdetails angezeigt.

Zoomansicht von Zählerdiagrammen

Informationen zur Zoomansicht in Zählerdiagrammen in Active IQ Unified Manager

Die Zählerdiagramme bieten eine Zoom-Ansicht, mit der Sie die Performance-Details für den von Ihnen angegebenen Zeitraum vergrößert anzeigen können. Dadurch erhalten Sie eine deutlich höhere Granularität bei der Anzeige von Performance-Details und Ereignissen, was bei der Fehlerbehebung von Performance-Problemen von Vorteil ist.

In der Zoom-Ansicht liefern einige der Aufschlüsselungsdiagramme zusätzliche Informationen im Vergleich zur Anzeige ohne Zoom-Ansicht. Beispielsweise zeigen die Zoom-Ansichtsseiten der Aufschlüsselungsdiagramme für IOPS, IOPS/TB und MBps QoS-Richtlinienwerte für Volumes und LUNs an, sofern diese in ONTAP festgelegt wurden.

Für systemdefinierte Performance-Schwellenwertrichtlinien sind in der Liste **Policies** nur die Richtlinien „`Node resources over-utilized`“ und „`QoS throughput limit breached`“ verfügbar. Die anderen systemdefinierten Schwellenwertrichtlinien sind derzeit nicht verfügbar.

Anzeige der Zoomansicht der Zählerdiagramme in Active IQ Unified Manager

Die Counter Charts Zoom View bietet für das ausgewählte Counter Chart und die zugehörige Zeitleiste ein höheres Detail Level. Dies vergrößert die Daten des Counter Chart, sodass Sie eine präzisere Ansicht von Performance Ereignissen und ihren zugrunde liegenden Ursachen erhalten.

Sie können die Zoom-Ansicht des Zählerdiagramms für jedes Zählerdiagramm anzeigen.

Schritte

1. Mit **Zoom View** wird das ausgewählte Diagramm in einem neuen Browserfenster geöffnet.
2. Wenn Sie ein Aufschlüsselungsdiagramm anzeigen und dann auf **Zoom View** klicken, wird das Aufschlüsselungsdiagramm in **Zoom View** angezeigt. In **Zoom View** kann **Total** ausgewählt werden, wenn die Ansichtsoption geändert werden soll.

Der Zeitbereich in der Zoomansicht in Active IQ Unified Manager wird angegeben

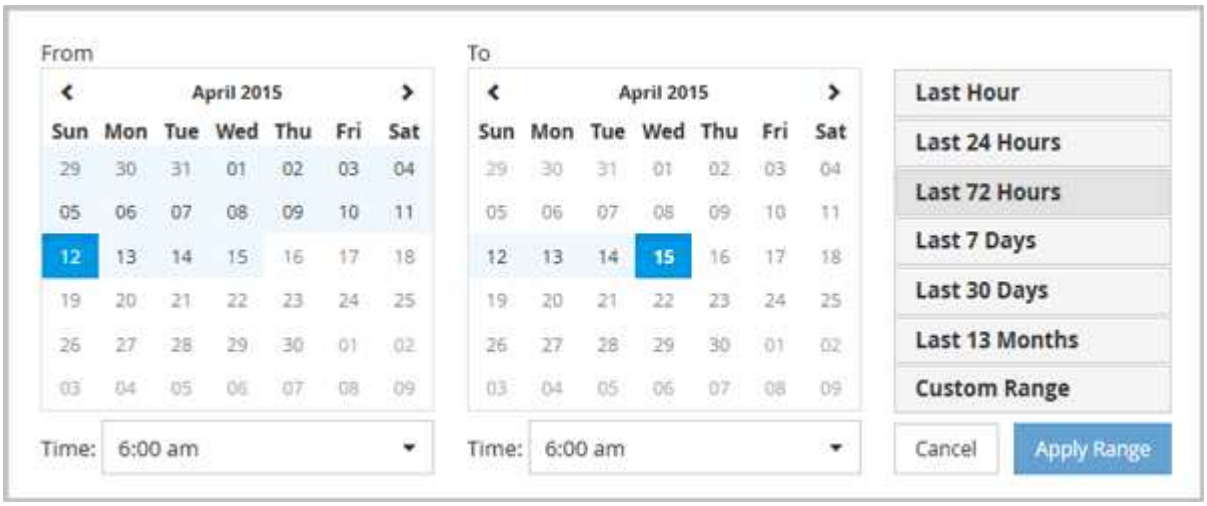
Das Steuerelement **Time Range** im Fenster Counter Charts Zoom View ermöglicht die Angabe eines Datums- und Zeitbereichs für das ausgewählte Diagramm. Dadurch lassen sich bestimmte Daten anhand eines voreingestellten oder eines benutzerdefinierten

Zeitbereichs schnell finden.

Sie können einen Zeitraum zwischen einer Stunde und 390 Tagen auswählen. 13 Monate entsprechen 390 Tagen, da jeder Monat mit 30 Tagen gezählt wird. Die Angabe eines Datums- und Zeitbereichs liefert detailliertere Informationen und ermöglicht es Ihnen, bestimmte Performance-Ereignisse oder Ereignisreihen genauer zu betrachten. Die Angabe eines Zeitraums erleichtert auch die Fehlerbehebung bei potenziellen Performance-Problemen, da bei der Angabe eines Datums- und Zeitbereichs Daten rund um das Performance-Ereignis detaillierter angezeigt werden. Mit der Option **Zeitbereich** lassen sich vordefinierte Datums- und Zeitbereiche auswählen oder ein eigener benutzerdefinierter Datums- und Zeitbereich von bis zu 390 Tagen angeben. Die Schaltflächen für vordefinierte Zeitbereiche reichen von der **Letzten Stunde** bis zu den **Letzten 13 Monaten**.

Wenn Sie die Option **Letzte 13 Monate** auswählen oder einen benutzerdefinierten Datumsbereich von mehr als 30 Tagen angeben, wird ein Dialogfeld angezeigt, das darauf hinweist, dass für Performance-Daten, die für einen Zeitraum von mehr als 30 Tagen angezeigt werden, stündliche Durchschnittswerte und keine 5-Minuten-Datenabfrage verwendet werden. Daher kann es zu einem Verlust der visuellen Granularität der Zeitachse kommen. Wenn Sie im Dialogfeld auf die Option **Nicht mehr anzeigen** klicken, wird die Meldung nicht angezeigt, wenn Sie die Option **Letzte 13 Monate** auswählen oder einen benutzerdefinierten Datumsbereich von mehr als 30 Tagen angeben. Zusammenfassende Daten gelten auch für einen kleineren Zeitbereich, wenn der Zeitbereich eine Uhrzeit/ein Datum umfasst, die bzw. das mehr als 30 Tage vom heutigen Tag entfernt ist.

Bei der Auswahl eines Zeitraums (benutzerdefiniert oder vordefiniert) basieren Zeiträume von 30 Tagen oder weniger auf Datenstichproben im 5-Minuten-Intervall. Zeiträume von mehr als 30 Tagen basieren auf Datenstichproben im einstündigen Intervall.



1. Nach einem Klick auf das Dropdown-Feld **Zeitbereich** erscheint der Bereich „Zeitbereich“.
2. Für die Auswahl eines vordefinierten Zeitraums ist rechts neben dem Bereich **Time Range** eine der Schaltflächen **Last…** anzuklicken. Bei Auswahl eines vordefinierten Zeitraums stehen Daten für bis zu 13 Monate zur Verfügung. Die ausgewählte Schaltfläche für den vordefinierten Zeitraum wird hervorgehoben, und die entsprechenden Tage und Uhrzeiten werden in den Kalendern und in den Zeitauswahlfeldern angezeigt.
3. Zum Auswählen eines benutzerdefinierten Datumsbereichs wird im Kalender **Von** auf der linken Seite auf das Startdatum geklickt. Zum Vorwärts- oder Rückwärtsnavigieren im Kalender wird auf **<** or **>** geklickt. Zum Festlegen des Enddatums wird im Kalender **Bis** auf der rechten Seite auf ein Datum geklickt. Das Standard-Enddatum ist das aktuelle Datum, sofern kein anderes Enddatum angegeben wird. Die Schaltfläche **Custom Range** rechts im Zeitbereich-Bedienfeld ist hervorgehoben und zeigt damit an, dass ein benutzerdefinierter Datumsbereich ausgewählt wurde.

4. Ein benutzerdefinierter Zeitraum wird über das Steuerelement **Time** unter dem Kalender **From** ausgewählt; dort wird die Startzeit festgelegt. Für die Festlegung der Endzeit dient rechts unter dem Kalender **To** das Steuerelement **Time**; dort wird die Endzeit ausgewählt. Die Schaltfläche **Custom Range** rechts im Bedienfeld Time Range ist hervorgehoben und zeigt damit an, dass ein benutzerdefinierter Zeitraum ausgewählt wurde.
5. Optional können Sie beim Auswählen eines vordefinierten Datumsbereichs Start- und Endzeitpunkt festlegen. Die Auswahl erfolgt wie zuvor beschrieben zunächst für den vordefinierten Datumsbereich und anschließend für den Start- und Endzeitpunkt. Die ausgewählten Daten werden in den Kalendern hervorgehoben, die von Ihnen festgelegten Start- und Endzeitpunkte werden in den **Time**-Steuerelementen angezeigt, und die Schaltfläche **Custom Range** wird hervorgehoben.
6. Nach Auswahl des Datums- und Zeitbereichs ist **Apply Range** auszuwählen. Die Performance-Statistiken für diesen Zeitraum sind in den Diagrammen und in der Ereigniszeitleiste zu sehen.

Auswahl von Leistungsschwellenwerten in der Zoomansicht der Zählerdiagramme in Active IQ Unified Manager

Durch das Anwenden von Schwellenwerten in der Zoomansicht der Zählerdiagramme erhalten Sie eine detaillierte Übersicht über das Auftreten von Performance-Schwellenwertereignissen. So können Sie Schwellenwerte anwenden oder entfernen und die Ergebnisse sofort einsehen. Dies kann hilfreich sein, um zu entscheiden, ob die Fehlerbehebung der nächste Schritt sein sollte.

Durch Auswählen von Schwellenwerten in der Zoomansicht der Zählerdiagramme lassen sich präzise Daten zu Performance-Schwellenwertereignissen anzeigen. Sie können jeden Schwellenwert anwenden, der im Bereich **Richtlinien** der Zoomansicht der Zählerdiagramme angezeigt wird.

In der Zoomansicht der Zählerdiagramme kann jeweils nur eine Richtlinie auf das Objekt angewendet werden.

Schritt

1. Auswählen oder Aufheben der Auswahl der , die mit einer Richtlinie verknüpft ist.

   Der ausgewählte Schwellenwert gilt für die Zoomansicht der Zählerdiagramme. Kritische Schwellenwerte werden als rote Linie dargestellt; Warnschwellenwerte werden als gelbe Linie dargestellt.

Volumenlatenz nach Clusterkomponente in Active IQ Unified Manager anzeigen

Detaillierte Latenzinformationen für ein Volume können Sie auf der Seite „Volume Performance Explorer“ einsehen. Das Diagramm „Latenz - Gesamt“ zeigt die Gesamtlatenz des Volumes an, während das Diagramm „Latenz - Aufschlüsselung“ hilfreich ist, um die Auswirkungen von Lese- und Schreiblatenz auf das Volume zu ermitteln.

Zusätzlich bietet das Diagramm „Latenz - Clusterkomponenten“ einen detaillierten Vergleich der Latenz jeder Clusterkomponente, um zu verdeutlichen, wie jede Komponente zur Gesamtlatenz des Volumes beiträgt. Folgende Clusterkomponenten werden angezeigt:

- Netzwerk
- Maximales QoS-Limit
- QoS-Limit (Min.)

- Netzwerkverarbeitung
- Cluster Interconnect
- Data Processing
- Aggregatoperationen
- Volume-Aktivierung
- MetroCluster Ressourcen
- Cloud-Latenz
- Synchrone SnapMirror Beziehung

Schritte

1. Auf der Seite **Volume Performance Explorer** für das ausgewählte Volume erfolgt die Auswahl der Option **Cluster Components** im Dropdown-Menü des Diagramms „Latenz“.

   Das Diagramm „Latenz - Clusterkomponenten“ wird angezeigt.

2. Mit **Zoom View** lässt sich eine größere Version des Diagramms anzeigen.

   Das Vergleichsdiagramm der Clusterkomponenten wird angezeigt. Sie können den Vergleich einschränken, indem Sie die Optionen auswählen oder abwählen, die den einzelnen Clusterkomponenten zugeordnet sind.

3. Zum Anzeigen der einzelnen Werte wird der Cursor in den Diagrammbereich bewegt, damit das Popup-Fenster angezeigt wird.

Anzeige des SVM IOPS Datenverkehrs nach Protokoll in Active IQ Unified Manager

Die Seite „Performance/SVM Explorer“ zeigt detaillierte IOPS-Informationen für eine SVM an. Das Zählerdiagramm „IOPS - Total“ zeigt die gesamte IOPS-Auslastung auf der SVM an, und das Zählerdiagramm „IOPS - Breakdown“ ist hilfreich, um die Auswirkungen von Lese-, Schreib- und anderen IOPS-Vorgängen auf die SVM zu bestimmen.

Zusätzlich zeigt das Diagramm „IOPS - Protokolle“ einen detaillierten Vergleich des IOPS-Verkehrs für jedes auf der SVM verwendete Protokoll. Folgende Protokolle stehen zur Verfügung:

- CIFS
- NFS
- FCP
- iSCSI
- NVMe-FC

Schritte

1. Auf der Seite **Performance/SVM Explorer** für die ausgewählte SVM erfolgt im IOPS-Diagramm die Auswahl von **Protokolle** im Dropdown-Menü.

   Das Diagramm „IOPS - Protokolle“ wird angezeigt.

2. Mit **Zoom View** lässt sich eine größere Version des Diagramms anzeigen.

Die Vergleichstabelle für erweiterte IOPS-Protokolle wird angezeigt. Sie können den Vergleich einschränken, indem Sie die Optionen abwählen oder auswählen, die einem Protokoll zugeordnet sind.

3. Die genauen Werte werden angezeigt, wenn Sie den Cursor in den Diagrammbereich eines der beiden Diagramme bewegen und das Popup-Fenster eingeblendet wird.

Anzeigen von Latenzdiagrammen für Volumes und LUNs zur Überprüfung der Leistungsgarantie in Active IQ Unified Manager

Sie können die Volumes und LUNs anzeigen, die Sie für das Programm “Performance Guarantee” abonniert haben, um zu überprüfen, ob die Latenz den Ihnen garantierten Level nicht überschritten hat.

Die Performance-Garantie für die Latenz ist ein Wert in Millisekunden pro Operation, der nicht überschritten werden sollte. Sie basiert auf einem stündlichen Durchschnitt, nicht auf dem standardmäßigen fünfminütigen Zeitraum der Performance-Erfassung.

Schritte

1. In der Ansicht **Performance: Alle Volumes** oder **Performance: Alle LUNs** kann das Volume oder die LUN ausgewählt werden, das bzw. die von Interesse ist.
2. Für das ausgewählte Volume oder die ausgewählte LUN erfolgt die Auswahl **Stündlicher Durchschnitt** auf der Seite **Performance Explorer** im Auswahlfeld **Statistiken anzeigen in**.

   Die horizontale Linie im Latenzdiagramm zeigt einen gleichmäßigeren Verlauf, wenn die Fünf-Minuten-Erfassungen durch den stündlichen Durchschnitt ersetzt werden.

3. Wenn Sie weitere Volumes auf demselben Aggregat haben, die unter die Performance-Garantie fallen, können Sie diese Volumes hinzufügen, um ihren Latenzwert im selben Diagramm anzuzeigen.

Anzeigen der Leistung für All SAN Array Cluster in Active IQ Unified Manager

In der Ansicht „Performance: Alle Cluster“ kann der Performance Status Ihrer All SAN Array Cluster angezeigt werden.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Übersichtsinformationen für All SAN Array Cluster sind in der Ansicht „Performance: All Clusters“ und Details auf der Seite „Cluster / Performance Explorer“ verfügbar.

Schritte

1. Im linken Navigationsbereich wird **Storage** > **Cluster** ausgewählt.
2. Es muss sichergestellt sein, dass die Spalte “Personality” in der Ansicht **Systemstatus: Alle Cluster** angezeigt wird, oder dass sie über das Steuerelement **Ein-/Ausblenden** hinzugefügt wird.

   In dieser Spalte wird „`All SAN Array`“ für Ihre All SAN Array Cluster angezeigt.

3. Informationen zur Performance in diesen Clustern sind in der Ansicht **Performance: All Clusters** verfügbar.

   Anzeige der Performance-Informationen für den All SAN Array Cluster.

4. Detaillierte Informationen zur Performance in diesen Clustern lassen sich über den Namen eines All SAN Array Clusters aufrufen.
5. Die Registerkarte **Explorer** auswählen.
6. Auf der Seite **Cluster / Performance Explorer** erfolgt die Auswahl von **Nodes on this Cluster** im Menü **View and Compare**.

   Sie können die Performance Statistiken beider Knoten in diesem Cluster vergleichen, um sicherzustellen, dass die Last auf beiden Knoten nahezu identisch ist. Bei größeren Abweichungen zwischen den beiden Knoten können Sie den zweiten Knoten zu den Diagrammen hinzufügen und die Werte über einen längeren Zeitraum vergleichen, um mögliche Konfigurationsprobleme zu identifizieren.

Anzeige der Knoten-IOPS basierend auf lokalen Workloads in Active IQ Unified Manager

Das Diagramm des Knoten-IOPS-Zählers kann hervorheben, wo Vorgänge nur den lokalen Knoten durchlaufen und dabei eine Netzwerk-LIF verwenden, um lesen/schreiben-Vorgänge auf Volumes auf einem Remote-Knoten auszuführen. Die Diagramme „IOPS - `Total (Local)`“ und „`Breakdown (Local)`“ zeigen die IOPS für Daten an, die sich ausschließlich in lokalen Volumes auf dem aktuellen Knoten befinden.

Die “Local”-Versionen dieser Zählerdiagramme ähneln den Knotendiagrammen für Performance-Kapazität und Auslastung, da auch sie nur die Statistiken für Daten anzeigen, die sich auf lokalen Volumes befinden.

Durch den Vergleich der “Local”-Versionen dieser Zählerdiagramme mit den regulären Total Versionen dieser Zählerdiagramme lässt sich erkennen, ob viel Datenverkehr über den lokalen Knoten läuft, um auf Volumes auf dem Remote-Knoten zuzugreifen. Diese Situation kann zu Performance-Problemen führen, die sich möglicherweise durch eine hohe Auslastung des Knotens bemerkbar machen, wenn zu viele Operationen über den lokalen Knoten laufen, um ein Volume auf einem Remote-Knoten zu erreichen. In solchen Fällen kann es sinnvoll sein, ein Volume auf den lokalen Knoten zu verschieben oder auf dem Remote-Knoten eine LIF zu erstellen, mit der sich der Datenverkehr von Hosts verbinden lässt, die auf dieses Volume zugreifen.

Schritte

1. Auf der Seite **Performance/Node Explorer** für den ausgewählten Knoten erfolgt die Auswahl der Option **Total** im Dropdown-Menü des IOPS-Diagramms.

   Das Diagramm „IOPS - Total“ wird angezeigt.

2. Über **Zoom View** lässt sich eine größere Version des Diagramms in einem neuen Browser-Tab anzeigen.
3. Auf der Seite **Performance/Node Explorer** wird im IOPS-Diagramm im Dropdown-Menü **Total (Local)** ausgewählt.

   Das Diagramm „IOPS - Total (Local)“ wird angezeigt.

4. Über **Zoom View** lässt sich eine größere Version des Diagramms in einem neuen Browser-Tab anzeigen.
5. Beide Diagramme lassen sich nebeneinander anzeigen, um Bereiche zu identifizieren, in denen die IOPS-Werte deutlich voneinander abweichen.
6. Wenn sich der Cursor über diesen Bereichen befindet, lassen sich die lokalen und gesamten IOPS für einen bestimmten Zeitpunkt vergleichen.

Komponenten der Landingpages des Objekts

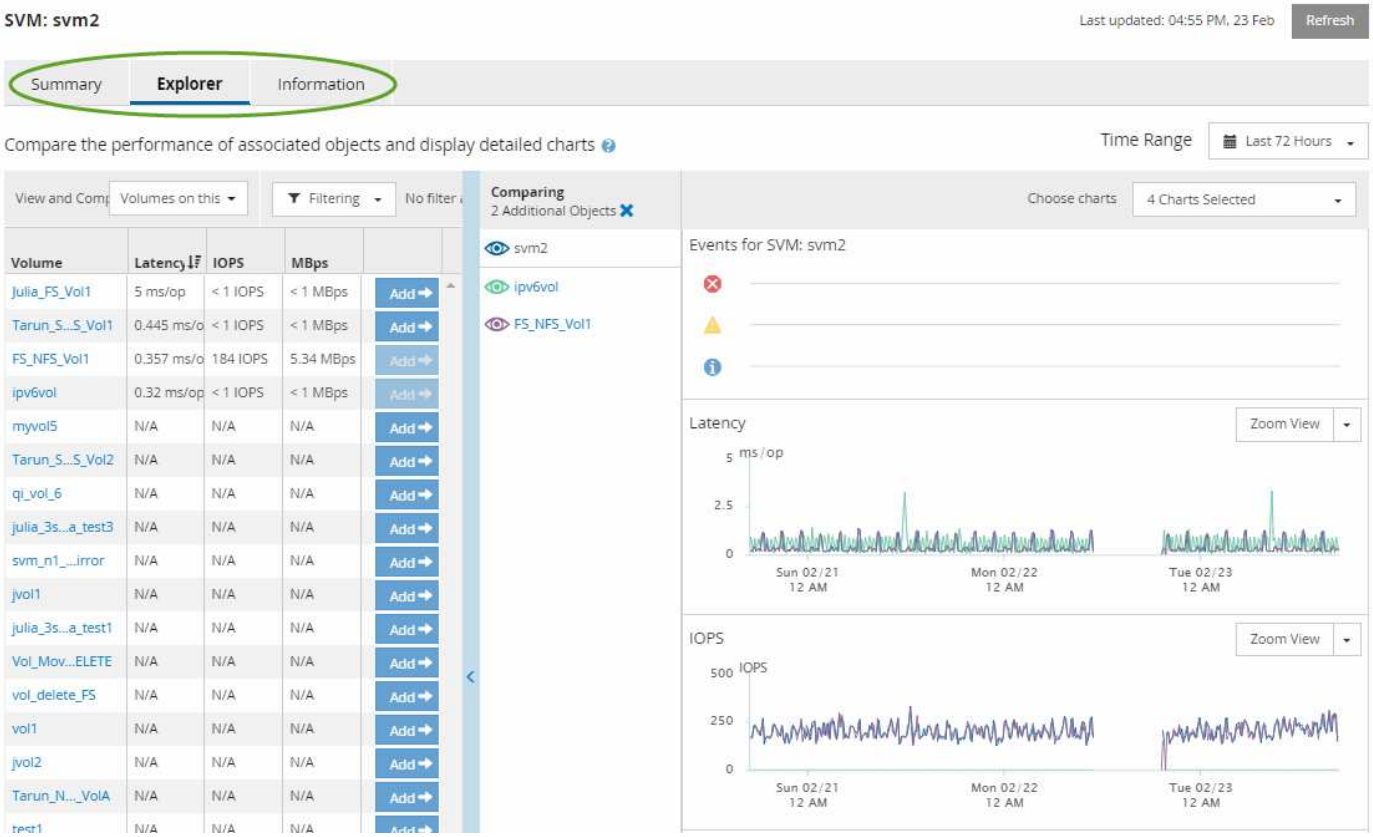
Die Komponenten der Object Landing pages in Active IQ Unified Manager im Überblick

Die Objektübersichtsseiten liefern Details zu allen kritischen, Warn- und Informationsereignissen. Sie bieten einen detaillierten Überblick über die Performance aller Clusterobjekte und ermöglichen es Ihnen, einzelne Objekte über verschiedene Zeiträume hinweg auszuwählen und zu vergleichen.

Die Objekt-Landingpages ermöglichen die Untersuchung der Gesamt-Performance aller Objekte sowie den Vergleich von Objekt-Performance-Daten in einem übersichtlichen Nebeneinanderformat. Dies ist bei der Bewertung der Performance und bei der Fehlerbehebung hilfreich.

Die in den Zählerübersichtsfeldern und Zählerdiagrammen angezeigten Daten basieren auf einem Fünf-Minuten-Stichprobenintervall. Die im Objektinventarraster auf der linken Seite der Seite angezeigten Daten basieren auf einem einstündigen Stichprobenintervall.

Das folgende Bild zeigt ein Beispiel für eine Objekt-Landingpage mit den Explorer-Informationen:



Je nach dem angezeigten Storage Objekt kann die Objektübersichtsseite die folgenden Registerkarten enthalten, die Performance Daten zu dem Objekt bereitstellen:

- Zusammenfassung

  Die Anzeige umfasst drei oder vier Zählerdiagramme, die die Ereignisse und die Performance pro Objekt für den vorangegangenen Zeitraum von 72 Stunden enthalten, einschließlich einer Trendlinie, die die Höchst- und Tiefstwerte während dieses Zeitraums anzeigt.

- Explorer

  Zeigt ein Raster von Storage-Objekten an, die mit dem aktuellen Objekt verknüpft sind, wodurch sich die Performance-Werte des aktuellen Objekts mit denen der verknüpften Objekte vergleichen lassen. Diese Registerkarte enthält bis zu elf Zählerdiagramme und eine Zeitbereichsauswahl, mit denen sich verschiedene Vergleiche durchführen lassen.

- Informationen

  Zeigt Werte für Konfigurationsattribute des Storage-Objekts an, die nicht die Performance betreffen, einschließlich der installierten Version der ONTAP-Software, des Namens des HA-Partners sowie der Anzahl der Ports und LIFs.

- Spitzenleister

  Für Cluster: Zeigt die Storage Objekte mit der höchsten bzw. niedrigsten Performance an, basierend auf dem von Ihnen ausgewählten Performance-Zähler.

- Failover-Planung

  Für Knoten: Zeigt die geschätzte Auswirkung auf die Performance eines Knotens an, wenn der HA-Partner des Knotens ausfällt.

- Details

  Für Volumes: Zeigt detaillierte Performance-Statistiken für alle E/A-Aktivitäten und -Operationen der ausgewählten Volume-Workload an. Diese Registerkarte ist für FlexVol Volumes, FlexGroup Volumes und Bestandteile von FlexGroups verfügbar.

Die Seite „Leistungsübersicht“ in Active IQ Unified Manager

Die Übersichtsseite zeigt Zählerdiagramme mit Details zu den Ereignissen und zur Performance pro Objekt für den vorherigen 72-Stunden-Zeitraum. Diese Daten werden nicht automatisch aktualisiert, sondern entsprechen dem Stand des letzten Seitenaufrufs. Die Diagramme auf der Übersichtsseite beantworten die Frage „*Muss ich genauer prüfen?*“

Diagramme und Zählerstatistiken

Die Übersichtsdiagramme bieten einen schnellen allgemeinen Überblick für den Zeitraum der letzten 72 Stunden und helfen Ihnen, mögliche Probleme zu identifizieren, die einer weiteren Untersuchung bedürfen.

Die Zählerstatistiken auf der Seite „Summary“ werden in Diagrammen dargestellt.

Sie können den Cursor über die Trendlinie in einem Diagramm bewegen, um die Zählerwerte für einen bestimmten Zeitpunkt anzuzeigen. Die Übersichtsdiagramme zeigen außerdem die Gesamtzahl der aktiven kritischen Ereignisse und Warnmeldungen für den vorangegangenen 72-Stunden-Zeitraum für die folgenden Zähler an:

- **Latenz**

  Durchschnittliche Antwortzeit für alle E/A-Anforderungen; angegeben in Millisekunden pro Operation.

  Wird für alle Objekttypen angezeigt.

- **IOPS**

  Durchschnittliche Betriebsgeschwindigkeit; angegeben in Eingabe-/Ausgabeoperationen pro Sekunde.

  Wird für alle Objekttypen angezeigt.

- **MB/s**

  Durchschnittlicher Durchsatz; angegeben in Megabyte pro Sekunde.

  Wird für alle Objekttypen angezeigt.

- **Genutzte Performance Kapazität**

  Prozentsatz der Performancekapazität, der von einem Knoten oder Aggregat verbraucht wird.

  Wird nur für Knoten und Aggregate angezeigt.

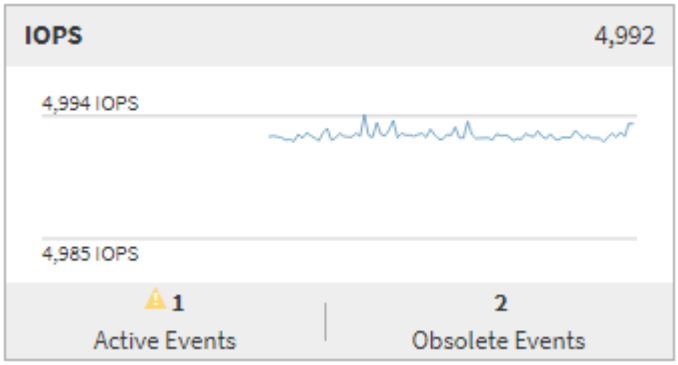
- **Auslastung**

  Prozentuale Objektauslastung für Knoten und Aggregate bzw. Bandbreitenauslastung für Ports.

  Wird nur für Knoten, Aggregate und Ports angezeigt.

Beim Positionieren des Cursors über der Ereignisanzahl für aktive Ereignisse werden Typ und Anzahl der Ereignisse angezeigt. Kritische Ereignisse werden rot (🟥) und Warnereignisse gelb (🟨) angezeigt.

Die Zahl oben rechts im Diagramm im grauen Balken ist der Durchschnittswert der letzten 72 Stunden. Die Zahlen unten und oben im Trendliniendiagramm sind die Minimal- und Maximalwerte der letzten 72 Stunden. Der graue Balken unter dem Diagramm enthält die Anzahl aktiver (neuer und bestätigter) Ereignisse und veralteter Ereignisse der letzten 72 Stunden.



- **Latenzzählerdiagramm**

  Das Diagramm des Latenzzählers bietet einen Überblick über die Objektlatenz im vorangegangenen 72-Stunden-Zeitraum. Latenz bezeichnet die durchschnittliche Antwortzeit für alle E/A-Anforderungen; ausgedrückt in Millisekunden pro Operation entspricht sie der Servicezeit, der Wartezeit oder beidem, die bzw. das ein Datenpaket oder Datenblock in der betrachteten Cluster Storage Komponente erfährt.

  Oberer Wert (Zählerwert): Die Zahl in der Kopfzeile zeigt den Durchschnitt für den vorangegangenen Zeitraum von 72 Stunden an.

  Mitte (Performance-Diagramm): Der Wert unten im Diagramm zeigt die niedrigste, der Wert oben die höchste Latenz der letzten 72 Stunden an. Wenn sich der Mauszeiger über der Trendlinie befindet, wird

der Latenzwert für einen bestimmten Zeitpunkt angezeigt.

Unten (Ereignisse): Beim Überfahren mit der Maus zeigt das Pop-up die Details der Ereignisse an. Über den Link **Active Events** unterhalb des Diagramms gelangen Sie zur Seite „Ereignisinventar“, auf der die vollständigen Ereignisdetails angezeigt werden.

- **IOPS-Zählerdiagramm**

  Das IOPS-Zählerdiagramm bietet einen allgemeinen Überblick über den IOPS-Systemstatus des Objekts für den vorangegangenen Zeitraum von 72 Stunden. IOPS gibt die Geschwindigkeit des Storage-Systems in der Anzahl der Ein-/Ausgabeoperationen pro Sekunde an.

  Oberer Wert (Zählerwert): Die Zahl in der Kopfzeile zeigt den Durchschnitt für den vorangegangenen Zeitraum von 72 Stunden an.

  Mitte (Performance-Diagramm): Der Wert unten im Diagramm zeigt den niedrigsten IOPS-Wert, der Wert oben im Diagramm den höchsten IOPS-Wert der vorangegangenen 72 Stunden an. Die Position des Mauszeigers über der Trendlinie zeigt den IOPS-Wert für einen bestimmten Zeitpunkt an.

  Unten (Ereignisse): Beim Überfahren mit der Maus zeigt das Pop-up die Details der Ereignisse an. Über den Link **Active Events** unterhalb des Diagramms gelangen Sie zur Seite „Ereignisinventar“, auf der die vollständigen Ereignisdetails angezeigt werden.

- **MB/s-Zählerdiagramm**

  Das MB/s-Zählerdiagramm zeigt die MB/s-Performance des Objekts und gibt an, wie viele Daten in Megabyte pro Sekunde zum Objekt und vom Objekt übertragen wurden. Das MB/s-Zählerdiagramm bietet einen allgemeinen Überblick über den MB/s-Systemstatus des Objekts für den vorangegangenen Zeitraum von 72 Stunden.

  Top (Zählerwert): Die Zahl in der Kopfzeile zeigt die durchschnittliche Anzahl an MB/s für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Performance-Diagramm): Der Wert unten im Diagramm zeigt den niedrigsten MB/s-Wert, und der Wert oben im Diagramm zeigt den höchsten MB/s-Wert für den vorangegangenen 72-Stunden-Zeitraum an. Der MB/s-Wert für einen bestimmten Zeitpunkt wird angezeigt, wenn sich der Mauszeiger über der Trendlinie im Diagramm befindet.

  Unten (Ereignisse): Beim Überfahren mit der Maus zeigt das Pop-up die Details der Ereignisse an. Über den Link **Active Events** unterhalb des Diagramms gelangen Sie zur Seite „Ereignisinventar“, auf der die vollständigen Ereignisdetails angezeigt werden.

- **Diagramm des Zählers „Performance Capacity Used“**

  Das Zählerdiagramm „Verwendete Performance-Kapazität“ zeigt den Prozentsatz der Performance-Kapazität an, die das Objekt verbraucht.

  Oben (Zählerwert): Die Zahl in der Kopfzeile zeigt die durchschnittlich genutzte Performancekapazität für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Performance-Diagramm): Der Wert am unteren Rand des Diagramms zeigt den niedrigsten Prozentsatz der genutzten Performance-Kapazität an, und der Wert am oberen Rand des Diagramms zeigt den höchsten Prozentsatz der genutzten Performance-Kapazität für den vorangegangenen Zeitraum von 72 Stunden an. Wenn Sie den Mauszeiger über die Trendlinie im Diagramm bewegen, wird der Wert der genutzten Performance-Kapazität für einen bestimmten Zeitpunkt angezeigt.

Unten (Ereignisse): Beim Überfahren mit der Maus zeigt das Pop-up die Details der Ereignisse an. Über den Link **Active Events** unterhalb des Diagramms gelangen Sie zur Seite „Ereignisinventar“, auf der die vollständigen Ereignisdetails angezeigt werden.

- **Auslastungszählerdiagramm**

  Das Zählerdiagramm für die Auslastung zeigt die prozentuale Auslastung des Objekts an. Das Zählerdiagramm für die Auslastung bietet einen allgemeinen Überblick über den prozentualen Auslastungsgrad des Objekts oder die Bandbreitenauslastung im vorangegangenen 72-Stunden-Zeitraum.

  Top (Zählerwert): Die Zahl in der Kopfzeile zeigt den durchschnittlichen Auslastungsgrad für den vorangegangenen Zeitraum von 72 Stunden an.

  Mitte (Performance-Diagramm): Der Wert unten im Diagramm zeigt den niedrigsten Auslastungsprozentsatz an, und der Wert oben im Diagramm zeigt den höchsten Auslastungsprozentsatz für den vorhergehenden Zeitraum von 72 Stunden an. Mit dem Mauszeiger über der Trendlinie ist der Auslastungswert für einen bestimmten Zeitpunkt sichtbar.

  Unten (Ereignisse): Beim Überfahren mit der Maus zeigt das Pop-up die Details der Ereignisse an. Über den Link **Active Events** unterhalb des Diagramms gelangen Sie zur Seite „Ereignisinventar“, auf der die vollständigen Ereignisdetails angezeigt werden.

Veranstaltungen

Die Ereignisverlaufstabelle listet, sofern vorhanden, die zuletzt für das jeweilige Objekt aufgetretenen Ereignisse auf. Ein Klick auf den Ereignisnamen zeigt auf der Seite „Ereignisdetails“ Details zum Ereignis an.

Die Seite „Performance Explorer“ in Active IQ Unified Manager kann überprüft werden.

Die Seite „Performance Explorer“ ermöglicht den Vergleich der Performance ähnlicher Objekte in einem Cluster, beispielsweise aller Volumes in einem Cluster. Dies ist bei der Fehlerbehebung von Performance-Ereignissen und bei der Feinabstimmung der Objekt-Performance hilfreich. Objekte können außerdem mit dem Root-Objekt verglichen werden, das die Basis bildet, mit der andere Objektvergleiche durchgeführt werden.

Sie können auf die Schaltfläche **Zur Systemstatusansicht wechseln** klicken, um die Seite mit den Systemstatusdetails für dieses Objekt anzuzeigen. In manchen Fällen erhalten Sie wichtige Informationen zu den Storage-Konfigurationseinstellungen dieses Objekts, die bei der Fehlerbehebung hilfreich sein können.

Die Seite „Performance Explorer“ zeigt eine Liste der Clusterobjekte und ihrer Performancedaten. Auf dieser Seite werden alle Clusterobjekte desselben Typs (z. B. Volumes und ihre objektspezifischen Performance-Statistiken) in Tabellenform angezeigt. Diese Ansicht bietet einen effizienten Überblick über die Performance der Clusterobjekte.

Wenn in einer Zelle der Tabelle “N/A” erscheint, bedeutet dies, dass für diesen Zähler kein Wert verfügbar ist, da zu diesem Zeitpunkt keine Ein-/Ausgabe für dieses Objekt stattfindet.

Die Seite „Performance Explorer“ enthält die folgenden Komponenten:

- **Zeitraum**

  Ermöglicht die Auswahl eines Zeitbereichs für die Objektdaten.

Sie können einen vordefinierten Zeitraum auswählen oder einen eigenen benutzerdefinierten Zeitraum festlegen.

- **Anzeigen und vergleichen**

  Hier können Sie auswählen, welcher Typ korrelierter Objekte im Raster angezeigt wird.

  Die verfügbaren Optionen hängen vom Stammobjekttyp und den verfügbaren Daten ab. In der Dropdown-Liste „Anzeigen und Vergleichen“ lässt sich ein Objekttyp auswählen. Der ausgewählte Objekttyp wird in der Liste angezeigt.

- **Filtern**

  Ermöglicht es Ihnen, die Datenmenge, die Sie erhalten, anhand Ihrer Vorgaben einzugrenzen.

  Sie können Filter erstellen, die auf die Objektdaten angewendet werden, zum Beispiel IOPS größer als 4. Sie können bis zu vier Filter gleichzeitig hinzufügen.

- **Vergleich**

  Zeigt eine Liste der Objekte an, die Sie zum Vergleich mit dem Stammobjekt ausgewählt haben.

  Die Daten für die Objekte im Vergleichsbereich werden in den Zählerdiagrammen angezeigt.

- **Statistiken anzeigen in**

  Für Volumes und LUNs können Sie auswählen, ob die Statistiken nach jedem Erfassungszyklus (standardmäßig 5 Minuten) angezeigt oder als stündlicher Durchschnitt dargestellt werden. Mit dieser Funktion können Sie das Latenzdiagramm zur Unterstützung des NetApp „Performance Guarantee“-Programms anzeigen.

- **Zählerdiagramme**

  Zeigt grafisch dargestellte Daten für jede Performance Kategorie an.

  In der Regel werden standardmäßig nur drei oder vier Diagramme angezeigt. Über die Komponente „Diagramme auswählen“ können Sie weitere Diagramme einblenden oder bestimmte Diagramme ausblenden. Sie können außerdem die Ereignis-Zeitleiste ein- oder ausblenden.

- **Zeitleiste der Ereignisse**

  Zeigt Performance- und Systemstatusereignisse an, die auf der Zeitachse für den Zeitraum auftreten, den Sie in der Zeitbereichskomponente ausgewählt haben.

Performance mithilfe von QoS-Richtliniengruppeninformationen managen

Verwaltung der Performance mithilfe von QoS-Richtliniengruppeninformationen in Active IQ Unified Manager

Unified Manager ermöglicht die Anzeige der QoS-Richtliniengruppen (Quality of Service), die auf allen überwachten Clustern verfügbar sind. Die Richtlinien können mit ONTAP Software (System Manager oder ONTAP CLI) oder über die Unified Manager

Performance Service Level-Richtlinien definiert worden sein. Unified Manager zeigt außerdem an, bei welchen Volumes und LUNs eine QoS-Richtliniengruppe zugewiesen ist.

Weitere Informationen zum Anpassen der QoS-Einstellungen finden Sie unter "Überblick über das Performance-Management"

Steuerung des Workload-Durchsatzes mit Storage QoS in Active IQ Unified Manager

Sie können eine QoS-Richtliniengruppe (Quality of Service) erstellen, um das Limit für E/A-Vorgänge pro Sekunde (IOPS) oder den Durchsatz (MB/s) der darin enthaltenen Workloads zu steuern. Wenn sich die Workloads in einer Richtliniengruppe ohne festgelegtes Limit befinden, z. B. in der Standardrichtliniengruppe, oder das festgelegte Limit nicht Ihren Anforderungen entspricht, können Sie das Limit erhöhen oder die Workloads in eine neue oder vorhandene Richtliniengruppe mit dem gewünschten Limit verschieben.

„`Traditional`“ QoS-Richtliniengruppen können einzelnen Workloads zugewiesen werden, beispielsweise einem einzelnen Volume oder einer LUN. In diesem Fall kann der Workload die volle Durchsatzbegrenzung nutzen. QoS-Richtliniengruppen können auch mehreren Workloads zugewiesen werden; in diesem Fall wird die Durchsatzbegrenzung von den Workloads „`shared`“ genutzt. Beispielsweise würde ein QoS-Limit von 9.000 IOPS, das drei Workloads zugewiesen ist, die kombinierten IOPS auf maximal 9.000 IOPS begrenzen.

“Adaptive” QoS-Richtliniengruppen können auch einzelnen Workloads oder mehreren Workloads zugewiesen werden. Selbst bei einer Zuweisung zu mehreren Workloads erhält jeder Workload die volle Durchsatzbegrenzung, anstatt sich den Durchsatzwert mit anderen Workloads zu teilen. Außerdem passen adaptive QoS-Richtlinien die Durchsatzeinstellung pro Workload automatisch anhand der Volume-Größe an und halten dadurch das Verhältnis von IOPS zu Terabyte aufrecht, wenn sich die Größe des Volume ändert. Wenn beispielsweise der Spitzenwert in einer adaptiven QoS-Richtlinie auf 5.000 IOPS/TB festgelegt ist, hat ein 10-TB-Volume einen maximalen Durchsatz von 50.000 IOPS. Wenn das Volume später auf 20 TB geändert wird, passt adaptive QoS den Maximalwert auf 100.000 IOPS an.

Ab ONTAP 9.5 kann die Blockgröße beim Definieren einer adaptiven QoS-Richtlinie berücksichtigt werden. Dadurch wird die Richtlinie effektiv von einem IOPS/TB-Schwellenwert auf einen MB/s-Schwellenwert umgestellt, wenn Workloads sehr große Blockgrößen verwenden und somit einen großen Teil des Durchsatzes beanspruchen.

Bei gemeinsam genutzten QoS-Gruppenrichtlinien drosselt die Richtliniengruppe die Workloads, um ihre Aktivität einzuschränken, wenn die IOPS oder MB/s aller Workloads in einer Richtliniengruppe den festgelegten Grenzwert überschreiten, wodurch die Performance aller Workloads in der Richtliniengruppe sinken kann. Wenn durch die Drosselung der Richtliniengruppe ein dynamisches Performance-Ereignis erzeugt wird, zeigt die Ereignisbeschreibung den Namen der betroffenen Richtliniengruppe an.

In der Ansicht „Performance: All Volumes“ können Sie die betroffenen Volumes nach IOPS und MB/s sortieren, um festzustellen, welche Workloads die höchste Auslastung aufweisen und möglicherweise zu dem Ereignis beigetragen haben. Auf der Seite „Performance/Volumes Explorer“ können Sie andere Volumes oder LUNs auf dem Volume auswählen, um deren IOPS- oder MBps-Durchsatznutzung mit der des betroffenen Workloads zu vergleichen.

Durch die Zuweisung von Workloads, die die Knotenressourcen übermäßig beanspruchen, zu einer restriktiveren Richtliniengruppeneinstellung wird die Aktivität dieser Workloads gedrosselt, wodurch die

Ressourcennutzung auf dem betreffenden Knoten reduziert werden kann. Wenn der Workload jedoch mehr Knotenressourcen nutzen können soll, lässt sich der Wert der Richtliniengruppe erhöhen.

Sie können den System Manager, die ONTAP-Befehle oder die Unified Manager Performance Service Levels verwenden, um Richtliniengruppen zu managen, einschließlich der folgenden Aufgaben:

- Erstellen einer Richtliniengruppe
- Hinzufügen oder Entfernen von Workloads in einer Richtliniengruppe
- Verschieben einer Workload zwischen Richtliniengruppen
- Ändern der Durchsatzbegrenzung einer Richtliniengruppe
- Verschieben einer Workload auf ein anderes Aggregat und/oder einen anderen Knoten

In Active IQ Unified Manager verfügbare QoS-Richtliniengruppen auf allen Clustern anzeigen

Sie können eine Liste aller QoS-Richtliniengruppen anzeigen, die auf den von Unified Manager überwachten Clustern verfügbar sind. Dies umfasst herkömmliche QoS-Richtlinien, adaptive QoS-Richtlinien und QoS-Richtlinien, die durch Unified Manager Performance Service Level Richtlinien verwaltet werden.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **QoS-Richtliniengruppen**.

   Standardmäßig wird die Ansicht „Performance: Herkömmliche QoS-Richtliniengruppen“ angezeigt.

2. Die detaillierten Konfigurationseinstellungen für jede verfügbare traditionelle QoS-Richtliniengruppe werden angezeigt.
3. Über die Schaltfläche zum Erweitern ( ) neben dem Namen der QoS-Richtliniengruppe können weitere Details zur Richtliniengruppe aufgerufen werden.
4. Im Menü „Ansicht“ kann eine der zusätzlichen Optionen ausgewählt werden, um alle adaptiven QoS-Richtliniengruppen oder alle QoS-Richtliniengruppen anzuzeigen, die mit Unified Manager Performance Service Levels erstellt wurden.

Anzeige von Volumes oder LUNs innerhalb derselben QoS-Richtliniengruppe in Active IQ Unified Manager

Sie können eine Liste der Volumes und LUNs anzeigen, die derselben QoS-Richtliniengruppe zugewiesen wurden.

Bei herkömmlichen QoS-Richtliniengruppen, die von mehreren Volumes “shared” genutzt werden, kann dies hilfreich sein, um festzustellen, ob bestimmte Volumes den für die Richtliniengruppe definierten Durchsatz übermäßig nutzen. Dies kann auch bei der Entscheidung helfen, ob weitere Volumes zur Richtliniengruppe hinzugefügt werden können, ohne die anderen Volumes negativ zu beeinflussen.

Bei adaptiven QoS-Richtlinien und Unified Manager Performance Service Levels Richtlinien kann es hilfreich sein, alle Volumes oder LUNs anzuzeigen, die eine Richtliniengruppe verwenden, damit ersichtlich ist, welche Objekte betroffen wären, wenn die Konfigurationseinstellungen für die QoS-Richtlinie geändert würden.

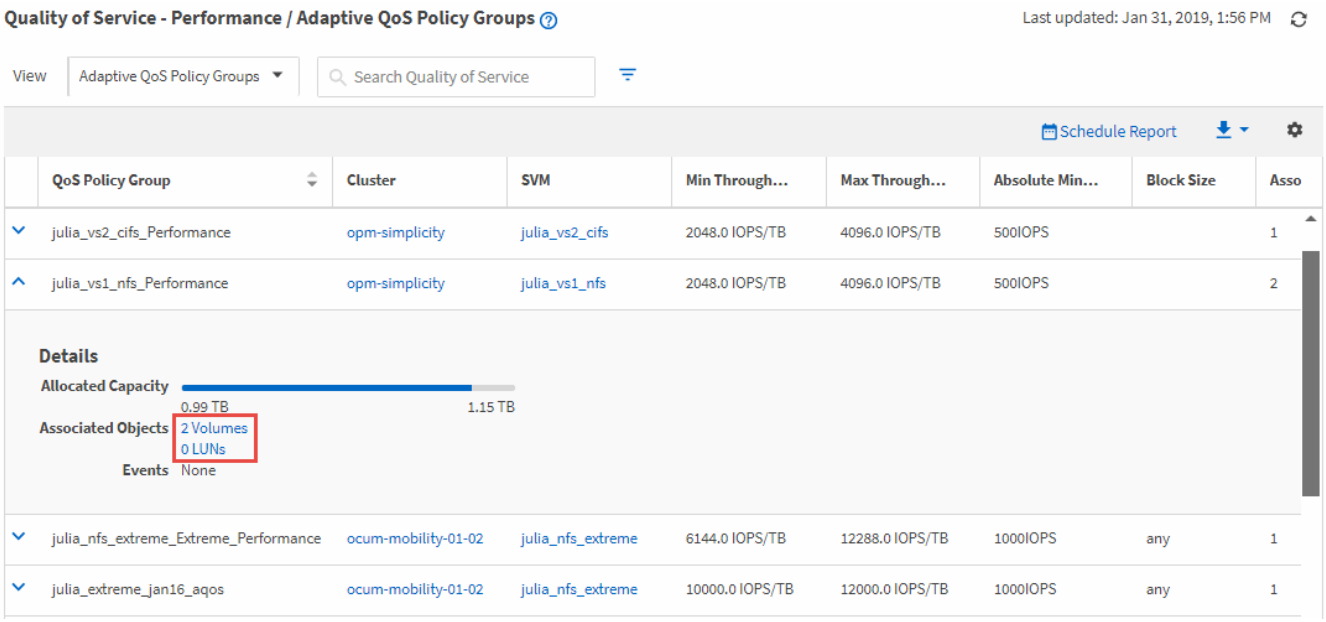
Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **QoS-Richtliniengruppen**.

   Standardmäßig wird die Ansicht „Performance: Herkömmliche QoS-Richtliniengruppen“ angezeigt.

2. Wenn Sie an der herkömmlichen Richtliniengruppe interessiert sind, bleiben Sie auf dieser Seite. Andernfalls bietet eine der zusätzlichen Ansichtsoptionen die Möglichkeit, alle adaptiven QoS-Richtliniengruppen oder alle QoS-Richtliniengruppen anzuzeigen, die von Unified Manager Performance Service Levels erstellt wurden.

3. In der gewünschten QoS-Richtlinie lassen sich über die Schaltfläche zum Erweitern ( ) neben dem Namen der QoS Policy Group weitere Details anzeigen.



4. Über den Link „Volumes“ oder „LUNs“ werden die Objekte angezeigt, die diese QoS-Richtlinie verwenden.

   Die Seite „Performance-Inventar“ für Volumes oder LUNs zeigt die sortierte Liste der Objekte an, die die QoS-Richtlinie verwenden.

QoS-Richtliniengruppeneinstellungen für Volumes oder LUNs in Active IQ Unified Manager anzeigen

Sie können die QoS-Richtliniengruppen anzeigen, die auf Ihre Volumes und LUNs angewendet wurden, und zur Ansicht „Performance/QoS Policy Groups“ wechseln, um die detaillierten Konfigurationseinstellungen für jede QoS-Richtlinie anzuzeigen.

Die Schritte zum Anzeigen der auf ein Volume angewendeten QoS-Richtlinie werden im Folgenden beschrieben. Die Schritte zum Anzeigen dieser Informationen für eine LUN sind ähnlich.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.

   Standardmäßig wird die Ansicht „Systemstatus: Alle Volumes“ angezeigt.

2. Im Menü „Ansicht“ können Sie **Performance: Volumes in QoS Policy Group** auswählen.

3. Das Volume, das Sie überprüfen möchten, finden Sie, wenn Sie nach rechts bis zur Spalte **QoS Policy Group** scrollen.

4. Den Namen der QoS-Richtliniengruppe auswählen.

   Je nachdem, ob es sich um eine traditionelle QoS-Richtlinie, eine adaptive QoS-Richtlinie oder eine QoS-Richtlinie handelt, die mithilfe von Unified Manager Performance Service Levels erstellt wurde, wird die entsprechende Quality of Service Seite angezeigt.

5. Die detaillierten Konfigurationseinstellungen für die QoS-Richtliniengruppe können angezeigt werden.
6. Über die Schaltfläche zum Erweitern ( ) neben dem Namen der QoS-Richtliniengruppe können weitere Details zur Richtliniengruppe aufgerufen werden.

Vergleich von Volumes oder LUNs innerhalb derselben QoS-Richtliniengruppe in Active IQ Unified Manager

Sie können die Volumes und LUNs anzeigen, die sich in denselben QoS-Richtliniengruppen befinden, und dann die Performance in einem einzigen IOPS-, MB/s- oder IOPS/TB-Diagramm vergleichen, um etwaige Probleme zu identifizieren.

Die Schritte zum Vergleich der Performance von Volumes in derselben QoS-Richtliniengruppe werden im Folgenden beschrieben. Die Schritte zum Anzeigen dieser Informationen für eine LUN sind ähnlich.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.

   Standardmäßig wird die Ansicht „Systemstatus: Alle Volumes“ angezeigt.

2. Im Menü „Ansicht“ können Sie **Performance: Volumes in QoS Policy Group** auswählen.
3. Der Name des Volume, das überprüft werden soll, ist auszuwählen.

   Für das Volume erscheint die Seite „Performance Explorer“.

4. Im Menü „Ansicht und Vergleich“ ist **Volumes in derselben QoS-Richtliniengruppe** auszuwählen.

   Die anderen Volumes, die dieselbe QoS-Richtlinie verwenden, sind in der folgenden Tabelle aufgeführt.

5. Mit der Schaltfläche **Hinzufügen** werden diese Volumes zu den Diagrammen hinzugefügt, sodass die IOPS, MB/s, IOPS/TB und andere Performance-Zähler für alle ausgewählten Volumes in den Diagrammen verglichen werden können.

   Sie können den Zeitraum ändern, um die Performance über andere Zeitintervalle als den Standardwert von 72 Stunden anzuzeigen.

QoS-Richtlinien in Durchsatzdiagrammen mit Active IQ Unified Manager anzeigen

Die von ONTAP definierten QoS-Richtlinieneinstellungen (Quality of Service), die auf ein Volume oder eine LUN angewendet wurden, lassen sich im Performance Explorer sowie in den Workload Analysis-Diagrammen für IOPS, IOPS/TB und MB/s anzeigen. Die in den Diagrammen angezeigten Informationen unterscheiden sich je nach Typ der QoS-Richtlinie, die auf die Workload angewendet wurde.

Die Einstellung „Durchsatzmaximum“ (oder „`peak`“) definiert den maximalen Durchsatz, den die Arbeitslast belegen kann, und begrenzt dadurch die Auswirkungen auf konkurrierende Arbeitslasten hinsichtlich der

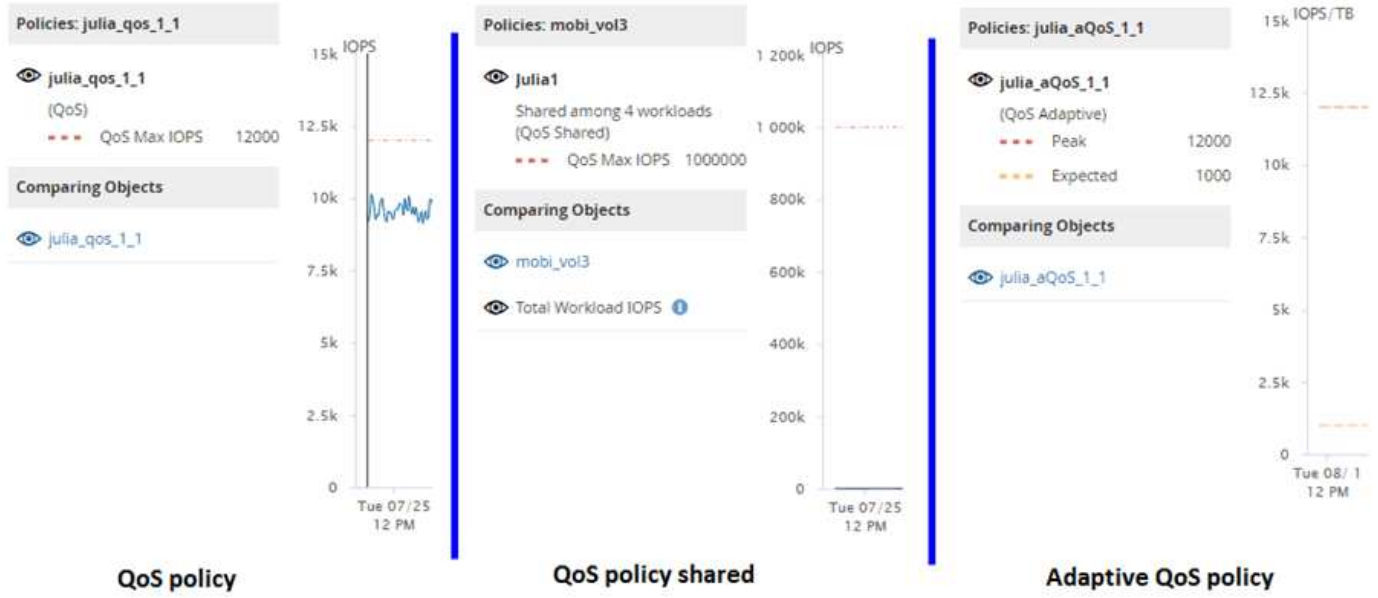
Systemressourcen. Die Einstellung „Durchsatzminimum“ (oder „`expected`“) definiert den minimalen Durchsatz, der der Arbeitslast zur Verfügung stehen muss, damit eine kritische Arbeitslast die Mindestdurchsatzziele unabhängig von der Nachfrage konkurrierender Arbeitslasten erreicht.

Gemeinsame und nicht gemeinsam genutzte QoS-Richtlinien für IOPS und MB/s verwenden die Begriffe „`minimum`“ und „`maximum`“, um die Unter- und Obergrenze zu definieren. Adaptive QoS-Richtlinien für IOPS/TB, die in ONTAP 9.3 eingeführt wurden, verwenden die Begriffe „`expected`“ und „`peak`“, um die Unter- und Obergrenze zu definieren.

Mit ONTAP lassen sich diese beiden Arten von QoS-Richtlinien erstellen. Je nachdem, wie sie auf Workloads angewendet werden, wird die QoS-Richtlinie in den Performance-Diagrammen auf drei Arten angezeigt.

Typ der Richtlinie	Funktionalität	Indikator in der Unified Manager-Schnittstelle
Einem einzelnen Workload zugewiesene gemeinsam genutzte QoS-Richtlinie oder einem einzelnen Workload oder mehreren Workloads zugewiesene nicht gemeinsam genutzte QoS-Richtlinie	Jede Arbeitslast kann die angegebene Durchsatzeinstellung nutzen	Zeigt “(QoS)” an
Gemeinsame QoS-Richtlinie, die mehreren Workloads zugewiesen ist	Alle Workloads teilen sich die angegebene Durchsatzeinstellung	Zeigt “(QoS Shared)” an
Adaptive QoS-Richtlinie, die einer einzelnen oder mehreren Arbeitslasten zugewiesen ist	Jede Arbeitslast kann die angegebene Durchsatzeinstellung nutzen	Zeigt “(QoS Adaptive)” an

Die folgende Abbildung zeigt ein Beispiel dafür, wie die drei Optionen in den Zählerdiagrammen dargestellt werden.



Wenn eine normale QoS-Richtlinie, die in IOPS definiert wurde, im IOPS/TB-Diagramm für eine Arbeitslast angezeigt wird, konvertiert ONTAP den IOPS-Wert in einen IOPS/TB-Wert, und Unified Manager zeigt diese Richtlinie im IOPS/TB-Diagramm zusammen mit dem Text “QoS, defined in IOPS” an.

Wenn eine adaptive QoS-Richtlinie, die in IOPS/TB definiert wurde, im IOPS-Diagramm für eine Arbeitslast angezeigt wird, konvertiert ONTAP den IOPS/TB-Wert in einen IOPS-Wert, und Unified Manager zeigt diese Richtlinie im IOPS-Diagramm zusammen mit dem Text „QoS Adaptive - Used, defined in IOPS/TB“ oder „QoS Adaptive - Allocated, defined in IOPS/TB“ an, je nachdem, wie die Einstellung für die Peak-IOPS-Zuweisung konfiguriert ist. Wenn die Zuweisungseinstellung auf „allocated-space“ gesetzt ist, werden die Peak-IOPS anhand der Größe des Volume berechnet. Wenn die Zuweisungseinstellung auf „used-space“ gesetzt ist, werden die Peak-IOPS anhand der im Volume gespeicherten Datenmenge unter Berücksichtigung von Storage-Effizienzen berechnet.

Das IOPS/TB-Diagramm zeigt Performance Daten nur dann an, wenn die vom Volume genutzte logische Kapazität mindestens 128 GB beträgt. Im Diagramm werden Lücken angezeigt, wenn die genutzte Kapazität im ausgewählten Zeitraum unter 128 GB fällt.

Anzeige der minimalen und maximalen QoS-Einstellungen für Workloads in Active IQ Unified Manager

Die von ONTAP definierten QoS-Richtlinieneinstellungen (Quality of Service) für ein Volume oder eine LUN können Sie in den Diagrammen des Performance Explorer anzeigen. Eine maximale Durchsatzeinstellung begrenzt die Auswirkungen konkurrierender Workloads auf die Systemressourcen. Eine minimale Durchsatzeinstellung stellt sicher, dass ein kritischer Workload die Mindestdurchsatzziele unabhängig von der Nachfrage konkurrierender Workloads erreicht.

Die QoS-Durchsatzwerte “minimum” und “maximum” für IOPS und MB/s werden in den Zählerdiagrammen nur angezeigt, wenn sie in ONTAP konfiguriert wurden. Minimale Durchsatzeinstellungen sind nur auf Systemen mit ONTAP 9.2 oder höher, nur auf AFF Systemen und derzeit nur für IOPS verfügbar.

Adaptive QoS-Richtlinien sind ab ONTAP 9.3 verfügbar und werden mit IOPS/TB anstelle von IOPS ausgedrückt. Diese Richtlinien passen den QoS-Richtlinienwert basierend auf der Volume-Größe pro Workload automatisch an, wodurch das Verhältnis von IOPS zu Terabyte bei einer Änderung der Volume-Größe beibehalten wird. Sie können eine adaptive QoS-Richtliniengruppe nur auf Volumes anwenden. Für adaptive QoS-Richtlinien werden anstelle von Minimum und Maximum die QoS-Begriffe „`expected`“ und „`peak`“ verwendet.

Unified Manager generiert Warnereignisse bei Verstößen gegen die QoS-Richtlinie, wenn der Workload-Durchsatz während jedes Performance-Erfassungszeitraums der vorherigen Stunde den definierten maximalen QoS-Richtlinienwert überschritten hat. Der Workload-Durchsatz kann den QoS-Schwellenwert während jedes Erfassungszeitraums nur für kurze Zeit überschreiten, Unified Manager zeigt im Diagramm jedoch den “durchschnittlichen” Durchsatz während des Erfassungszeitraums an. Aus diesem Grund können QoS-Ereignisse auftreten, obwohl der Durchsatz eines Workloads den im Diagramm angezeigten Richtlinienschwellenwert möglicherweise nicht überschritten hat.

Schritte

1. Auf der Seite **Performance Explorer** für das ausgewählte Volume oder die ausgewählte LUN können mit den folgenden Aktionen die QoS-Ober- und Untergrenzeneinstellungen angezeigt werden:

Wenn Sie möchten…	Folgendes ist zu tun…
Anzeige der IOPS-Obergrenze (QoS-Maximum)	Im Diagramm **IOPS Total** oder **Breakdown** können Sie **Zoom View** auswählen.

Wenn Sie möchten…	Folgendes ist zu tun…
Anzeige der MB/s-Obergrenze (des QoS-Maximums)	Im Diagramm „MB/s Gesamt“ oder „Aufschlüsselung“ kann **Zoom View** ausgewählt werden.
Anzeige des IOPS-Mindestwerts (des QoS-Minimums)	Im Diagramm **IOPS Total** oder **Breakdown** können Sie **Zoom View** auswählen.
IOPS/TB-Obergrenze anzeigen (QoS-Spitze)	Bei Volumes erfolgt dies im IOPS/TB-Diagramm über **Zoom View**.
Anzeige der IOPS/TB-Untergrenze (die erwartete QoS)	Bei Volumes erfolgt dies im IOPS/TB-Diagramm über **Zoom View**.

Die gestrichelte, horizontale Linie zeigt den in ONTAP festgelegten maximalen oder minimalen Durchsatzwert an. Sie können außerdem sehen, wann Änderungen an den QoS-Werten implementiert wurden.

2. Die spezifischen IOPS- und MB/s-Werte im Vergleich zur QoS-Einstellung werden angezeigt, wenn sich der Cursor im Diagrammbereich befindet und das Popup-Fenster eingeblendet wird.

Wenn Sie feststellen, dass bestimmte Volumes oder LUNs sehr hohe IOPS- oder MB/s-Werte aufweisen und die Systemressourcen stark beanspruchen, können Sie mithilfe von System Manager oder der ONTAP CLI die QoS-Einstellungen so anpassen, dass diese Arbeitslasten die Performance anderer Arbeitslasten nicht beeinträchtigen.

Weitere Informationen zum Anpassen der QoS-Einstellungen finden Sie unter "Überblick über das Performance-Management"

Managen der Performance mithilfe von Informationen zur Performance Kapazität und zu verfügbaren IOPS

Verwaltung der Leistungskapazität und der verfügbaren IOPS in Active IQ Unified Manager

Performance capacity gibt an, wie viel Durchsatz Sie aus einer Ressource herausholen können, ohne die nutzbare Performance dieser Ressource zu überschreiten. Bei der Anzeige mit vorhandenen Performance Zählern ist die Performance capacity der Punkt, an dem Sie die maximale Auslastung eines Knotens oder Aggregats erreichen, bevor Latenz zu einem Problem wird.

Unified Manager erfasst in jedem Cluster Statistiken zur Performance-Kapazität von Knoten und Aggregaten. *Genutzte Performance-Kapazität* ist der Prozentsatz der Performance-Kapazität, der derzeit verwendet wird, und *freie Performance-Kapazität* ist der Prozentsatz der Performance-Kapazität, der noch verfügbar ist.

Während die freie Performance Kapazität den prozentualen Anteil der Ressource angibt, der noch verfügbar ist, gibt *verfügbare IOPS* die Anzahl der IOPS an, die einer Ressource hinzugefügt werden können, bevor die maximale Performance Kapazität erreicht wird. Mithilfe dieser Metrik können Sie sicherstellen, dass einer Ressource Workloads mit einer vordefinierten Anzahl von IOPS hinzugefügt werden können.

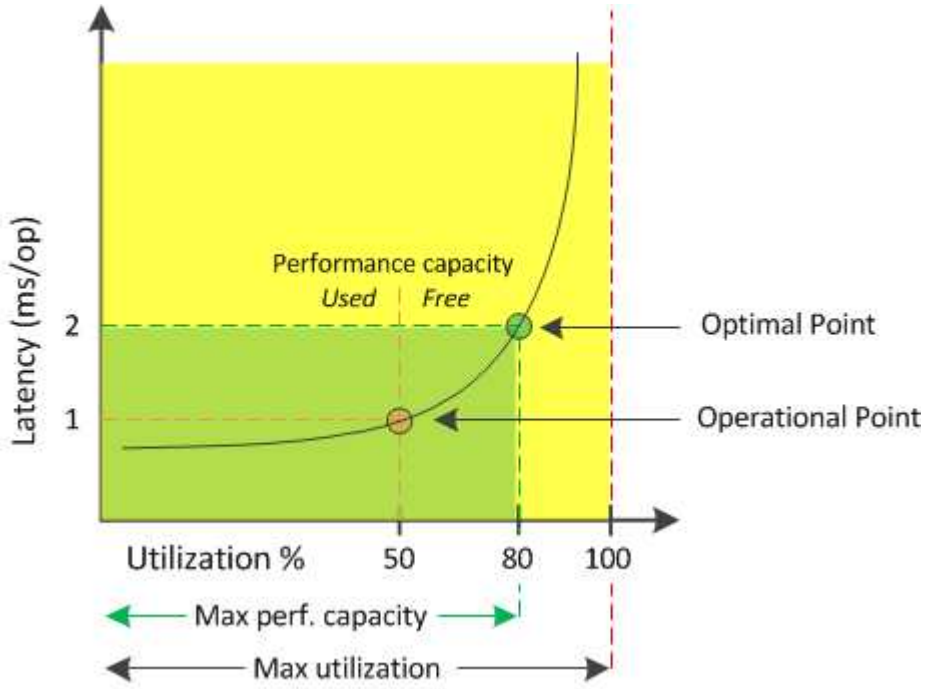
Die Überwachung der Performance-Kapazitätsinformationen bietet folgende Vorteile:

- Unterstützt die Provisionierung und den Ausgleich von Workflows.
- Hilft Ihnen dabei, eine Überlastung eines Knotens oder eine Überschreitung seiner Ressourcengrenzen zu verhindern und somit den Aufwand für die Fehlersuche zu reduzieren.
- Ermöglicht es Ihnen, genauer zu bestimmen, wo zusätzliche Storage Systeme benötigt werden.

Die verwendete Leistungs kapazität in Active IQ Unified Manager verstehen

Der Zähler für die genutzte Performance-Kapazität hilft Ihnen dabei zu erkennen, ob die Performance eines Knotens oder Aggregats einen Punkt erreicht, an dem sie sich bei steigenden Workloads verschlechtern könnte. Er kann Ihnen auch anzeigen, ob ein Knoten oder Aggregat in bestimmten Zeiträumen derzeit übermäßig genutzt wird. Die genutzte Performance-Kapazität ist der Auslastung ähnlich, bietet jedoch mehr Einblick in die verfügbaren Performance-Fähigkeiten einer physischen Ressource für einen bestimmten Workload.

Die optimale genutzte Performance-Kapazität ist der Punkt, an dem ein Knoten oder ein Aggregat optimal ausgelastet ist, eine optimale Latenz (Antwortzeit) aufweist und effizient genutzt wird. Die folgende Abbildung zeigt eine beispielhafte Latenz-Auslastungs-Kurve für ein Aggregat.



In diesem Beispiel zeigt der *Betriebspunkt* an, dass das Aggregat derzeit mit 50 % Auslastung und einer Latenz von 1,0 ms/Operation arbeitet. Anhand der vom Aggregat erfassten Statistiken ermittelt Unified Manager, dass für dieses Aggregat zusätzliche Performance-Kapazität verfügbar ist. In diesem Beispiel wird der *optimale Punkt* als der Punkt definiert, an dem das Aggregat eine Auslastung von 80 % und eine Latenz von 2,0 ms/Operation aufweist. Daher können diesem Aggregat weitere Volumes und LUNs hinzugefügt werden, sodass Ihre Systeme effizienter genutzt werden.

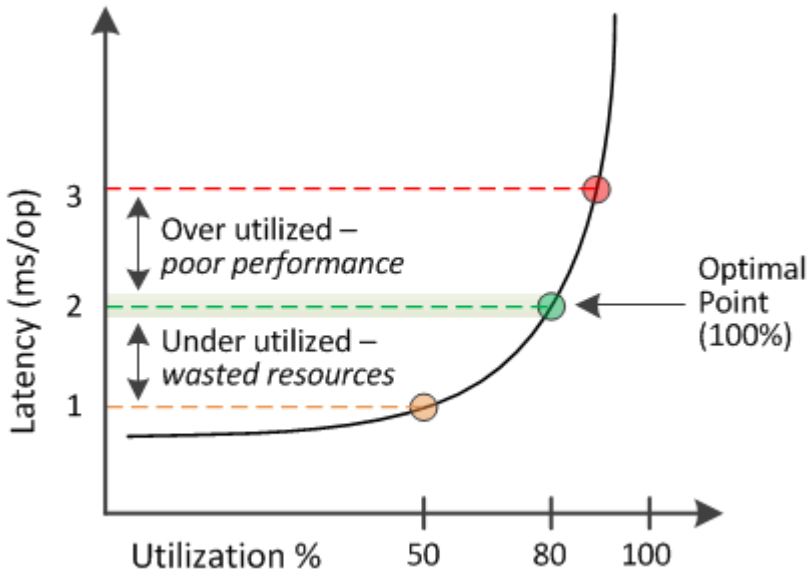
Der Zähler für die genutzte Performance-Kapazität ist voraussichtlich ein größerer Wert als der Zähler „`utilization`“, da die Performance-Kapazität die Auswirkungen auf die Latenz mit einbezieht. Wenn beispielsweise ein Node oder ein Aggregat zu 70 % ausgelastet ist, kann der Wert für die Performance-Kapazität je nach Latenzwert im Bereich von 80 % bis 100 % liegen.

In manchen Fällen kann der Auslastungszähler auf der Dashboard-Seite jedoch höher sein. Dies ist normal, da das Dashboard die aktuellen Zählerwerte bei jeder Erfassung aktualisiert; es zeigt keine Durchschnittswerte über einen bestimmten Zeitraum an, wie dies auf den anderen Seiten der Unified Manager-Benutzeroberfläche der Fall ist. Der Zähler für die verwendete Performance-Kapazität eignet sich am besten als Indikator für die über einen bestimmten Zeitraum gemittelte Performance, während sich der Auslastungszähler am besten zur Bestimmung der momentanen Ressourcennutzung eignet.

Verwendung des Werts für die genutzte Performance-Kapazität in Active IQ Unified Manager

Der Wert für die genutzte Performance-Kapazität hilft Ihnen, die Knoten und Aggregate zu identifizieren, die derzeit über- oder unterausgelastet sind. Dies ermöglicht es Ihnen, Workloads neu zu verteilen, um Ihre Storage-Ressourcen effizienter zu nutzen.

Die folgende Abbildung zeigt die Kurve der Latenz im Verhältnis zur Auslastung für eine Ressource und kennzeichnet mit farbigen Punkten drei Bereiche, in denen sich der aktuelle Betriebspunkt befinden könnte.



- Ein Nutzungsprozentsatz der Performance-Kapazität von 100 entspricht dem optimalen Punkt.

  Die Ressourcen werden derzeit effizient genutzt.

- Ein Prozentsatz der genutzten Performance-Kapazität von über 100 % weist darauf hin, dass der Knoten oder das Aggregat überlastet ist und dass Workloads eine suboptimale Performance erhalten.

  Der Ressource sollten keine neuen Workloads hinzugefügt werden, und die vorhandenen Workloads müssen möglicherweise neu verteilt werden.

- Ein Prozentsatz der Performance-Kapazität von unter 100 % zeigt an, dass der Node oder das Aggregat unterausgelastet ist und Ressourcen damit nicht effektiv zum Einsatz kommen.

  Der Ressource lassen sich weitere Workloads hinzufügen.

Im Gegensatz zur Auslastung kann der Prozentsatz der genutzten Performance-Kapazität über 100 % liegen. Es gibt keinen maximalen Prozentsatz, aber bei überlasteten Ressourcen liegt er typischerweise im Bereich von 110 % bis 140 %. Höhere Prozentsätze deuten auf eine Ressource mit schwerwiegenden Problemen hin.

Verfügbare IOPS in Active IQ Unified Manager

Der verfügbare IOPS-Zähler gibt die verbleibende Anzahl an IOPS an, die sich einem Knoten oder einem Aggregat hinzufügen lässt, bevor die Ressource ihr Limit erreicht.

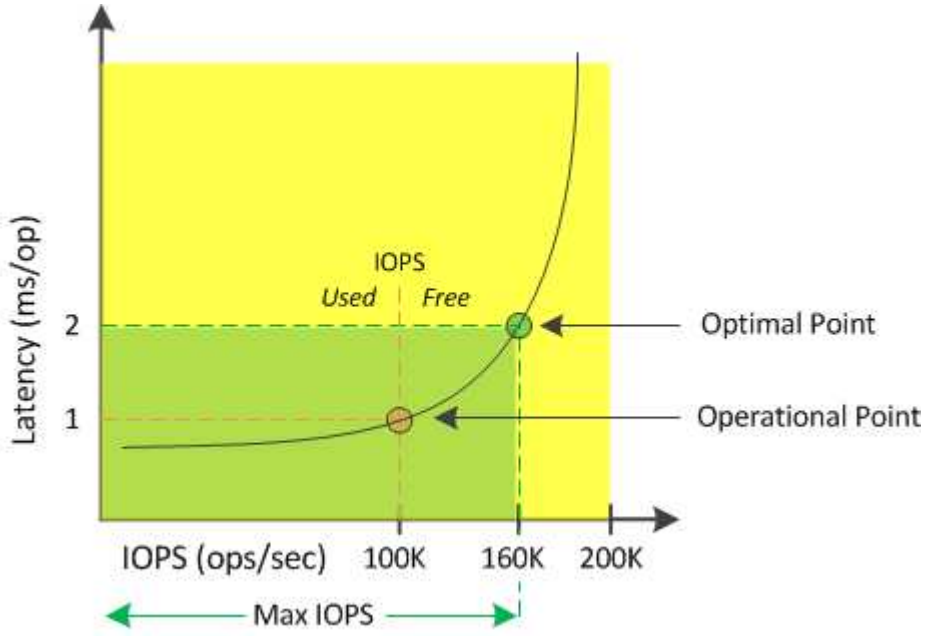
Die gesamten IOPS, die ein Knoten bereitstellen kann, basieren auf den physischen Eigenschaften des Knotens, z. B. auf der Anzahl der CPUs, der CPU-Geschwindigkeit und der Menge an RAM. Die gesamten IOPS, die ein Aggregat bereitstellen kann, basieren auf den physischen Eigenschaften der Festplatten, z. B. auf einer SATA-, SAS- oder SSD-Festplatte.

Die Summe der IOPS aller Volumes eines Aggregats entspricht möglicherweise nicht der Summe der IOPS des Aggregats. Dies wird im folgenden Knowledge-Base-Artikel erläutert: KB "Warum stimmt die Summe aller Volume-IOPs in einem Aggregat nicht mit den IOPs des Aggregats überein?"

Während der Zähler für freie Performance-Kapazität den Prozentsatz einer Ressource angibt, der noch verfügbar ist, zeigt der Zähler für verfügbare IOPS die genaue Anzahl von IOPS (Workloads) an, die einer Ressource hinzugefügt werden können, bevor die maximale Performance-Kapazität erreicht ist.

Wenn Sie beispielsweise ein Paar der Storage-Systeme FAS2520 und FAS8060 verwenden, bedeutet ein Wert von 30 % für die freie Performance-Kapazität, dass noch freie Performance-Kapazität vorhanden ist. Dieser Wert gibt jedoch keine Transparenz darüber, wie viele weitere Workloads Sie auf diesen Nodes noch einsetzen können. Der Zähler für verfügbare IOPS zeigt möglicherweise, dass auf dem FAS8060 500 IOPS verfügbar sind, auf dem FAS2520 jedoch nur 100.

Die folgende Abbildung zeigt eine Beispielkurve für Latenz gegenüber IOPS für einen Knoten.



Die maximale Anzahl von IOPS, die eine Ressource bereitstellen kann, ist die Anzahl von IOPS, wenn der Zähler für die genutzte Performance-Kapazität bei 100 % liegt (der optimale Punkt). Der Betriebspunkt zeigt an, dass der Knoten derzeit mit 100K IOPS bei einer Latenz von 1.0 ms/op arbeitet. Auf Grundlage der vom Knoten erfassten Statistiken ermittelt Unified Manager, dass die maximalen IOPS für den Knoten 160K betragen, was bedeutet, dass 60K IOPS frei oder verfügbar sind. Daher können diesem Knoten weitere Workloads hinzugefügt werden, damit Ihre Systeme effizienter genutzt werden.

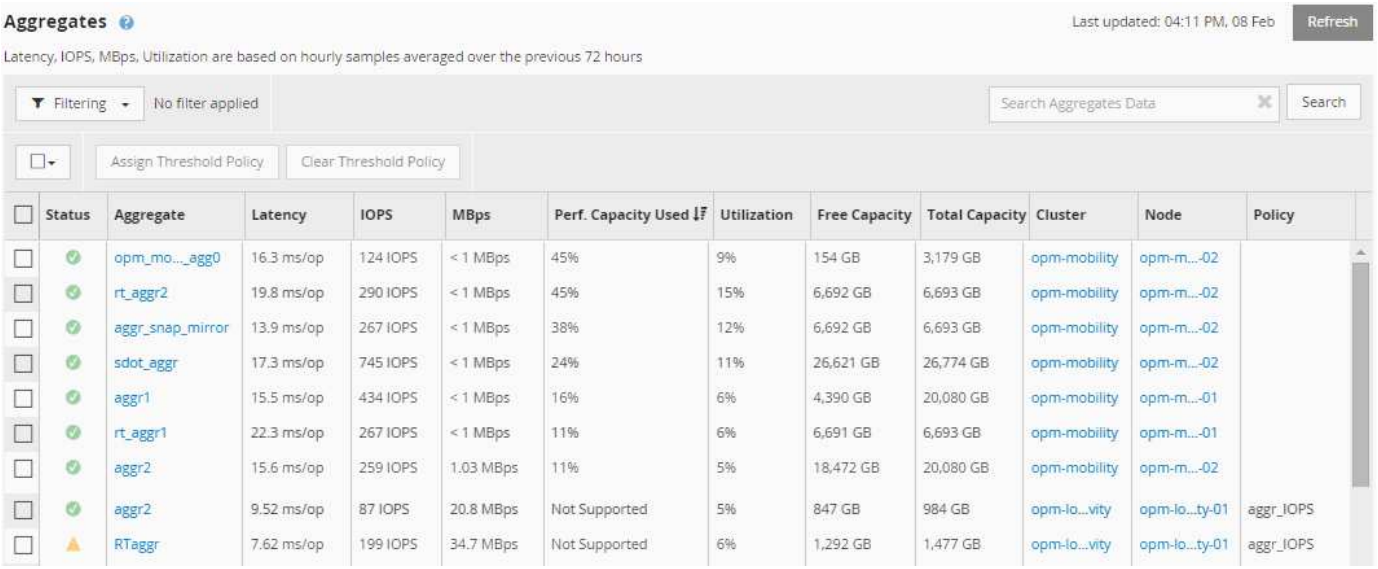
Bei minimaler Benutzeraktivität in der Ressource wird der verfügbare IOPS-Wert anhand einer generischen Arbeitslast auf Basis von ungefähr 4.500 IOPS pro CPU-Kern berechnet. Dies liegt

daran, dass Unified Manager nicht über die erforderlichen Daten verfügt, um die Eigenschaften der bereitgestellten Arbeitslast genau zu schätzen.

Verwendete Werte der Leistungsfähigkeit von Nodes und Aggregaten in Active IQ Unified Manager anzeigen

Sie können die Werte der genutzten Performance-Kapazität für alle Knoten oder für alle Aggregate in einem Cluster überwachen oder Details zu einem einzelnen Knoten oder Aggregat anzeigen.

Die Werte für die genutzte Performance-Kapazität erscheinen im Dashboard, auf den Seiten Performance Inventory, auf der Seite Top Performers, auf der Seite Create Threshold Policy, auf den Seiten Performance Explorer sowie in Detaildiagrammen. Beispielsweise enthält die Seite Performance: All Aggregates die Spalte Performance Capacity Used, in der der Wert der genutzten Performance-Kapazität für alle Aggregate angezeigt wird.



Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS
	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS

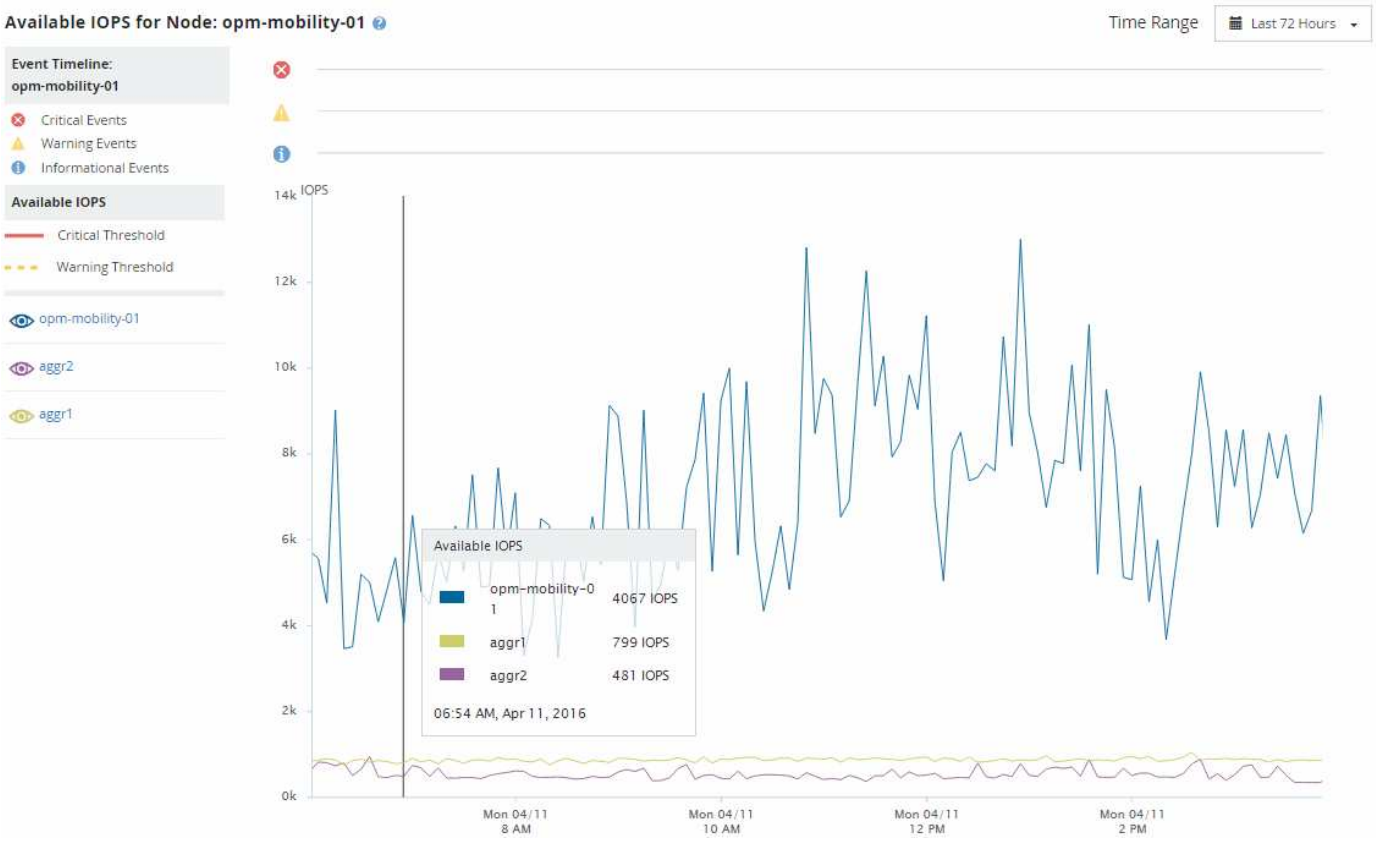
Mithilfe der Überwachung des Zählers für die genutzte Performance-Kapazität können Sie Folgendes identifizieren:

- Ob Knoten oder Aggregate in Clustern einen hohen Wert für die genutzte Performance-Kapazität aufweisen
- Ob auf Knoten oder Aggregaten in beliebigen Clustern aktive Ereignisse zur genutzten Performance-Kapazität vorliegen
- Die Knoten und Aggregate mit dem höchsten und niedrigsten Wert für die genutzte Performance-Kapazität in einem Cluster
- Latenz- und Auslastungszählerwerte in Verbindung mit Knoten oder Aggregaten mit hohen Werten für die genutzte Performance Kapazität
- Wie sich die Werte der genutzten Performance-Kapazität für Knoten in einem HA-Paar ändern, wenn einer der Knoten ausfällt
- Die am stärksten ausgelasteten Volumes und LUNs auf einem Aggregat mit einem hohen Wert für die genutzte Performance-Kapazität

Verfügbare IOPS-Werte für Knoten und Aggregate in Active IQ Unified Manager

Sie können die verfügbaren IOPS-Werte für alle Knoten oder für alle Aggregate in einem Cluster überwachen oder Details für einen einzelnen Knoten oder ein einzelnes Aggregat anzeigen.

Werte für verfügbare IOPS werden auf den Performance Inventory-Seiten und in den Diagrammen der Performance Explorer-Seite für Nodes und Aggregate angezeigt. Wenn Sie beispielsweise einen Node auf der Seite „Node/Performance Explorer“ anzeigen, können Sie das Zählerdiagramm „`Available IOPS`“ aus der Liste auswählen, um die verfügbaren IOPS-Werte für den Node und mehrere Aggregate auf diesem Node zu vergleichen.



Die Überwachung des verfügbaren IOPS-Zählers ermöglicht Ihnen Folgendes:

- Die Knoten oder Aggregate mit den höchsten verfügbaren IOPS-Werten helfen dabei, zu bestimmen, wo zukünftige Workloads eingesetzt werden können.
- Die Knoten oder Aggregate mit den niedrigsten verfügbaren IOPS-Werten dienen zur Identifizierung der Ressourcen, die im Hinblick auf potenzielle zukünftige Performanceprobleme überwacht werden sollten.
- Die am stärksten ausgelasteten Volumes und LUNs eines Aggregats mit einem geringen verfügbaren IOPS-Wert.

Anzeigen von Leistungskapazitätszählerdiagrammen in Active IQ Unified Manager

Auf der Seite „Performance Explorer“ können Sie Diagramme zur genutzten Performance Kapazität für Knoten und Aggregate anzeigen. Dadurch können Sie detaillierte Daten zur Performance Kapazität der ausgewählten Knoten und Aggregate für einen bestimmten Zeitraum anzeigen.

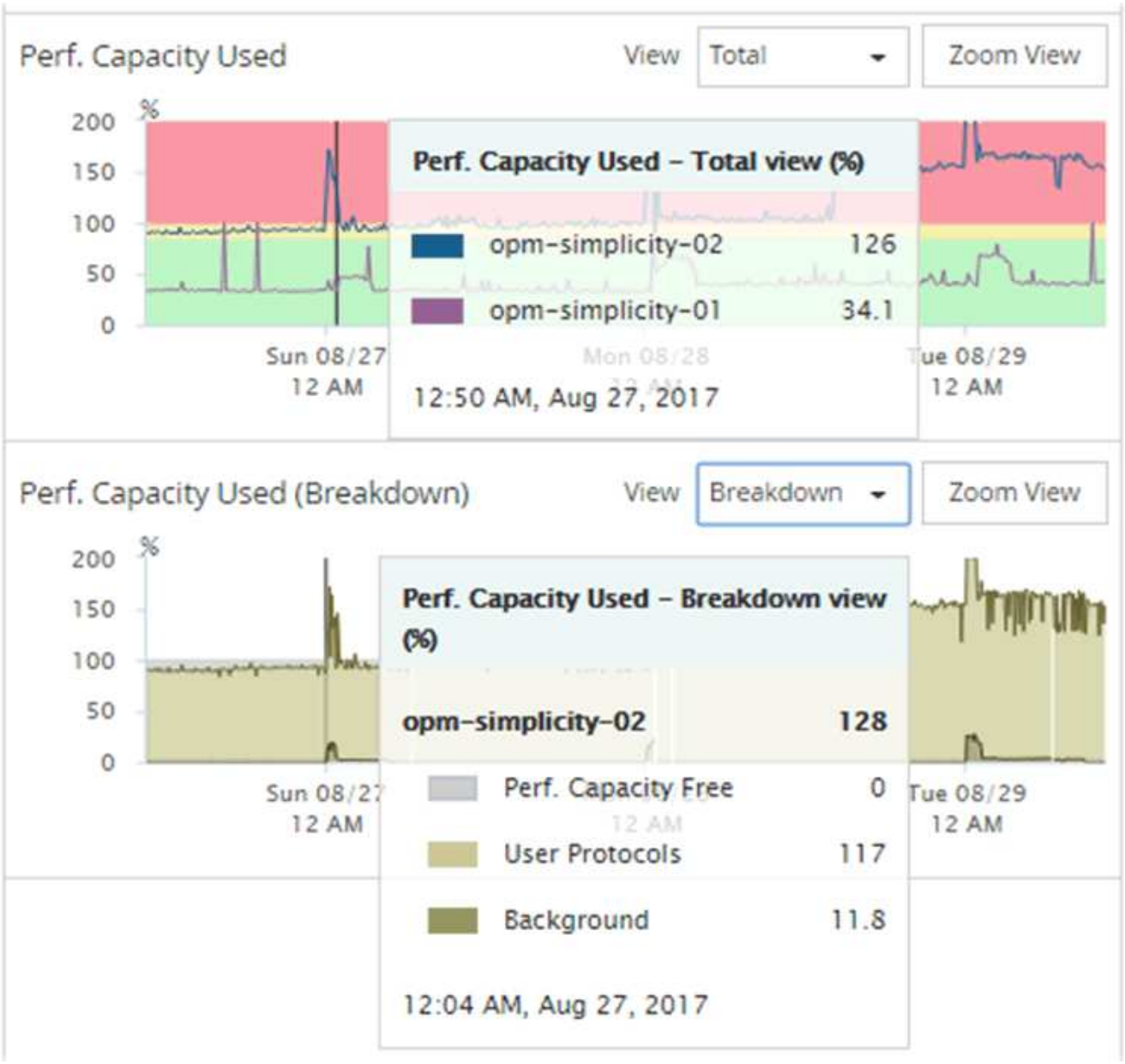
Das Standard-Zählerdiagramm zeigt die Werte der genutzten Performance-Kapazität für die ausgewählten Knoten oder Aggregate an. Das Aufschlüsselungs-Zählerdiagramm zeigt die Gesamtwerte der Performance-Kapazität für das Stammobjekt, getrennt nach der Nutzung durch Benutzerprotokolle und Hintergrundsystemprozesse. Zusätzlich wird auch der Umfang der freien Performance-Kapazität angezeigt.

> Da einige Hintergrundaktivitäten im Zusammenhang mit System- und Datenmanagement als Benutzer-Workloads identifiziert und als Benutzerprotokolle kategorisiert werden, kann der Anteil der Benutzerprotokolle künstlich hoch erscheinen, wenn diese Prozesse ausgeführt werden. Diese Prozesse laufen typischerweise um Mitternacht, wenn die Clusterauslastung gering ist. Falls um Mitternacht ein Anstieg der Benutzerprotokollaktivität zu beobachten ist, sollte geprüft werden, ob Cluster-Backup-Jobs oder andere Hintergrundaktivitäten für diese Zeit konfiguriert sind.

Schritte

1. Auf der **Landing** page eines Knotens oder Aggregats steht die Registerkarte **Explorer** zur Auswahl.
2. Im Bereich **Zählerdiagramme** können Sie **Diagramme auswählen** anklicken und anschließend das Diagramm **Perf. Verwendete Kapazität** auswählen.
3. Nach unten scrollen, bis das Diagramm angezeigt wird.

   Die Farben im Standarddiagramm zeigen an, wann sich das Objekt im optimalen Bereich befindet (gelb), wann es unterausgelastet ist (grün) und wann es überausgelastet ist (rot). Das Aufschlüsselungsdiagramm zeigt detaillierte Angaben zur Performance-Kapazität nur für das Root-Objekt.



4. Wenn Sie eines der Diagramme in voller Größe anzeigen möchten, klicken Sie auf **Zoom View**.

   Auf diese Weise können Sie mehrere Zählerdiagramme in separaten Fenstern öffnen, um die Werte der genutzten Performance-Kapazität mit den IOPS- oder MBps-Werten über denselben Zeitraum zu vergleichen.

Die Schwellenwerte für die genutzte Leistungskapazität in Active IQ Unified Manager konfigurieren

Sie können benutzerdefinierte Performance-Schwellenwertrichtlinien erstellen, sodass Ereignisse ausgelöst werden, wenn der Wert für die genutzte Performance-Kapazität für einen Knoten oder ein Aggregat den definierten Schwellenwert für die genutzte Performance-Kapazität überschreitet.

Zusätzlich können Knoten mit einer Schwellenwertrichtlinie für „`Performance capacity used takeover`“ konfiguriert werden. Diese Schwellenwertrichtlinie summiert die Statistiken zur genutzten Performance

Kapazität für beide Knoten in einem HA-Paar, um festzustellen, ob einem der Knoten bei Ausfall des anderen Knotens ausreichende Kapazität fehlen würde. Da die Workload während eines Failover die kombinierte Workload beider Partnerknoten ist, kann dieselbe Richtlinie für „`Performance capacity used takeover`“ auf beide Knoten angewendet werden.



Diese Gleichwertigkeit der genutzten Performance Kapazität gilt im Allgemeinen zwischen den Knoten. Wenn jedoch deutlich mehr knotenübergreifender Datenverkehr über den Failover-Partner zu einem der Knoten geleitet wird, kann die insgesamt genutzte Performance Kapazität bei der Ausführung aller Workloads auf dem einen Partnerknoten im Vergleich zum anderen Partnerknoten je nachdem, welcher Knoten ausgefallen ist, geringfügig abweichen.

Die Bedingungen für die verwendete Performance Kapazität können auch als sekundäre Einstellungen für Performance Schwellenwerte verwendet werden, um beim Definieren von Schwellenwerten für LUNs und Volumes eine kombinierte Schwellenwertrichtlinie zu erstellen. Die Bedingung für die verwendete Performance Kapazität wird auf das Aggregat oder den Knoten angewendet, auf dem sich das Volume oder die LUN befindet. Beispielsweise kann anhand der folgenden Kriterien eine kombinierte Schwellenwertrichtlinie erstellt werden:

Speicherobjekt	Performance-Zähler	Warnschwelle	Kritischer Schwellenwert	Dauer
Volumen	Latenz	15 ms/op	25 ms/op	20 Minuten
Aggregat	Genutzte Performance-Kapazität	80%	95%	

Kombinationsschwellenwertrichtlinien bewirken, dass ein Ereignis nur dann ausgelöst wird, wenn beide Bedingungen über die gesamte Dauer hinweg verletzt werden.

Verwenden des Zählers für genutzte Leistungskapazität in Active IQ Unified Manager

Üblicherweise streben Unternehmen einen Prozentsatz der genutzten Performance-Kapazität von unter 100 % an, um Ressourcen effizient zu nutzen und gleichzeitig zusätzliche Performance-Kapazität zur Unterstützung von Bedarfsspitzen zu reservieren. Mithilfe von Schwellenwertrichtlinien lässt sich anpassen, wann Warnmeldungen für hohe Werte der genutzten Performance-Kapazität gesendet werden.

Sie können auf der Grundlage Ihrer Performanceanforderungen spezifische Ziele festlegen. So könnten beispielsweise Finanzdienstleistungsunternehmen mehr Performancekapazität reservieren, um die rechtzeitige Ausführung von Transaktionen zu gewährleisten. Diese Unternehmen könnten Schwellenwerte für die genutzte Performancekapazität im Bereich von 70-80 Prozent festlegen. Fertigungsunternehmen mit geringeren Margen könnten dagegen weniger Performancekapazität reservieren, wenn sie bereit sind, zugunsten einer besseren Kontrolle der IT-Kosten ein Performance-Risiko einzugehen. Diese Unternehmen könnten Schwellenwerte für die genutzte Performancekapazität im Bereich von 85-95 Prozent festlegen.

Wenn der Wert der verwendeten Performance-Kapazität den in einer benutzerdefinierten Schwellenwertrichtlinie festgelegten Prozentsatz überschreitet, sendet Unified Manager eine Benachrichtigungs-E-Mail und fügt das Ereignis der Seite Event Inventory hinzu. Dadurch können Sie potenzielle Probleme managen, bevor sie sich auf die Performance auswirken. Diese Ereignisse können auch als Indikatoren dafür verwendet werden, dass Sie Workloads innerhalb Ihrer Knoten und Aggregate verschieben und ändern müssen.

Die Seite „Node Failover Planning“ verstehen und verwenden

Die Seite „Knotenausfallplanung“ in Active IQ Unified Manager kann verwendet werden

Die Seite „Performance/Knoten-Failover-Planung“ schätzt die Auswirkungen auf die Performance eines Knotens, wenn der High-Availability-Partnerknoten (HA-Partnerknoten) des Knotens ausfällt. Unified Manager stützt diese Schätzungen auf die historische Performance der Knoten im HA-Paar.

Die Abschätzung der Performance-Auswirkungen eines Failovers hilft Ihnen bei der Planung in den folgenden Szenarien:

- Wenn ein Failover die geschätzte Performance des Takeover-Node dauerhaft auf ein inakzeptables Level reduziert, können Sie Korrekturmaßnahmen in Erwägung ziehen, um die Performance-Auswirkungen eines Failover zu verringern.
- Vor der Einleitung eines manuellen Failover zur Durchführung von Hardwarewartungsarbeiten kann abgeschätzt werden, wie sich das Failover auf die Performance des Übernahmeknotens auswirkt, um den besten Zeitpunkt für die Durchführung der Aufgabe zu bestimmen.

Die Korrekturmaßnahmen werden auf der Seite „Leistung/Knoten-Failover-Planung“ in Active IQ Unified Manager ermittelt.

Anhand der Informationen, die auf der Seite „Performance/Node Failover Planning“ angezeigt werden, können Sie Maßnahmen ergreifen, um sicherzustellen, dass ein Failover nicht dazu führt, dass die Performance eines HA-Paares unter ein akzeptables Level sinkt.

Um beispielsweise die geschätzten Performance-Einbußen bei einem Failover zu verringern, können Sie einige Volumes oder LUNs von einem Knoten im HA-Paar auf andere Knoten im Cluster verschieben. Dadurch wird sichergestellt, dass der primäre Knoten nach einem Failover weiterhin eine akzeptable Performance liefern kann.

Eine Übersicht über die Komponenten der Seite „Leistung/Knoten-Failover-Planung“ in Active IQ Unified Manager

Die Komponenten der Seite „Performance/Node Failover Planning“ werden in einer Tabelle und im Vergleichsbereich angezeigt. Mithilfe dieser Abschnitte können Sie die Auswirkungen eines Node-Failovers auf die Performance des übernehmenden Node beurteilen.

Performance-Statistikraster

Die Seite „Performance/Node Failover Planning“ zeigt eine Tabelle mit Statistiken zu Latenz, IOPS, Auslastung und genutzter Performancekapazität an.

Die auf dieser Seite und auf der Seite „Performance/Node Performance Explorer“ angezeigten Latenz- und IOPS-Werte stimmen möglicherweise nicht überein, da unterschiedliche

Performance-Zähler zur Berechnung der Werte verwendet werden, um das Node-Failover vorherzusagen.

Im Raster hat jeder Knoten eine der folgenden Rollen:

- Primär

  Der Knoten, der die Funktion des HA-Partners übernimmt, wenn dieser ausfällt. Das Stammobjekt ist immer der primäre Knoten.

- Partner

  Der Knoten, der im Failover-Szenario ausfällt.

- Geschätzte Übernahme

  Dasselbe wie beim primären Node. Die für diesen Node angezeigten Performance-Statistiken zeigen die Performance des Takeover-Node, nachdem er den ausgefallenen Partner übernommen hat.

Obwohl die Workload des Übernahmeknotens nach einem Failover der kombinierten Workload beider Knoten entspricht, ergeben sich die Statistiken für den geschätzten Übernahmeknoten nicht aus der Summe der Statistiken des primären Knotens und des Partnerknotens. Wenn die Latenz des primären Knotens beispielsweise 2 ms/op und die Latenz des Partnerknotens 3 ms/op beträgt, kann der geschätzte Übernahmeknoten eine Latenz von 4 ms/op aufweisen. Dieser Wert ist eine Berechnung, die Unified Manager durchführt.

Sie können auf den Namen des Partner-Node klicken, wenn dieser zum Root-Objekt werden soll. Nachdem die Seite „Performance/Node Performance Explorer“ angezeigt wird, können Sie auf die Registerkarte **Failover Planning** klicken, um zu sehen, wie sich die Performance in diesem Node-Ausfallszenario ändert. Wenn beispielsweise Node1 der primäre Node und Node2 der Partner-Node ist, können Sie auf Node2 klicken, damit dieser zum primären Node wird. Auf diese Weise ist erkennbar, wie sich die geschätzte Performance je nachdem ändert, welcher Node ausfällt.

Vergleichsfenster

Die folgende Liste beschreibt die Komponenten, die standardmäßig im Vergleichsbereich angezeigt werden:

- **Ereignisdiagramme**

  Sie werden im gleichen Format wie auf der Seite „Leistung/Knotenleistungs-Explorer“ angezeigt. Sie beziehen sich ausschließlich auf den primären Knoten.

- **Zählerdiagramme**

  Sie zeigen historische Statistiken für den in der Tabelle angezeigten Performance-Zähler an. In jedem Diagramm zeigt das Diagramm für den Node „Geschätzte Übernahme“ die geschätzte Performance, wenn zu einem beliebigen Zeitpunkt ein Failover erfolgt wäre.

  Angenommen, das Auslastungsdiagramm zeigt für den geschätzten Übernahmeknoten am 8. Februar um 11 Uhr 73 % an. Wenn zu diesem Zeitpunkt ein Failover aufgetreten wäre, hätte die Auslastung des Übernahmeknotens 73 % betragen.

  Die historischen Statistiken helfen Ihnen, den optimalen Zeitpunkt für die Einleitung eines Failover zu finden und so die Möglichkeit einer Überlastung des Übernahmeknotens zu minimieren. Sie können ein

Failover nur zu Zeitpunkten planen, an denen die prognostizierte Performance des Übernahmeknotens akzeptabel ist.

Standardmäßig werden im Vergleichsbereich Statistiken sowohl für das Stammobjekt als auch für den Partnerknoten angezeigt. Anders als auf der Seite „Performance/Node Performance Explorer“ wird auf dieser Seite keine Schaltfläche „Add“ zum Hinzufügen von Objekten für den Statistikvergleich angezeigt.

Der Bereich „Vergleichen“ kann auf die gleiche Weise angepasst werden wie auf der Seite „Performance/Node Performance Explorer“. Die folgende Liste zeigt Beispiele für die Anpassung der Diagramme:

- Durch Klicken auf einen Node-Name werden die Statistiken des Node in den Zählerdiagrammen ein- oder ausgeblendet.
- Über **Zoom View** lässt sich ein detailliertes Diagramm für einen bestimmten Zähler in einem neuen Fenster anzeigen.

Schwellenwertrichtlinien für die Node Failover Planung in Active IQ Unified Manager erstellen

Sie können eine Knotenschwellenwertrichtlinie erstellen, sodass Sie auf der Seite „Performance/Node Failover Planning“ benachrichtigt werden, wenn ein potenzieller Failover die Performance des Übernahmeknotens auf ein inakzeptables Level verschlechtern würde.

Die systemdefinierte Performance-Schwellenwertrichtlinie mit dem Namen “Node HA pair over-utilized” generiert ein Warnereignis, wenn der Schwellenwert in sechs aufeinanderfolgenden Erfassungszeiträumen (30 Minuten) überschritten wird. Der Schwellenwert gilt als überschritten, wenn die kombinierte genutzte Performance-Kapazität der Nodes in einem HA-Paar 200 % übersteigt.

Das Ereignis aus der systemdefinierten Schwellenwertrichtlinie weist darauf hin, dass ein Failover dazu führt, dass die Latenz des übernehmenden Knotens auf ein inakzeptables Level ansteigt. Wenn für einen bestimmten Knoten ein von dieser Richtlinie generiertes Ereignis angezeigt wird, können Sie zur Seite Performance/Node Failover Planning für diesen Knoten navigieren, um den aufgrund eines Failover prognostizierten Latenzwert anzuzeigen.

Zusätzlich zur Verwendung dieser systemdefinierten Schwellenwertrichtlinie können Sie Schwellenwertrichtlinien mithilfe des Zählers „Performance Capacity Used - Takeover“ erstellen und die Richtlinie dann auf ausgewählte Knoten anwenden. Durch die Angabe eines Schwellenwerts unter 200 % erhalten Sie ein Ereignis, bevor der Schwellenwert für die systemdefinierte Richtlinie überschritten wird. Sie können außerdem die Mindestdauer, für die der Schwellenwert überschritten wird, auf unter 30 Minuten festlegen, wenn Sie benachrichtigt werden möchten, bevor das Ereignis für die systemdefinierte Richtlinie generiert wird.

Sie können beispielsweise eine Schwellenwertrichtlinie definieren, die ein Warnereignis generiert, wenn die kombinierte genutzte Performance-Kapazität der Nodes in einem HA-Paar länger als 10 Minuten 175 % überschreitet. Diese Richtlinie kann auf Node1 und Node2 angewendet werden, die ein HA-Paar bilden. Nach Erhalt einer Benachrichtigung über ein Warnereignis für Node1 oder Node2 kann für diesen Node die Seite Performance/Node Failover Planning aufgerufen werden, um die geschätzten Performance-Auswirkungen auf den übernehmenden Node zu bewerten. Es können Korrekturmaßnahmen ergriffen werden, um eine Überlastung des übernehmenden Node zu vermeiden, falls tatsächlich ein Failover eintritt. Wenn Maßnahmen ergriffen werden, solange die kombinierte genutzte Performance-Kapazität der Nodes unter 200 % liegt, erreicht die Latenz des übernehmenden Node auch dann kein inakzeptables Level, wenn während dieser Zeit ein Failover eintritt.

Das Diagramm „Aufschlüsselung der genutzten Performance-Kapazität“ wird für die Failover-Planung in Active IQ Unified Manager verwendet

Das detaillierte Diagramm „Ausgenutzte Performance Kapazität - Aufschlüsselung“ zeigt die genutzte Performance Kapazität für den primären Knoten und den Partnerknoten. Es zeigt außerdem die Menge an freier Performance Kapazität auf dem geschätzten Übernahmeknoten. Anhand dieser Informationen lässt sich feststellen, ob bei einem Ausfall des Partnerknotens ein Performance Problem auftreten könnte.

Zusätzlich zur Anzeige der für die Knoten insgesamt genutzten Performance-Kapazität schlüsselt das Aufschlüsselungsdiagramm die Werte für jeden Knoten in Benutzerprotokolle und Hintergrundprozesse auf.

- Benutzerprotokolle sind die E/A-Operationen von Benutzerapplikationen zum und vom Cluster.
- Hintergrundprozesse sind die internen Systemprozesse, die an Storage, Datenreplizierung und Systemstatus beteiligt sind.

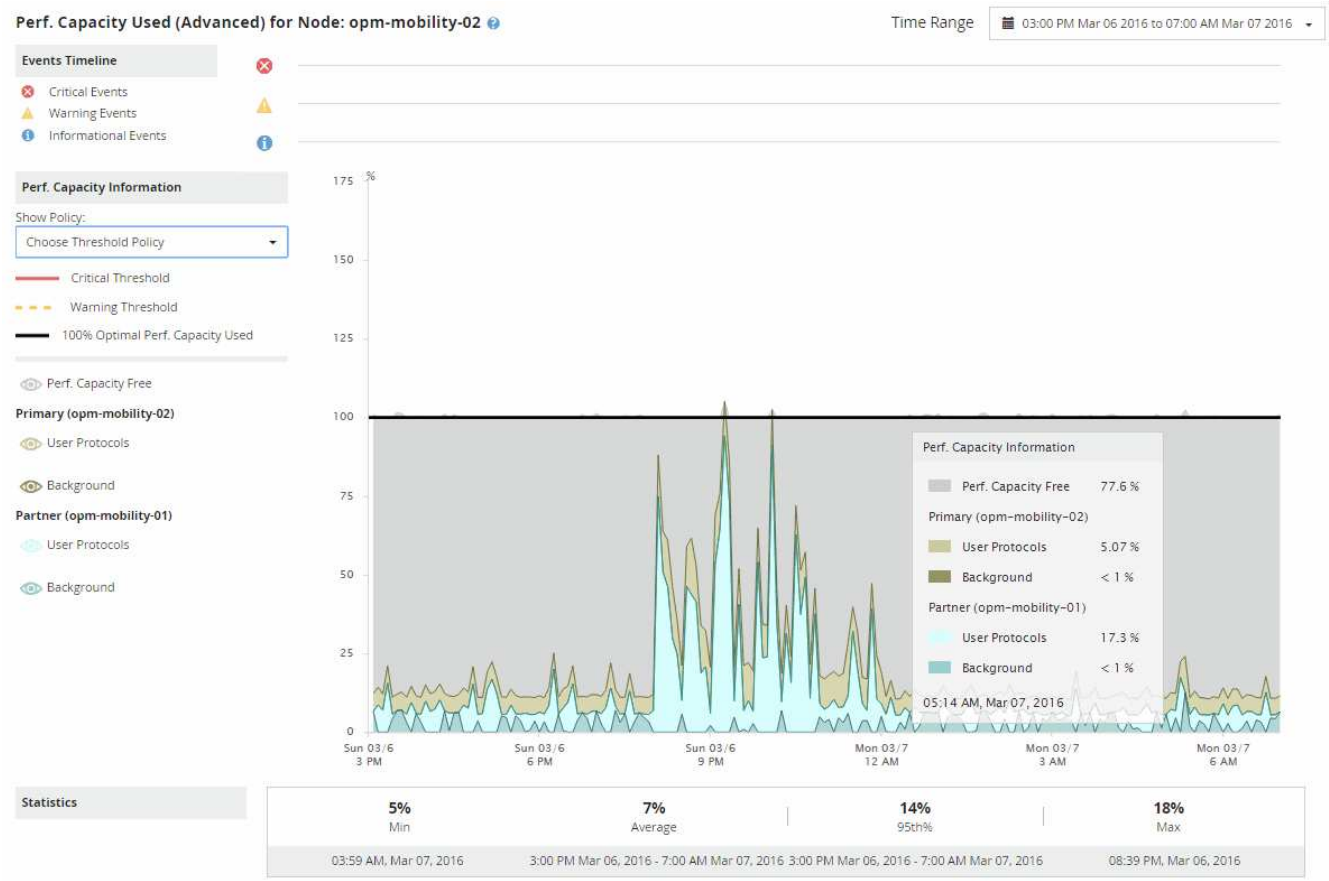
Diese zusätzliche Detailebene ermöglicht es Ihnen, festzustellen, ob ein Performanceproblem durch die Aktivität von Benutzerapplikationen oder durch Hintergrundprozesse des Systems, wie z. B. Deduplizierung, RAID-Rekonstruktion, Datenträgerbereinigung und SnapMirror Kopiervorgänge, verursacht wird.

Schritte

1. Zur Seite **Performance/Node Failover Planning** für den Knoten wechseln, der als geschätzter Übernahmeknoten dienen soll.
2. Über das Auswahlfeld **Zeitraum** lässt sich der Zeitraum festlegen, für den die historischen Statistiken im Zählerraster und in den Zählerdiagrammen angezeigt werden.

   Die Zählerdiagramme mit Statistiken für den Primärknoten, den Partnerknoten und den Knoten „Geschätzte Übernahme“ werden angezeigt.
3. In der Liste **Diagramme auswählen** ist **Perf. Verwendete Kapazität** auszuwählen.
4. Im Diagramm **Perf. Capacity Used** werden **Breakdown** ausgewählt und **Zoom View** angeklickt.

   Das detaillierte Diagramm für Perf. Capacity Used wird angezeigt.



5. Beim Bewegen des Cursors über das detaillierte Diagramm werden im Popup-Fenster Informationen zur verwendeten Performance-Kapazität angezeigt.

   Der Perf. Prozentsatz der freien Performance-Kapazität ist die Performance-Kapazität, die auf dem Knoten für die geschätzte Übernahme verfügbar ist. Er gibt an, wie viel Performance-Kapazität nach einem Failover auf dem Übernahmeknoten verbleibt. Wenn er 0 % beträgt, verursacht ein Failover auf dem Übernahmeknoten einen Anstieg der Latenz auf ein inakzeptables Level.

6. Zur Vermeidung eines niedrigen freien Prozentsatzes der Performance-Kapazität empfiehlt sich die Prüfung von Korrekturmaßnahmen.

   Wenn Sie einen Failover für die Knotenwartung einleiten möchten, wählen Sie einen Zeitpunkt für den Failover des Partnerknotens, zu dem der Prozentsatz der freien Performance-Kapazität nicht 0 beträgt.

Daten erfassen und die Workload-Performance überwachen

Datenerfassung und Überwachung der Workload-Performance in Active IQ Unified Manager

Unified Manager erfasst und analysiert alle 5 Minuten die Aktivität der Workloads, um Performance-Ereignisse zu identifizieren, und erkennt alle 15 Minuten Konfigurationsänderungen. Er speichert historische Performance- und Ereignisdaten im 5-Minuten-Takt für maximal 30 Tage und verwendet diese Daten, um die zu erwartende Latenzspanne für alle überwachten Workloads vorherzusagen.

Unified Manager muss mindestens drei Tage lang Arbeitslastaktivitäten erfassen, bevor die Analyse beginnen

und die Latenzprognose für die E/A-Reaktionszeit auf der Seite „Arbeitslastanalyse“ und auf der Seite „Ereignisdetails“ angezeigt werden kann. Während dieser Erfassungsphase werden in der Latenzprognose nicht alle Änderungen angezeigt, die durch die Arbeitslastaktivität auftreten. Nach der Erfassung von drei Tagen Aktivität aktualisiert Unified Manager die Latenzprognose alle 24 Stunden um 0:00 Uhr, um Änderungen der Arbeitslastaktivität zu berücksichtigen und einen präziseren dynamischen Performance-Schwellenwert festzulegen.

Während der ersten vier Tage, in denen Unified Manager eine Arbeitslast überwacht, wird die Latenzprognose für diese Arbeitslast nicht in den Latenzdiagrammen angezeigt, wenn seit der letzten Datenerfassung mehr als 24 Stunden vergangen sind. Ereignisse, die vor der letzten Erfassung erkannt wurden, sind weiterhin verfügbar.

Die Umstellung auf die Sommerzeit ändert die Systemzeit, wodurch sich die Latenzprognose der Performance-Statistiken für überwachte Workloads ändert. Unified Manager beginnt umgehend mit der Korrektur der Latenzprognose, was etwa 15 Tage in Anspruch nimmt. Während dieser Zeit kann Unified Manager weiterhin verwendet werden, aber da Unified Manager die Latenzprognose zum Erkennen dynamischer Ereignisse verwendet, sind einige Ereignisse möglicherweise nicht korrekt. Ereignisse, die vor der Zeitumstellung erkannt wurden, sind davon nicht betroffen.

Die Überwachung von Workload-Typen mit Active IQ Unified Manager

Mit Unified Manager können Sie die Performance von zwei Arten von Arbeitslasten überwachen: benutzerdefinierte und systemdefinierte.

- ***Benutzerdefinierte Arbeitslasten***

  Der E/A-Durchsatz von Applikationen zum Cluster. Dies sind Prozesse, die an Lese- und Schreibanforderungen beteiligt sind. Ein Volume, eine LUN, eine NFS-Freigabe, eine SMB/CIFS-Freigabe und eine Workload ist eine benutzerdefinierte Workload.

  Unified Manager überwacht lediglich die Workload-Aktivität auf dem Cluster. Es überwacht weder die Anwendungen noch die Clients oder die Pfade zwischen den Anwendungen und dem Cluster.

  Wenn eine oder mehrere der folgenden Bedingungen für eine Arbeitslast zutreffen, kann diese nicht vom Unified Manager überwacht werden:

  - Es handelt sich um eine Data Protection (DP)-Kopie im Nur-Lese-Modus. (DP-Volumes werden auf benutzergenerierten Datenverkehr überwacht.)
  - Es handelt sich um einen Offline-Datenklon.
  - Es handelt sich um ein gespiegeltes Volume in einer MetroCluster Konfiguration.

- ***Systemdefinierte Workloads***

  Die internen Prozesse im Zusammenhang mit Storage-Effizienz, Datenreplizierung und Systemstatus umfassen:

  - Speichereffizienz, wie z. B. Deduplizierung
  - Festplattenzustand, einschließlich RAID-Rekonstruktion, Festplatten-Scrubbing usw.
  - Datenreplizierung, wie SnapMirror Kopien

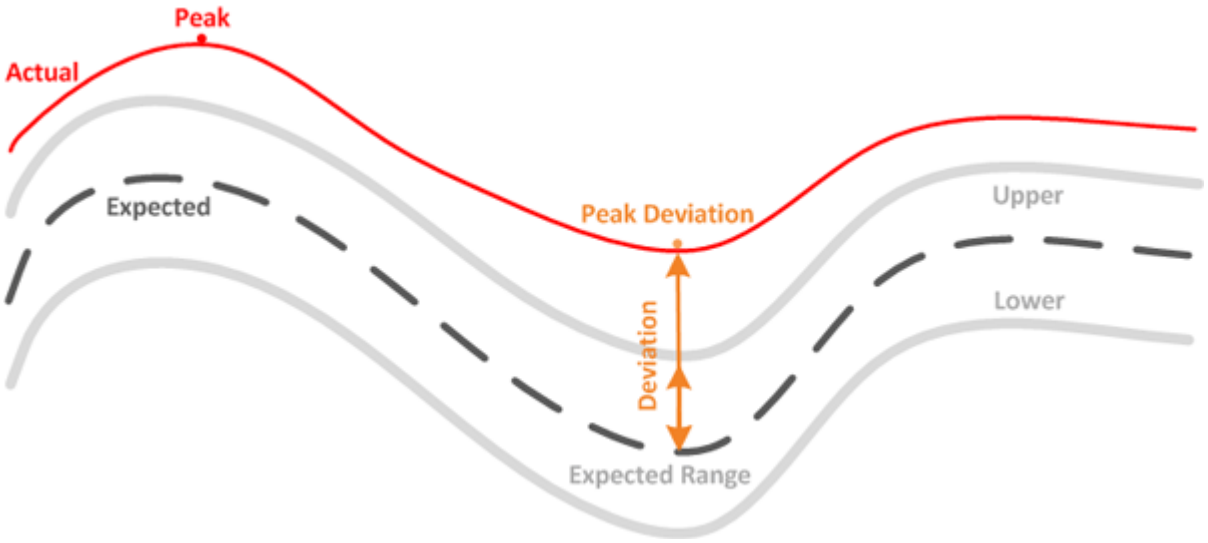
- Managementaktivitäten
- Dateisystemstatus, der verschiedene WAFL Aktivitäten umfasst
- Dateisystemscanner, wie z. B. WAFL Scan
- Kopier-Offload, z. B. ausgelagerte Storage-Effizienzvorgänge von VMware hosts
- Systemstatus, wie z. B. Volume-Verschiebungen, Datenkomprimierung usw.
- Nicht überwachte Volumes

Leistungsdaten für systemdefinierte Workloads werden in der GUI nur dann angezeigt, wenn bei der von diesen Workloads verwendeten Clusterkomponente ein Engpass besteht. Beispielsweise können Sie nicht nach dem Namen eines systemdefinierten Workloads suchen, um dessen Leistungsdaten in der GUI anzuzeigen.

Grundlegendes zu Kennzahlen für die Messung der Workload-Leistung in Active IQ Unified Manager

Unified Manager misst die Performance von Workloads auf einem Cluster anhand historischer und erwarteter statistischer Werte, die die Latenzprognosewerte für die Workloads bilden. Unified Manager vergleicht die tatsächlichen statistischen Werte der Workloads mit der Latenzprognose, um festzustellen, wann die Workload Performance zu hoch oder zu niedrig ist. Ein Workload, der nicht wie erwartet funktioniert, löst ein dynamisches Performance Ereignis aus und benachrichtigt Sie.

In der folgenden Abbildung stellt der rote Istwert die tatsächlichen Performance-Statistiken im betrachteten Zeitraum dar. Dieser Istwert hat den Performance-Schwellenwert überschritten, der die Obergrenze der Latenzprognose darstellt. Der Spitzenwert entspricht dem höchsten Istwert im betrachteten Zeitraum. Die Abweichung misst die Differenz zwischen den erwarteten Werten (der Prognose) und den Istwerten, wobei die maximale Abweichung die größte Differenz zwischen den erwarteten Werten und den Istwerten angibt.



Die folgende Tabelle enthält die Messwerte der Workload-Performance.

Messung	Beschreibung
Aktivität	Der Prozentsatz des QoS-Limits, der von den Workloads in der Richtliniengruppe genutzt wird. Wenn Unified Manager eine Änderung an einer Richtliniengruppe erkennt, z. B. das Hinzufügen oder Entfernen eines Volumes oder die Änderung des QoS-Grenzwerts, können die tatsächlichen und erwarteten Werte 100 % des festgelegten Grenzwerts überschreiten. Wenn ein Wert 100 % des festgelegten Grenzwerts überschreitet, wird er als >100% angezeigt. Wenn ein Wert unter 1 % des festgelegten Grenzwerts liegt, wird er als <1% angezeigt.
Tatsächlich	Der gemessene Performance-Wert zu einem bestimmten Zeitpunkt für eine bestimmte Arbeitslast.
Abweichung	Die Differenz zwischen den erwarteten und den tatsächlichen Werten. Sie entspricht dem Verhältnis von Istwert minus Erwartungswert zum oberen Wert des erwarteten Bereichs minus Erwartungswert. Ein negativer Abweichungswert weist darauf hin, dass die Workload Performance niedriger als erwartet ist, während ein positiver Abweichungswert darauf hinweist, dass die Workload Performance höher als erwartet ist.
Erwartet	Die erwarteten Werte basieren auf der Analyse historischer Performance-Daten für eine bestimmte Arbeitslast. Unified Manager analysiert diese statistischen Werte, um den erwarteten Wertebereich (Latenzprognose) zu bestimmen.
Latenzprognose (Erwarteter Bereich)	Die Latenzprognose ist eine Vorhersage der erwarteten oberen und unteren Performance-Werte zu einem bestimmten Zeitpunkt. Bei der Workload-Latenz bilden die oberen Werte den Performance-Schwellenwert. Wenn der tatsächliche Wert den Performance-Schwellenwert überschreitet, löst Unified Manager ein dynamisches Performance-Ereignis aus.
Spitze	Der über einen Zeitraum gemessene Maximalwert.
Maximale Abweichung	Der über einen bestimmten Zeitraum gemessene maximale Abweichungswert.
Warteschlangentiefe	Die Anzahl der ausstehenden E/A-Anforderungen, die an der Interconnect-Komponente warten.

Messung	Beschreibung
Verwendung	Für die Netzwerk-, Datenverarbeitungs- und Aggregatkomponenten der prozentuale Anteil der Auslastungszeit zur Ausführung von Workload-Vorgängen über einen bestimmten Zeitraum. Beispielsweise der prozentuale Anteil der Zeit, den die Netzwerk- oder Datenverarbeitungskomponenten für die Verarbeitung einer E/A-Anforderung oder ein Aggregat zur Erfüllung einer Lese- oder Schreibanforderung benötigen.
Schreibdurchsatz	Der Schreibdurchsatz in Megabyte pro Sekunde (MB/s) von Workloads auf einem lokalen Cluster zum Partner-Cluster in einer MetroCluster Konfiguration.

Informationen dazu, wie Active IQ Unified Manager den erwarteten Leistungsbereich berechnet

Die Latenzprognose ist eine Vorhersage der erwarteten oberen und unteren Performance-Werte zu einem bestimmten Zeitpunkt. Bei der Workload-Latenz bilden die oberen Werte den Performance-Schwellenwert. Wenn der tatsächliche Wert den Performance-Schwellenwert überschreitet, löst Unified Manager ein dynamisches Performance-Ereignis aus.

Während der üblichen Geschäftszeiten zwischen 9:00 und 17:00 Uhr rufen die meisten Mitarbeiter ihre E-Mails beispielsweise zwischen 9:00 und 10:30 Uhr ab. Die dadurch erhöhte Nachfrage auf den E-Mail-Servern führt in diesem Zeitraum zu einer höheren Auslastung des Backend Storage. Mitarbeiter bemerken möglicherweise längere Reaktionszeiten ihrer E-Mail-Programme.

Während der Mittagspause zwischen 12:00 und 13:00 Uhr sowie nach Feierabend nach 17:00 Uhr sind die meisten Mitarbeiter wahrscheinlich nicht an ihren Computern. Die Auslastung der E-Mail-Server sinkt dadurch in der Regel, was wiederum die Auslastung des Backend-Storage verringert. Alternativ können geplante Workload-Vorgänge wie Storage-Datensicherungen oder Virenscans nach 17:00 Uhr beginnen und die Aktivität auf dem Backend-Storage erhöhen.

Über mehrere Tage hinweg bestimmen die Zu- und Abnahme der Aktivität einer Arbeitslast den erwarteten Aktivitätsbereich (Latenzprognose) mit oberen und unteren Grenzwerten für eine Arbeitslast. Liegt die tatsächliche Aktivität der Arbeitslast eines Objekts außerhalb dieser oberen oder unteren Grenzwerte und bleibt sie über einen gewissen Zeitraum außerhalb, kann dies darauf hindeuten, dass das Objekt über- oder unterausgelastet ist.

So entsteht die Latenzprognose

Unified Manager muss mindestens 3 Tage lang Workload-Aktivitätsdaten erfassen, bevor die Analyse beginnen und die Latenzprognose für die E/A-Antwortzeit in der GUI angezeigt werden kann. Die erforderliche Mindestdatenerfassung berücksichtigt nicht alle Änderungen, die sich aus der Workload-Aktivität ergeben. Nach der Erfassung der ersten 3 Tage an Aktivität passt Unified Manager die Latenzprognose alle 24 Stunden um 0:00 Uhr an, um Änderungen der Workload-Aktivität zu berücksichtigen und einen präziseren dynamischen Performance-Schwellenwert festzulegen.

Die Umstellung auf die Sommerzeit ändert die Systemzeit, wodurch sich die Latenzprognose der Performance-Statistiken für überwachte Workloads ändert. Unified Manager beginnt

> umgehend mit der Korrektur der Latenzprognose, was etwa 15 Tage in Anspruch nimmt. Während dieser Zeit kann Unified Manager weiterhin verwendet werden, aber da Unified Manager die Latenzprognose zum Erkennen dynamischer Ereignisse verwendet, sind einige Ereignisse möglicherweise nicht korrekt. Ereignisse, die vor der Zeitumstellung erkannt wurden, sind davon nicht betroffen.

Die Latenzprognose kann für die Leistungsanalyse in Active IQ Unified Manager verwendet werden

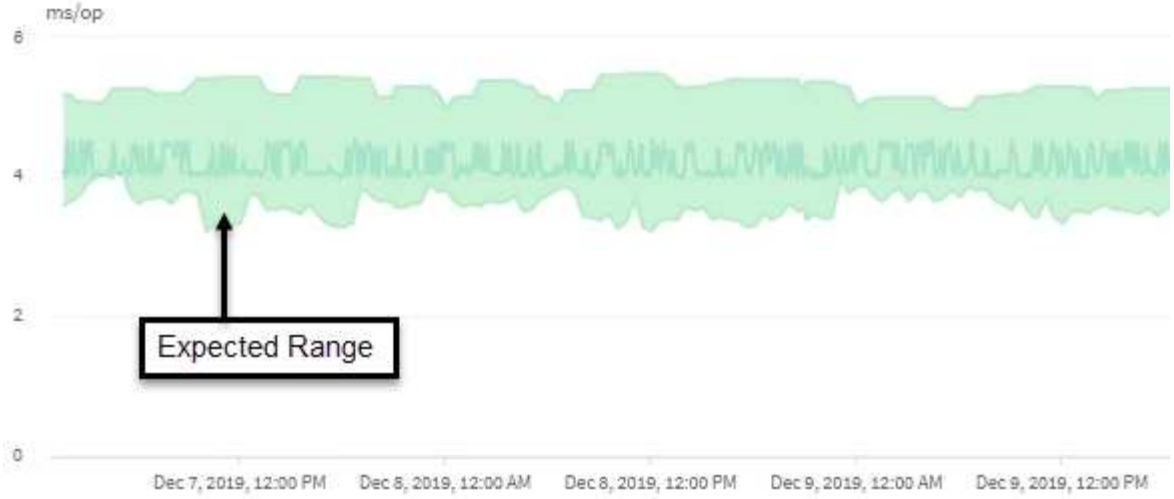
Unified Manager nutzt die Latenzprognose, um die typische E/A-Latenz (Reaktionszeit) Ihrer überwachten Workloads darzustellen. Eine Benachrichtigung erfolgt, wenn die tatsächliche Latenz eines Workloads über der Obergrenze der Latenzprognose liegt, wodurch ein dynamisches Performance-Ereignis ausgelöst wird, sodass das Performance-Problem analysiert und eine Korrekturmaßnahme zu seiner Behebung ergriffen werden kann.

Die Latenzprognose legt die Performance-Basislinie für die Arbeitslast fest. Unified Manager lernt im Laufe der Zeit aus vergangenen Performance-Messungen, um die erwarteten Performance- und Aktivitätsniveaus für die Arbeitslast zu prognostizieren. Die obere Grenze des erwarteten Bereichs legt den dynamischen Performance-Schwellenwert fest. Unified Manager verwendet die Basislinie, um zu bestimmen, wann die tatsächliche Latenz über oder unter einem Schwellenwert liegt oder außerhalb der Grenzen ihres erwarteten Bereichs. Der Vergleich zwischen den tatsächlichen Werten und den erwarteten Werten erstellt ein Performance-Profil für die Arbeitslast.

Wenn die tatsächliche Latenz einer Arbeitslast aufgrund von Konflikten auf einer Clusterkomponente den dynamischen Performance-Schwellenwert überschreitet, ist die Latenz hoch und die Arbeitslast arbeitet langsamer als erwartet. Die Performance anderer Arbeitslasten, die dieselben Clusterkomponenten gemeinsam nutzen, kann ebenfalls geringer als erwartet sein.

Unified Manager analysiert das Überschreiten des Schwellenwerts und ermittelt, ob es sich bei der Aktivität um ein Performance-Ereignis handelt. Wenn die hohe Workload-Aktivität über einen längeren Zeitraum, beispielsweise mehrere Stunden, konstant bleibt, stuft Unified Manager die Aktivität als normal ein und passt die Latenzprognose dynamisch an, um den neuen dynamischen Performance-Schwellenwert zu bilden.

Bei manchen Workloads kann die Aktivität konstant niedrig sein, sodass sich die prognostizierte Latenz im Zeitverlauf nur geringfügig ändert. Um die Anzahl der Ereignisse bei der Analyse von Performanceereignissen zu minimieren, löst Unified Manager ein Ereignis nur für Volumes mit geringer Aktivität aus, deren Operationen und Latenzen deutlich höher als erwartet ausfallen.



In diesem Beispiel weist die Latenz für ein Volume eine Latenzprognose auf, die grau dargestellt bei minimal 3,5 Millisekunden pro Operation (ms/op) und maximal 5,5 ms/op liegt. Wenn die tatsächliche Latenz, blau dargestellt, aufgrund eines kurzzeitigen Anstiegs des Netzwerkverkehrs oder einer Überlastung einer Clusterkomponente plötzlich auf 10 ms/op ansteigt, liegt sie über der Latenzprognose und hat den dynamischen Performance-Schwellenwert überschritten.

Wenn der Netzwerkverkehr abgenommen hat oder die Clusterkomponente nicht mehr um Ressourcen konkurriert, liegt die Latenz wieder innerhalb der Latenzprognose. Wenn die Latenz über einen längeren Zeitraum bei oder über 10 ms/op bleibt, kann zur Behebung des Ereignisses eine Korrekturmaßnahme erforderlich sein.

Verwenden der Workload-Latenz zur Identifizierung von Leistungsproblemen in Active IQ Unified Manager

Die Workload-Latenz (Antwortzeit) ist die Zeit, die ein Volume in einem Cluster benötigt, um auf E/A-Anforderungen von Clientanwendungen zu reagieren. Unified Manager verwendet die Latenz, um Performance-Ereignisse zu erkennen und Sie darüber zu informieren.

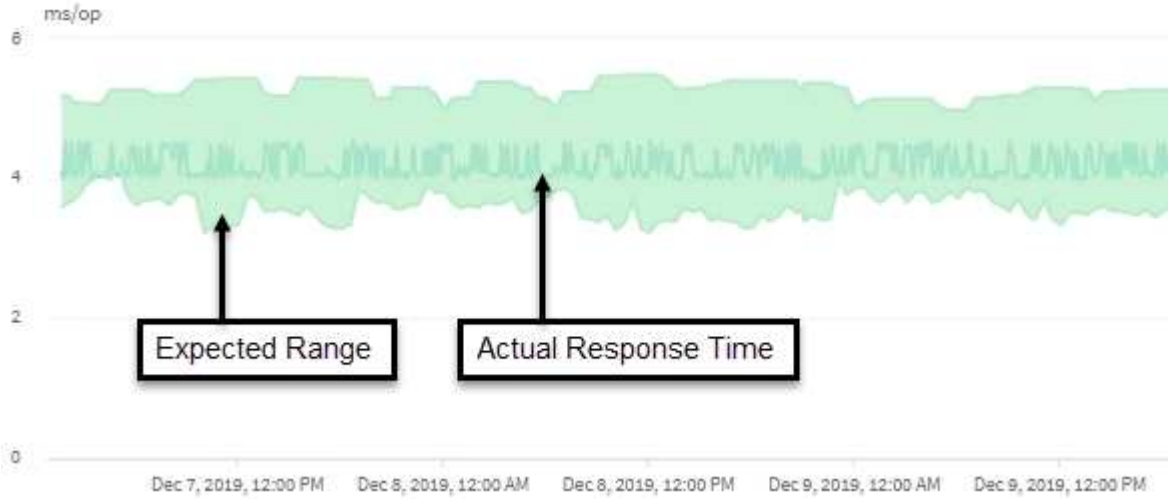
Eine hohe Latenz bedeutet, dass Anfragen von Anwendungen an ein Volume auf einem Cluster länger als üblich dauern. Die Ursache für die hohe Latenz kann im Cluster selbst liegen, beispielsweise durch Engpässe bei einer oder mehreren Clusterkomponenten. Hohe Latenz kann auch durch Probleme außerhalb des Clusters verursacht werden, etwa durch Netzwerkengpässe, Probleme mit dem Client, auf dem die Anwendungen ausgeführt werden, oder Probleme mit den Anwendungen selbst.

Unified Manager überwacht lediglich die Workload-Aktivität auf dem Cluster. Es überwacht weder die Anwendungen noch die Clients oder die Pfade zwischen den Anwendungen und dem Cluster.

Vorgänge im Cluster, wie z. B. Backups oder die Deduplizierung, die den Bedarf an Clusterkomponenten erhöhen, die auch von anderen Workloads genutzt werden, können ebenfalls zu hohen Latenzzeiten führen. Wenn die tatsächliche Latenz den dynamischen Performance Schwellenwert des erwarteten Bereichs (Latenzprognose) überschreitet, analysiert Unified Manager das Ereignis, um festzustellen, ob es sich um ein Performance-Ereignis handelt, das möglicherweise behoben werden muss. Die Latenz wird in Millisekunden pro Vorgang (ms/op) gemessen.

Auf dem Diagramm „Gesamtlatenz“ auf der Seite „Workload-Analyse“ können Sie eine Analyse der

Latenzstatistiken anzeigen, um zu sehen, wie sich die Aktivität einzelner Prozesse, z. B. Lese- und Schreibanforderungen, im Vergleich zu den Gesamt-Latenzstatistiken verhält. Der Vergleich hilft Ihnen dabei, festzustellen, welche Operationen die höchste Aktivität aufweisen oder ob bestimmte Operationen ungewöhnliche Aktivität zeigen, die sich auf die Latenz eines Volumes auswirkt. Bei der Analyse von Performance-Ereignissen können Sie anhand der Latenzstatistiken ermitteln, ob ein Ereignis durch ein Problem im Cluster verursacht wurde. Sie können außerdem die spezifischen Workload-Aktivitäten oder Clusterkomponenten identifizieren, die an dem Ereignis beteiligt sind.



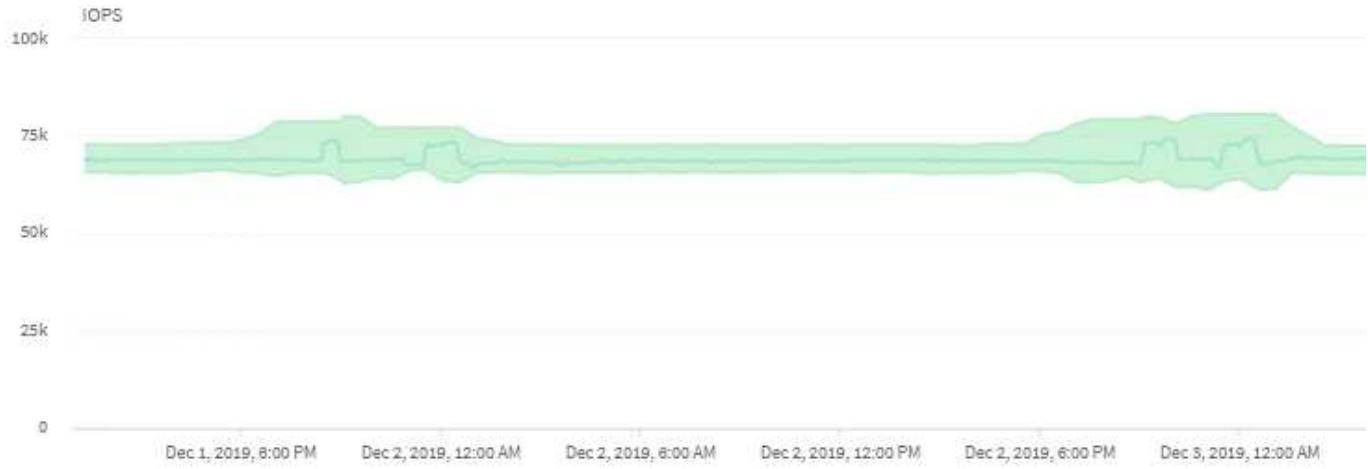
Dieses Beispiel zeigt das Latenzdiagramm. Die tatsächliche Antwortzeit (Latenz) ist eine blaue Linie, und die Latenzprognose (erwarteter Bereich) ist grün.

Die blaue Linie kann Lücken aufweisen, wenn Unified Manager keine Daten erfassen konnte. Dies kann passieren, wenn der Cluster oder das Volume nicht erreichbar war, Unified Manager währenddessen ausgeschaltet war oder die Datenerfassung länger als die vorgesehenen 5 Minuten dauerte.

Bewertung, wie sich Clusteroperationen auf die Workload-Latenz in Active IQ Unified Manager auswirken können

Operationen (IOPS) stellen die Aktivität aller benutzerdefinierten und systemdefinierten Workloads auf einem Cluster dar. Die IOPS-Statistiken helfen dabei festzustellen, ob Clusterprozesse, wie das Erstellen von Backups oder das Ausführen der Deduplizierung, die Workload-Latenz (Antwortzeit) beeinträchtigen oder ein Performance-Ereignis verursacht haben oder dazu beigetragen haben.

Bei der Analyse von Performance-Ereignissen können Sie anhand der IOPS-Statistiken feststellen, ob ein Performance-Ereignis durch ein Problem im Cluster verursacht wurde. Sie können die spezifischen Workload-Aktivitäten identifizieren, die möglicherweise maßgeblich zum Performance-Ereignis beigetragen haben. IOPS werden in Operationen pro Sekunde (ops/sec) gemessen.



Dieses Beispiel zeigt das IOPS-Diagramm. Die tatsächlichen Operationsstatistiken sind als blaue Linie dargestellt, die IOPS-Prognose der Operationsstatistiken als grüne Linie.

> In manchen Fällen, in denen ein Cluster überlastet ist, zeigt Unified Manager möglicherweise die Meldung `Data collection is taking too long on Cluster cluster_name` an. Dies bedeutet, dass nicht genügend Statistiken erfasst wurden, damit Unified Manager eine Analyse durchführen kann. Damit Statistiken erfasst werden können, ist eine Reduzierung der vom Cluster genutzten Ressourcen erforderlich.

Überwachung der MetroCluster Leistung mit Active IQ Unified Manager

Unified Manager ermöglicht es Ihnen, den Schreibdurchsatz zwischen Clustern in einer MetroCluster Konfiguration zu überwachen, um Workloads mit einem hohen Schreibdurchsatz zu identifizieren.

Wenn diese leistungsstarken Workloads dazu führen, dass andere Volumes im lokalen Cluster hohe E/A-Antwortzeiten aufweisen, löst Unified Manager Performance-Ereignisse aus, um Sie zu benachrichtigen.

> Unified Manager behandelt die Cluster in einer MetroCluster Konfiguration als einzelne Cluster. Unified Manager unterscheidet nicht zwischen Partnerclustern und korreliert auch nicht den Schreibdurchsatz der einzelnen Cluster.

Wenn ein lokaler Cluster in einer MetroCluster Konfiguration seine Daten auf seinen Partnercluster spiegelt, werden die Daten in NVRAM geschrieben und dann über die Interswitch Links (ISLs) an die Remote-Aggregate übertragen. Unified Manager analysiert den NVRAM, um die Workloads zu identifizieren, deren hoher Schreibdurchsatz den NVRAM überlastet und dadurch zu Ressourcenkonflikten im NVRAM führt.

Workloads, deren Abweichung bei der Antwortzeit den Performance-Schwellenwert überschritten hat, werden als *victims* bezeichnet, und Workloads, deren Abweichung beim Schreibdurchsatz zum NVRAM höher als üblich ist und dadurch die Ressourcenkonkurrenz verursacht, werden als *bullies* bezeichnet. Da nur die Schreibanforderungen an den Partnercluster gespiegelt werden, analysiert Unified Manager den Lesedurchsatz nicht.

Sie können den Durchsatz jedes Clusters in einer MetroCluster Konfiguration anzeigen, indem Sie die Workloads der entsprechenden LUNs und Volumes auf den folgenden Bildschirmen analysieren. Sie können die Ergebnisse nach dem Cluster filtern. Im linken Navigationsbereich:

- **Storage > Cluster > Performance: Alle Cluster**-Ansicht. Siehe
- **Storage > Volumes > Performance: Alle Volumes** Ansicht.
- **Storage > LUNs > Performance: Alle LUNs** Ansicht.
- **Workload Analyse > Alle Workloads**

Verwandte Informationen

"Performance Ereignisanalyse und Benachrichtigung"

"Performance Ereignisanalyse für eine MetroCluster Konfiguration"

"Rollen der an einem Performance-Ereignis beteiligten Workloads"

"Identifizieren von betroffenen Workloads bei einem Performance-Ereignis"

"Identifizieren von Bully Workloads, die an einem Performance-Ereignis beteiligt sind"

"Ermitteln der Shark-Workloads, die an einem Performance-Ereignis beteiligt sind"

Performance-Ereignisse und Warnmeldungen verstehen

Leistungsereignisse und Warnmeldungen in Active IQ Unified Manager verstehen

Performance Ereignisse sind Vorfälle im Zusammenhang mit der Workload Performance eines Clusters. Sie helfen Ihnen, Workloads mit langsamen Antwortzeiten zu identifizieren. Zusammen mit Systemstatusereignissen, die gleichzeitig aufgetreten sind, können Sie die Probleme ermitteln, die diese langsamen Antwortzeiten möglicherweise verursacht oder dazu beigetragen haben.

Wenn Unified Manager mehrere Vorkommen derselben Ereignisbedingung für dieselbe Clusterkomponente erkennt, betrachtet Unified Manager alle Vorkommen als ein einziges Ereignis und nicht als separate Ereignisse.

Sie können Warnmeldungen so konfigurieren, dass automatisch eine E-Mail-Benachrichtigung gesendet wird, wenn Performance Ereignisse bestimmter Schweregrade auftreten.

Quellen von Leistungsereignissen in Active IQ Unified Manager identifizieren

Performance-Ereignisse sind Probleme im Zusammenhang mit der Performance von Workloads auf einem Cluster. Sie helfen Ihnen, Storage-Objekte mit langsamen Antwortzeiten zu identifizieren, die auch als hohe Latenz bezeichnet werden. Zusammen mit anderen Systemstatusereignissen, die zur gleichen Zeit aufgetreten sind, können Sie die Probleme ermitteln, die die langsamen Antwortzeiten möglicherweise verursacht oder dazu beigetragen haben.

Unified Manager empfängt Performance-Ereignisse aus folgenden Quellen:

- **Benutzerdefinierte Performance-Schwellenwertrichtlinienereignisse**

  Performance-Probleme aufgrund von benutzerdefinierten Schwellenwerten, die Sie festgelegt haben.

Performance-Schwellenwertrichtlinien werden für Storage-Objekte, zum Beispiel Aggregate und Volumes, konfiguriert, sodass Ereignisse generiert werden, wenn ein Schwellenwert für einen Performance-Zähler überschritten wurde.

Zum Empfangen dieser Ereignisse müssen Sie eine Performance-Schwellenwertrichtlinie definieren und sie einem Storage-Objekt zuweisen.

- **Systemdefinierte Ereignisse von Performance-Schwellenwertrichtlinien**

  Performance Probleme aufgrund von Schwellenwerten, die systemdefiniert sind. Diese Schwellenwertrichtlinien sind in der Installation von Unified Manager enthalten, um häufig auftretende Performance Probleme abzudecken.

  Diese Schwellenwertrichtlinien sind standardmäßig aktiviert, und Sie sehen möglicherweise kurz nach dem Hinzufügen eines Clusters Ereignisse.

- **Dynamische Performance-Schwellenwert-Ereignisse**

  Performanceprobleme, die auf Ausfälle oder Fehler in einer IT-Infrastruktur oder auf Workloads zurückzuführen sind, die Clusterressourcen übermäßig nutzen. Die Ursache dieser Ereignisse kann ein einfaches Problem sein, das sich im Lauf der Zeit von selbst behebt oder durch eine Reparatur oder Konfigurationsänderung behoben werden kann. Ein dynamisches Schwellenwertereignis zeigt an, dass die Workloads auf einem ONTAP System aufgrund anderer Workloads mit hoher Auslastung gemeinsam genutzter Clusterkomponenten langsam sind.

  Diese Schwellenwerte sind standardmäßig aktiviert, und es kann vorkommen, dass nach drei Tagen der Datenerfassung von einem neuen Cluster Ereignisse auftreten.

Leistungsereignisse nach Schweregrad in Active IQ Unified Manager priorisieren

Jedes Performance-Ereignis ist einem Typ des Schweregrads zugeordnet, damit Sie die Ereignisse priorisieren können, die eine sofortige Korrekturmaßnahme erfordern.

- **Kritisch**

  Ein Performance-Ereignis ist aufgetreten, das zu einer Dienstunterbrechung führen könnte, wenn nicht umgehend eine Korrekturmaßnahme ergriffen wird.

  Kritische Ereignisse werden nur auf Grundlage benutzerdefinierter Schwellenwerte gesendet.

- **Warnung**

  Ein Performance Zähler für ein Clusterobjekt liegt außerhalb des normalen Bereichs und sollte überwacht werden, um sicherzustellen, dass er nicht den kritischen Schweregrad erreicht. Ereignisse dieses Schweregrads führen nicht zu einer Dienstunterbrechung, und sofortige Korrekturmaßnahmen sind möglicherweise nicht erforderlich.

  Benutzerdefinierte, systemdefinierte oder dynamische Schwellenwerte senden Warnereignisse.

- **Informationen**

  Das Ereignis tritt auf, wenn ein neues Objekt erkannt oder eine Benutzeraktion ausgeführt wird. Wenn beispielsweise ein beliebiges Storage Objekt gelöscht wird oder Konfigurationsänderungen vorgenommen werden, wird ein Ereignis mit dem Typ des Schweregrads Information generiert.

Informationsereignisse werden direkt von ONTAP gesendet, wenn eine Konfigurationsänderung erkannt wird.

Weitere Informationen sind unter den folgenden Links verfügbar:

- "Was passiert, wenn ein Ereignis empfangen wird"
- "Welche Informationen in einer Benachrichtigungs-E-Mail enthalten sind"
- "Hinzufügen von Warnmeldungen"
- "Hinzufügen von Benachrichtigungen für Performance-Ereignisse"

Überwachen von Konfigurationsänderungen, die von Active IQ Unified Manager erkannt wurden

Unified Manager überwacht Ihre Cluster auf Konfigurationsänderungen, um festzustellen, ob eine Änderung ein Performance Ereignis verursacht hat oder dazu beigetragen haben könnte. Die Seiten des Performance Explorer zeigen ein Änderungssymbol ( ) an, das das Datum und die Uhrzeit angibt, zu denen die Änderung erkannt wurde.

Auf den Seiten von Performance Explorer und auf der Seite Workload Analysis können die Performance-Diagramme geprüft werden, um festzustellen, ob sich das Änderungsereignis auf die Performance des ausgewählten Clusterobjekts ausgewirkt hat. Wenn die Änderung gleichzeitig oder ungefähr zur selben Zeit wie ein Performance-Ereignis erkannt wurde, hat sie möglicherweise zu dem Problem beigetragen, das die Ereigniswarnung ausgelöst hat.

Unified Manager kann die folgenden Änderungsereignisse erkennen, die als Informationsereignisse kategorisiert sind:

- Ein Volume bewegt sich zwischen Aggregaten.

  Unified Manager kann erkennen, ob eine Volume Verschiebung ausgeführt wird, abgeschlossen wurde oder fehlgeschlagen ist. Wenn Unified Manager während einer Volume Verschiebung nicht verfügbar ist, erkennt er die Volume Verschiebung nach der Wiederverfügbarkeit und zeigt ein entsprechendes Änderungsereignis an.

- Der Durchsatzgrenzwert (MB/s oder IOPS) einer QoS-Richtliniengruppe, die einen oder mehrere überwachte Workloads enthält, ändert sich.

  Die Änderung eines Grenzwerts einer Richtliniengruppe kann zu vorübergehenden Spitzen bei der Latenz (Antwortzeit) führen, die wiederum Ereignisse für die Richtliniengruppe auslösen können. Die Latenz normalisiert sich allmählich wieder, und alle durch die Spitzen verursachten Ereignisse verlieren ihre Relevanz.

- Ein Knoten in einem HA-Paar übernimmt den Storage seines Partnerknotens oder gibt ihn zurück.

  Unified Manager kann erkennen, wann eine Übernahme, Teilübernahme oder Rückgabe abgeschlossen wurde. Wenn die Übernahme durch einen ausgefallenen Knoten verursacht wird, erkennt Unified Manager dieses Ereignis nicht.

- Ein ONTAP Upgrade oder ein Revert-Vorgang wird erfolgreich abgeschlossen.

  Die vorherige und die neue Version werden angezeigt.

Informationen zu systemdefinierten Leistungsschwellenwertrichtlinien in Active IQ Unified Manager

Unified Manager bietet einige standardmäßige Schwellenwertrichtlinien, die die Cluster-Performance überwachen und automatisch Ereignisse generieren. Diese Richtlinien sind standardmäßig aktiviert, und sie erzeugen Warn- oder Informationsereignisse, sobald die überwachten Performance-Schwellenwerte überschritten werden.

Systemdefinierte Performance-Schwellenwertrichtlinien sind auf Cloud Volumes ONTAP, ONTAP Edge oder ONTAP Select Systemen nicht aktiviert.

Wenn Sie unnötige Ereignisse aus systemdefinierten Performance-Schwellenwertrichtlinien erhalten, können Sie die Ereignisse für einzelne Richtlinien auf der Seite Event Setup deaktivieren.

Schwellenwertrichtlinien für Cluster

Die systemdefinierten Cluster Performance Schwellenwertrichtlinien sind standardmäßig jedem Cluster zugewiesen, das von Unified Manager überwacht wird:

- **Ungleichgewicht der Clusterlast**

  Identifiziert Situationen, in denen ein Knoten im Cluster unter einer deutlich höheren Last arbeitet als andere Knoten im Cluster und dadurch möglicherweise die Workload-Latenzen beeinflusst.

  Dies geschieht durch den Vergleich des Werts der genutzten Performance-Kapazität für alle Knoten in einem Cluster, um festzustellen, ob ein Knoten den Schwellenwert von 30 % seit mehr als 24 Stunden überschritten hat. Dies ist ein Warnereignis.

- **Ungleichgewicht der Clusterkapazität**

  Identifiziert Situationen, in denen ein Aggregat eine deutlich höhere genutzte Kapazität als andere Aggregate im Cluster aufweist und dadurch den für den Betrieb erforderlichen Speicherplatz potenziell beeinträchtigt.

  Dies geschieht durch den Vergleich der genutzten Kapazitätswerte aller Aggregate im Cluster, um festzustellen, ob zwischen beliebigen Aggregaten eine Differenz von 70 % besteht. Dies ist ein Warnereignis.

Node-Schwellenwertrichtlinien

Die systemdefinierten Schwellenwertrichtlinien für die Knoten-Performance sind standardmäßig jedem Knoten in den von Unified Manager überwachten Clustern zugewiesen:

- **Schwellenwert für die genutzte Performance-Kapazität überschritten**

  Identifiziert Situationen, in denen ein einzelner Knoten über die Grenzen seiner Betriebseffizienz hinaus arbeitet und dadurch potenziell die Workload-Latenzen beeinträchtigt.

  Dies erfolgt durch die Suche nach Nodes, die ihre Performance-Kapazität länger als 12 Stunden zu mehr als 100 % auslasten. Dies ist ein Warnereignis.

- **HA-Paar des Knotens überlastet**

  Kennzeichnet Situationen, in denen Knoten in einem HA-Paar außerhalb der Grenzen der betrieblichen

Effizienz des HA-Paars arbeiten.

Dies erfolgt durch Überprüfung des Werts für die genutzte Performance Kapazität der beiden Knoten im HA Paar. Wenn die kombinierte genutzte Performance Kapazität der beiden Knoten länger als 12 Stunden 200 % überschreitet, wirkt sich ein Controller Failover auf die Latenzzeiten der Workloads aus. Dies ist ein Informationsereignis.

- **Festplattenfragmentierung des Node**

  Kennzeichnet Situationen, in denen eine oder mehrere Festplatten in einem Aggregat fragmentiert sind, wodurch wichtige System Services verlangsamt werden und möglicherweise die Workload-Latenzen auf einem Knoten beeinträchtigt werden.

  Dies geschieht durch die Analyse bestimmter Verhältnisse von Lese- und Schreibvorgängen über alle Aggregate auf einem Knoten hinweg. Diese Richtlinie kann auch während der Resynchronisierung von SyncMirror oder bei Fehlern während von Disk-Scrub-Vorgängen ausgelöst werden. Dies ist ein Warnereignis.

  > Die Richtlinie „`Node disk fragmentation`“ analysiert ausschließlich HDD-Aggregate; Flash Pool, SSD und FabricPool Aggregate werden nicht analysiert.

Schwellenwertrichtlinien für Aggregate

Die systemdefinierte Performance-Schwellenwertrichtlinie für Aggregate ist standardmäßig jedem Aggregat in den von Unified Manager überwachten Clustern zugewiesen:

- **Überlastete Aggregate-Festplatten**

  Diese Richtlinie identifiziert Situationen, in denen ein Aggregat oberhalb der Grenzen seiner betrieblichen Effizienz arbeitet und dadurch potenziell die Latenzen von Workloads beeinträchtigt. Sie identifiziert diese Situationen, indem sie nach Aggregaten sucht, bei denen die Festplatten im Aggregat länger als 30 Minuten zu mehr als 95 % ausgelastet sind. Diese Richtlinie mit mehreren Bedingungen führt dann die folgende Analyse durch, um die Ursache des Problems zu ermitteln:

  - Wird auf einer Festplatte im Aggregat gerade eine Hintergrundwartung durchgeführt?

    Zu den Hintergrundwartungsaktivitäten, die bei einer Festplatte ausgeführt werden können, gehören Festplattenrekonstruktion, Festplattenbereinigung, SyncMirror Resynchronisierung und Paritätsreparatur.

  - Gibt es einen Kommunikationsengpass bei der Fibre Channel Verbindung des Disk Shelf?
  - Ist im Aggregat zu wenig freier Speicherplatz vorhanden? Ein Warnereignis wird für diese Richtlinie nur dann ausgegeben, wenn eine (oder mehrere) der drei untergeordneten Richtlinien ebenfalls als verletzt gelten. Ein Performance Ereignis wird nicht ausgelöst, wenn nur die Festplatten im Aggregat zu mehr als 95 % ausgelastet sind.

  > Die Richtlinie „Überbelegung von Aggregatdatenträgern“ analysiert reine HDD-Aggregate und Flash Pool-Aggregate (Hybrid-Aggregate); SSD- und FabricPool Aggregate werden nicht analysiert.

Richtlinien für Latenzschwellenwerte von Workloads

Die systemdefinierten Richtlinien für Latenzschwellenwerte von Workloads sind jeder Workload zugewiesen,

für die eine konfigurierte Performance Service Level-Richtlinie mit einem definierten Wert für „`expected latency`“ vorhanden ist:

- **Workload-Volume/LUN-Latenzschwellenwert gemäß Performance Service Level überschritten**

  Identifiziert Volumes (Dateifreigaben) und LUNs, deren Grenze für die “expected latency” überschritten wurde und die die Workload-Performance beeinträchtigen. Dies ist ein Warnereignis.

  Dies geschieht durch das Ermitteln von Workloads, deren erwarteter Latenzwert während der vorangegangenen Stunde in 30 % der Zeit überschritten wurde.

QoS Schwellenwertrichtlinien

Die systemdefinierten QoS Performance-Schwellenwertrichtlinien werden allen Workloads zugewiesen, für die eine ONTAP QoS Richtlinie für den maximalen Durchsatz (IOPS, IOPS/TB oder MB/s) konfiguriert ist. Unified Manager löst ein Ereignis aus, wenn der Durchsatzwert des Workloads 15 % unter dem konfigurierten QoS-Wert liegt:

- **QoS Max IOPS oder MB/s Schwellenwert**

  Identifiziert Volumes und LUNs, die ihr QoS-Maximum an IOPS oder ihre MB/s-Durchsatzbegrenzung überschritten haben und die Workload-Latenz beeinträchtigen. Dies ist ein Warnereignis.

  Wenn einer Richtliniengruppe eine einzelne Arbeitslast zugewiesen ist, erfolgt dies durch die Suche nach Arbeitslasten, die während jedes Erfassungszeitraums der vorangegangenen Stunde den in der zugewiesenen QoS-Richtliniengruppe definierten maximalen Durchsatzschwellenwert überschritten haben.

  Wenn mehrere Workloads eine einzige QoS-Richtlinie gemeinsam nutzen, addiert das System die IOPS oder MB/s aller Workloads in der Richtlinie und vergleicht diese Gesamtsumme mit dem Schwellenwert.

- **QoS Peak IOPS/TB oder IOPS/TB mit Blockgrößenschwellenwert**

  Kennzeichnet Volumes, die ihre adaptive QoS-Spitzenwert-Durchsatzbegrenzung für IOPS/TB (oder IOPS/TB mit Blockgrößenbegrenzung) überschritten haben und die Latenz der Workloads beeinträchtigen. Dies ist ein Warnereignis.

  Dies geschieht, indem der in der adaptiven QoS-Richtlinie definierte Schwellenwert für maximale IOPS/TB in einen QoS-Maximal-IOPS-Wert auf Basis der Größe jedes Volumes umgerechnet wird und anschließend nach Volumes gesucht wird, die den QoS-Maximal-IOPS-Wert während jedes Performance-Erfassungszeitraums der vorangegangenen Stunde überschritten haben.

  > Diese Richtlinie gilt nur für Volumes, wenn der Cluster mit ONTAP 9.3 oder höherer Software installiert ist.

  Wenn das Element “block size” in der adaptiven QoS-Richtlinie definiert wurde, wird der Schwellenwert basierend auf der Größe jedes Volumes in einen QoS-Wert für maximale MB/s umgewandelt. Anschließend wird nach Volumes gesucht, die während jedes Performance Erfassungszeitraums in der vorherigen Stunde den QoS-Wert für max. MB/s überschritten haben.

  > Diese Richtlinie gilt nur für Volumes, wenn der Cluster mit ONTAP 9.5 und höherer Software installiert ist.

Analyse von Leistungsereignissen und Benachrichtigungen in Active IQ Unified Manager

Performance Ereignisse informieren Sie über E/A-Performanceprobleme bei einem Workload, die durch Ressourcenkonflikte auf einer Cluster-Komponente verursacht werden. Unified Manager analysiert das Ereignis, um alle beteiligten Workloads, die umkämpfte Komponente und zu ermitteln, ob das Ereignis weiterhin ein Problem darstellt, das möglicherweise behoben werden muss.

Unified Manager überwacht die E/A-Latenz (Antwortzeit) und die IOPS (Operationen) für Volumes auf einem Cluster. Wenn andere Workloads eine Clusterkomponente übermäßig beanspruchen, steht die Komponente beispielsweise in Konkurrenz und kann die Anforderungen der Workloads nicht auf einem optimalen Level erfüllen. Die Performance anderer Workloads, die dieselbe Komponente verwenden, kann dadurch beeinträchtigt werden, sodass sich ihre Latenzen erhöhen. Wenn die Latenz den dynamischen Performance-Schwellenwert überschreitet, löst Unified Manager ein Performance-Ereignis aus und benachrichtigt Sie.

Ereignisanalyse

Unified Manager führt die folgenden Analysen anhand der Performance Statistiken der vorherigen 15 Tage durch, um die betroffenen Workloads, die verursachenden Workloads und die an einem Ereignis beteiligte Clusterkomponente zu identifizieren:

- Identifiziert beeinträchtigte Workloads, deren Latenz den dynamischen Performance-Schwellenwert überschritten hat, der die obere Grenze der Latenzprognose darstellt:
  - Bei Volumes auf HDD- oder Flash Pool Hybridaggregaten (lokale Ebene) werden Ereignisse nur dann ausgelöst, wenn die Latenz größer als 5 Millisekunden (ms) ist und die IOPS mehr als 10 Operationen pro Sekunde (ops/sec) betragen.
  - Bei Volumes auf All-SSD-Aggregaten oder FabricPool Aggregaten (Cloud-Tier) werden Ereignisse nur dann ausgelöst, wenn die Latenz größer als 1 ms ist und die IOPS mehr als 100 Ops/Sek. betragen.
- Identifiziert die Clusterkomponente im Konflikt.

  Wenn die Latenz der betroffenen Workloads am Cluster-Interconnect größer als 1 ms ist, wertet Unified Manager dies als erheblich und löst ein Ereignis für den Cluster-Interconnect aus.

- Identifiziert die störenden Workloads, die die Clusterkomponente übermäßig beanspruchen und zu Ressourcenkonflikten führen.
- Die beteiligten Workloads werden anhand ihrer Abweichung bei der Auslastung oder Aktivität einer Clusterkomponente eingestuft, um festzustellen, welche Störenfriede die größte Änderung bei der Nutzung der Clusterkomponente aufweisen und welche Opfer am stärksten beeinträchtigt sind.

Ein Ereignis kann nur kurzzeitig auftreten und sich dann selbst beheben, sobald die betroffene Komponente nicht mehr im Konflikt steht. Ein kontinuierliches Ereignis tritt innerhalb eines Fünf-Minuten-Intervalls für dieselbe Clusterkomponente wiederholt auf und bleibt aktiv. Bei kontinuierlichen Ereignissen löst Unified Manager eine Warnung aus, nachdem dasselbe Ereignis in zwei aufeinanderfolgenden Analyseintervallen erkannt wurde.

Sobald ein Ereignis behoben ist, bleibt es in Unified Manager als Teil der Aufzeichnung früherer Performance Probleme für ein Volume verfügbar. Jedes Ereignis verfügt über eine eindeutige ID, die den Ereignistyp sowie die beteiligten Volumes, den Cluster und die Clusterkomponenten identifiziert.

Ein einzelnes Volume kann gleichzeitig an mehr als einem Ereignis beteiligt sein.

Ereignisstatus

Ereignisse können sich in einem der folgenden Zustände befinden:

- **Aktiv**

  Zeigt an, dass das Performance-Ereignis derzeit aktiv ist (neu oder bestätigt). Das Problem, das das Ereignis verursacht, hat sich nicht von selbst behoben oder ist noch nicht gelöst. Der Performance-Zähler für das Storage-Objekt bleibt weiterhin über dem Performance-Schwellenwert.

- **Veraltet**

  Zeigt an, dass das Ereignis nicht mehr aktiv ist. Das Problem, das das Ereignis verursacht hat, hat sich selbst behoben oder wurde gelöst. Der Performance-Zähler für das Storage-Objekt liegt nicht mehr über dem Performance-Schwellenwert.

Ereignisbenachrichtigung

Die Ereignisse werden auf der Dashboard-Seite und auf vielen anderen Seiten der Benutzeroberfläche angezeigt, und Warnmeldungen für diese Ereignisse werden an festgelegte E-Mail-Adressen gesendet. Detaillierte Analyseinformationen zu einem Ereignis sowie Vorschläge zu seiner Behebung sind auf der Seite „Ereignisdetails“ und auf der Seite „Arbeitslastanalyse“ verfügbar.

Ereignisinteraktion

Auf der Seite „Ereignisdetails“ und auf der Seite „Arbeitslastanalyse“ können Sie auf folgende Weise mit Ereignissen interagieren:

- Beim Bewegen der Maus über ein Ereignis erscheint eine Meldung mit Datum und Uhrzeit der Ereigniserkennung.

  Wenn mehrere Ereignisse für denselben Zeitraum vorliegen, zeigt die Meldung die Anzahl der Ereignisse an.

- Beim Klicken auf ein einzelnes Ereignis öffnet sich ein Dialogfeld, das detailliertere Informationen über das Ereignis sowie die beteiligten Clusterkomponenten enthält.

  Die betreffende Komponente ist eingekreist und rot hervorgehoben. Über **View full analysis** lässt sich die vollständige Analyse auf der Seite mit den Ereignisdetails anzeigen. Wenn für denselben Zeitraum mehrere Ereignisse vorliegen, zeigt das Dialogfeld Details zu den drei neuesten Ereignissen an. Durch Klicken auf ein Ereignis lässt sich die Ereignisanalyse auf der Seite mit den Ereignisdetails anzeigen.

Es wird erläutert, wie Active IQ Unified Manager die Leistungsauswirkungen eines Ereignisses ermittelt.

Unified Manager nutzt die Abweichung bei Aktivität, Auslastung, Schreibdurchsatz, Clusterkomponentennutzung oder E/A-Latenz (Antwortzeit) einer Arbeitslast, um das Level der Auswirkungen auf die Performance der Arbeitslast zu bestimmen. Diese Informationen bestimmen die Rolle jeder Arbeitslast im Ereignis und wie sie auf der Seite „Ereignisdetails“ eingestuft werden.

Unified Manager vergleicht die zuletzt analysierten Werte einer Arbeitslast mit dem erwarteten Wertebereich (Latenzprognose). Die Differenz zwischen den zuletzt analysierten Werten und dem erwarteten Wertebereich identifiziert die Arbeitslasten, deren Performance am stärksten durch das Ereignis beeinträchtigt wurde.

Angenommen, ein Cluster enthält zwei Workloads: Workload A und Workload B. Die prognostizierte Latenz für Workload A liegt bei 5-10 Millisekunden pro Operation (ms/op), und die tatsächliche Latenz liegt in der Regel bei etwa 7 ms/op. Die prognostizierte Latenz für Workload B liegt bei 10-20 ms/op, und die tatsächliche Latenz liegt in der Regel bei etwa 15 ms/op. Beide Workloads liegen deutlich innerhalb ihrer prognostizierten Latenz. Aufgrund von Ressourcenkonflikten im Cluster steigt die Latenz beider Workloads auf 40 ms/op und überschreitet damit den dynamischen Performance-Schwellenwert, der die Obergrenze der prognostizierten Latenz darstellt, wodurch Ereignisse ausgelöst werden. Die Abweichung der Latenz von den erwarteten Werten zu den Werten oberhalb des Performance-Schwellenwerts beträgt für Workload A etwa 33 ms/op und für Workload B etwa 25 ms/op. Die Latenz beider Workloads steigt zwar auf 40 ms/op, aber Workload A hatte die größere Auswirkung auf die Performance, weil die Latenzabweichung hier mit 33 ms/op höher war.

Auf der Seite mit den Ereignisdetails können Sie im Abschnitt „Systemdiagnose“ Workloads nach ihrer Abweichung bei Aktivität, Auslastung oder Durchsatz für eine Clusterkomponente sortieren. Workloads können auch nach Latenz sortiert werden. Wenn Sie eine Sortieroption auswählen, analysiert Unified Manager die Abweichung bei Aktivität, Auslastung, Durchsatz oder Latenz seit der Erkennung des Ereignisses von den erwarteten Werten, um die Sortierreihenfolge der Workloads zu bestimmen. Bei der Latenz zeigen die roten Punkte (🔴) die Überschreitung eines Performance-Schwellenwerts durch einen betroffenen Workload und die anschließenden Auswirkungen auf die Latenz an. Jeder rote Punkt weist auf ein höheres Level der Latenzabweichung hin und hilft Ihnen dabei, die betroffenen Workloads zu identifizieren, deren Latenz am stärksten von einem Ereignis beeinflusst wurde.

Clusterkomponenten und Ressourcenkonflikte in Active IQ Unified Manager verstehen

Cluster-Performance-Probleme lassen sich erkennen, wenn eine Clusterkomponente in einen Ressourcenkonflikt gerät. Die Performance der Workloads, die die Komponente nutzen, nimmt ab, und ihre Antwortzeit (Latenz) für Clientanfragen steigt, was ein Ereignis in Unified Manager auslöst.

Eine Komponente, die um Ressourcen konkurriert, kann nicht auf einem optimalen Level arbeiten. Ihre Performance hat abgenommen, und die Performance anderer Clusterkomponenten und Workloads, die als *victims* bezeichnet werden, kann eine erhöhte Latenz aufweisen. Eine Komponente lässt sich aus der Ressourcenkonkurrenz herausbringen, indem ihre Workload reduziert oder ihre Fähigkeit erhöht wird, mehr Arbeit zu bewältigen, sodass die Performance wieder normale Werte erreicht. Da Unified Manager die Workload-Performance in Fünf-Minuten-Intervallen erfasst und analysiert, erkennt Unified Manager nur, wenn eine Clusterkomponente dauerhaft überbeansprucht wird. Vorübergehende Spitzen der Überbeanspruchung, die innerhalb des Fünf-Minuten-Intervalls nur kurz andauern, werden nicht erkannt.

Ein Storage-Aggregat kann beispielsweise überlastet sein, weil ein oder mehrere Workloads darauf um die Erfüllung ihrer E/A-Anforderungen konkurrieren. Andere Workloads auf dem Aggregat können dadurch beeinträchtigt werden, was zu einer geringeren Performance führt. Um den Aktivitätsgrad auf dem Aggregat zu verringern, stehen verschiedene Maßnahmen zur Verfügung, z. B. das Verschieben eines oder mehrerer Workloads auf ein weniger stark ausgelastetes Aggregat oder einen weniger stark ausgelasteten Knoten, um die Gesamtlast auf dem aktuellen Aggregat zu senken. Bei einer QoS-Richtliniengruppe kann die Durchsatzbegrenzung angepasst werden, oder Workloads können in eine andere Richtliniengruppe verschoben werden, sodass die Workloads nicht mehr gedrosselt werden.

Unified Manager überwacht die folgenden Clusterkomponenten und benachrichtigt Sie, wenn diese in Konflikt geraten:

- **Netzwerk**

  Stellt die Wartezeit von E/A-Anfragen durch die externen Netzwerkprotokolle im Cluster dar. Die Wartezeit entspricht der Zeit, die vergeht, bis „`transfer ready`“-Transaktionen abgeschlossen sind, bevor der Cluster auf eine E/A-Anfrage reagieren kann. Bei einer Überlastung der Netzwerkkomponente bedeutet dies, dass eine hohe Wartezeit auf der Protokollschicht die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **Netzwerkverarbeitung**

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen der Protokollschicht und dem Cluster beteiligt ist. Der Knoten, der die Netzwerkverarbeitung übernimmt, kann sich seit der Erkennung des Ereignisses geändert haben. Wenn die Netzwerkverarbeitungskomponente um Ressourcen konkurriert, bedeutet dies, dass eine hohe Auslastung des Netzwerkverarbeitungsknotens die Latenz eines oder mehrerer Workloads beeinträchtigt.

  Bei Verwendung eines All SAN Array Cluster in einer Aktiv/Aktiv-Konfiguration wird der Wert der Netzwerkverarbeitungslatenz für beide Knoten angezeigt, sodass Sie überprüfen können, ob die Knoten die Last gleichmäßig teilen.

- **Maximaler QoS-Grenzwert**

  Stellt die maximale Durchsatzeinstellung (Spitzenwert) der dem Storage Workload zugewiesenen QoS-Richtliniengruppe (Quality of Service) dar. Wenn die Richtliniengruppenkomponente um Ressourcen konkurriert, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch die festgelegte Durchsatzbegrenzung gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- **Mindest-QoS-Grenzwert**

  Stellt die Latenz einer Arbeitslast dar, die durch die für andere Arbeitslasten zugewiesene minimale QoS-Durchsatzeinstellung (erwartet) verursacht wird. Wenn die für bestimmte Arbeitslasten festgelegte minimale QoS-Vorgabe den Großteil der Bandbreite nutzt, um den zugesicherten Durchsatz zu gewährleisten, werden andere Arbeitslasten gedrosselt und weisen eine höhere Latenz auf.

- **Cluster-Verbindung**

  Stellt die Kabel und Adapter dar, mit denen Cluster-Knoten physisch verbunden sind. Wenn die Cluster-Interconnect-Komponente ausgelastet ist, bedeutet dies, dass hohe Wartezeiten für E/A-Anforderungen am Cluster-Interconnect die Latenz eines oder mehrerer Workloads beeinträchtigen.

- **Data Processing**

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen dem Cluster und dem Storage-Aggregat beteiligt ist, das die Workload enthält. Der Knoten, der die Data Processing verarbeitet, hat sich seit der Erkennung des Ereignisses möglicherweise geändert. Wenn die Data Processing Komponente einen Ressourcenkonflikt aufweist, bedeutet dies, dass eine hohe Auslastung des Data Processing Knotens die Latenz einer oder mehrerer Workloads beeinträchtigt.

- **Volume Aktivierung**

  Stellt den Prozess dar, der die Nutzung aller aktiven Volumes verfolgt. In großen Umgebungen, in denen mehr als 1000 Volumes aktiv sind, verfolgt dieser Prozess, wie viele kritische Volumes gleichzeitig über den Knoten auf Ressourcen zugreifen müssen. Wenn die Anzahl gleichzeitig aktiver Volumes den empfohlenen maximalen Schwellenwert überschreitet, tritt bei einigen der nicht kritischen Volumes die hier

angegebene Latenz auf.

- **MetroCluster Ressourcen**

  Stellt die MetroCluster Ressourcen dar, einschließlich NVRAM und Interswitch Links (ISLs), die zum Spiegeln von Daten zwischen Clustern in einer MetroCluster Konfiguration verwendet werden. Wenn bei der MetroCluster Komponente eine Ressourcenkonkurrenz besteht, bedeutet dies, dass ein hoher Schreibdurchsatz von Workloads im lokalen Cluster oder ein Problem mit dem Zustand einer Verbindung die Latenz eines oder mehrerer Workloads im lokalen Cluster beeinträchtigt. Wenn sich der Cluster nicht in einer MetroCluster Konfiguration befindet, erscheint dieses Symbol nicht.

- **Aggregat- oder SSD-Aggregat-Operationen**

  Stellt das Storage-Aggregat dar, auf dem die Workloads ausgeführt werden. Wenn die Aggregatkomponente in Konkurrenz steht, bedeutet dies, dass eine hohe Auslastung des Aggregats die Latenz eines oder mehrerer Workloads beeinträchtigt. Ein Aggregat besteht entweder ausschließlich aus HDDs, aus einer Mischung aus HDDs und SSDs (ein Flash Pool Aggregat) oder aus einer Mischung aus HDDs und einer Cloud-Tier-Ebene (ein FabricPool Aggregat). Ein „SSD Aggregate“ besteht ausschließlich aus SSDs (ein All-Flash-Aggregat) oder aus einer Mischung aus SSDs und einer Cloud-Tier-Ebene (ein FabricPool Aggregat).

- **Cloud-Latenz**

  Stellt die Softwarekomponente im Cluster dar, die für die E/A-Verarbeitung zwischen dem Cluster und dem Cloud-Tier zuständig ist, auf dem Benutzerdaten gespeichert werden. Wenn die Cloud-Latenzkomponente ausgelastet ist, bedeutet dies, dass eine große Anzahl von Lesezugriffen auf Volumes, die auf dem Cloud-Tier gehostet werden, die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **Synchrones SnapMirror**

  Stellt die Softwarekomponente im Cluster dar, die an der Replikation von Benutzerdaten vom primären Volume zum sekundären Volume in einer synchronen SnapMirror Beziehung beteiligt ist. Wenn die synchrone SnapMirror Komponente um Ressourcen konkurriert, bedeutet dies, dass die Aktivität synchroner SnapMirror Operationen die Latenz eines oder mehrerer Workloads beeinträchtigt.

Arbeitslastrollen in Leistungsereignissen in Active IQ Unified Manager

Unified Manager verwendet Rollen, um die Beteiligung eines Workloads an einem Performance-Ereignis zu identifizieren. Zu diesen Rollen gehören Opfer, Täter und Aggressoren. Ein benutzerdefinierter Workload kann gleichzeitig Opfer, Täter und Aggressor sein.

Rolle	Beschreibung
Opfer	Eine benutzerdefinierte Arbeitslast, deren Performance aufgrund anderer Arbeitslasten, sogenannter Bullies, die eine Clusterkomponente übermäßig beanspruchen, gesunken ist. Nur benutzerdefinierte Arbeitslasten werden als Opfer identifiziert. Unified Manager identifiziert Opfer-Arbeitslasten anhand ihrer Latenzabweichung, wobei die tatsächliche Latenz während eines Ereignisses im Vergleich zur Latenzprognose (erwarteter Bereich) deutlich angestiegen ist.

Rolle	Beschreibung
Mobber	Eine benutzerdefinierte oder systemdefinierte Arbeitslast, deren übermäßige Nutzung einer Clusterkomponente dazu geführt hat, dass die Performance anderer Arbeitslasten, sogenannter Opfer, abgenommen hat. Unified Manager identifiziert Bully-Workloads anhand ihrer Abweichung bei der Nutzung einer Clusterkomponente, wobei die tatsächliche Nutzung während eines Ereignisses im Vergleich zum erwarteten Nutzungsbereich stark angestiegen ist.
Hai	Eine benutzerdefinierte Workload mit der höchsten Auslastung einer Clusterkomponente im Vergleich zu allen an einem Ereignis beteiligten Workloads. Unified Manager identifiziert Shark Workloads anhand ihrer Nutzung einer Clusterkomponente während eines Ereignisses.

Workloads auf einem Cluster können viele der Cluster-Komponenten gemeinsam nutzen, wie z. B. Aggregate und die CPU für Netzwerk- und Datenverarbeitung. Wenn ein Workload, wie z. B. ein Volume, seine Nutzung einer Cluster-Komponente so weit steigert, dass die Komponente die Workload-Anforderungen nicht mehr effizient erfüllen kann, befindet sich die Komponente in Ressourcenkonflikten (Contention). Der Workload, der eine Cluster-Komponente übermäßig nutzt, wird als Bully bezeichnet. Die anderen Workloads, die diese Komponenten gemeinsam nutzen und deren Performance durch den Bully beeinträchtigt wird, sind die Opfer (Victims). Aktivitäten von systemdefinierten Workloads wie Deduplizierung oder Snapshot Kopien können ebenfalls zu “Bullying” eskalieren.

Wenn Unified Manager ein Ereignis erkennt, identifiziert er alle beteiligten Workloads und Clusterkomponenten, einschließlich der Bully-Workloads, die das Ereignis verursacht haben, der Clusterkomponente, um die konkurriert wird, und der Opfer-Workloads, deren Performance aufgrund der erhöhten Aktivität der Bully-Workloads abgenommen hat.

Kann Unified Manager die ressourcenintensiven Workloads nicht identifizieren, gibt er nur eine Warnung zu den betroffenen Workloads und der beteiligten Clusterkomponente aus.

Unified Manager kann Workloads identifizieren, die Opfer dominanter Workloads sind, und auch erkennen, wann diese Workloads selbst zu dominanten Workloads werden. Ein Workload kann für sich selbst ein dominanter Workload sein. Beispielsweise führt ein hochperformanter Workload, der durch ein Limit einer Richtliniengruppe gedrosselt wird, dazu, dass alle Workloads in der Richtliniengruppe gedrosselt werden, einschließlich ihm selbst. Ein Workload, der bei einem laufenden Performance-Ereignis ein dominanter Workload oder ein Opfer ist, kann seine Rolle ändern oder nicht mehr an dem Ereignis beteiligt sein.

Performance-Schwellenwerte managen

Verwalten von Leistungsschwellenwerten in Active IQ Unified Manager

Performance-Schwellenwertrichtlinien ermöglichen es Ihnen, den Punkt zu bestimmen, an dem Unified Manager ein Ereignis generiert, um Systemadministratoren über Probleme zu informieren, die sich auf die Workload-Performance auswirken könnten. Diese Schwellenwertrichtlinien sind als *benutzerdefinierte* Performance-Schwellenwerte

bekannt.

Diese Version unterstützt benutzerdefinierte, systemdefinierte und dynamische Performance Schwellenwerte. Bei dynamischen und systemdefinierten Performance Schwellenwerten analysiert Unified Manager die Workload Aktivität, um den geeigneten Schwellenwert zu ermitteln. Mit benutzerdefinierten Schwellenwerten können Sie die oberen Performance Grenzwerte für viele Performance Zähler und für viele Storage Objekte festlegen.

Systemdefinierte Performance-Schwellenwerte und dynamische Performance-Schwellenwerte werden von Unified Manager festgelegt und sind nicht konfigurierbar. Falls Sie unnötige Ereignisse von systemdefinierten Performance-Schwellenwertrichtlinien erhalten, können einzelne Richtlinien auf der Seite „Ereigniseinstellungen“ deaktiviert werden.

Verwendung benutzerdefinierter Leistungsschwellenwertrichtlinien in Active IQ Unified Manager

Sie legen für Storage-Objekte (z. B. für Aggregate und Volumes) Performance-Schwellenwertrichtlinien fest, damit der Storage-Administrator ein Ereignis erhält, das ihn darüber informiert, dass im Cluster ein Performance-Problem auftritt.

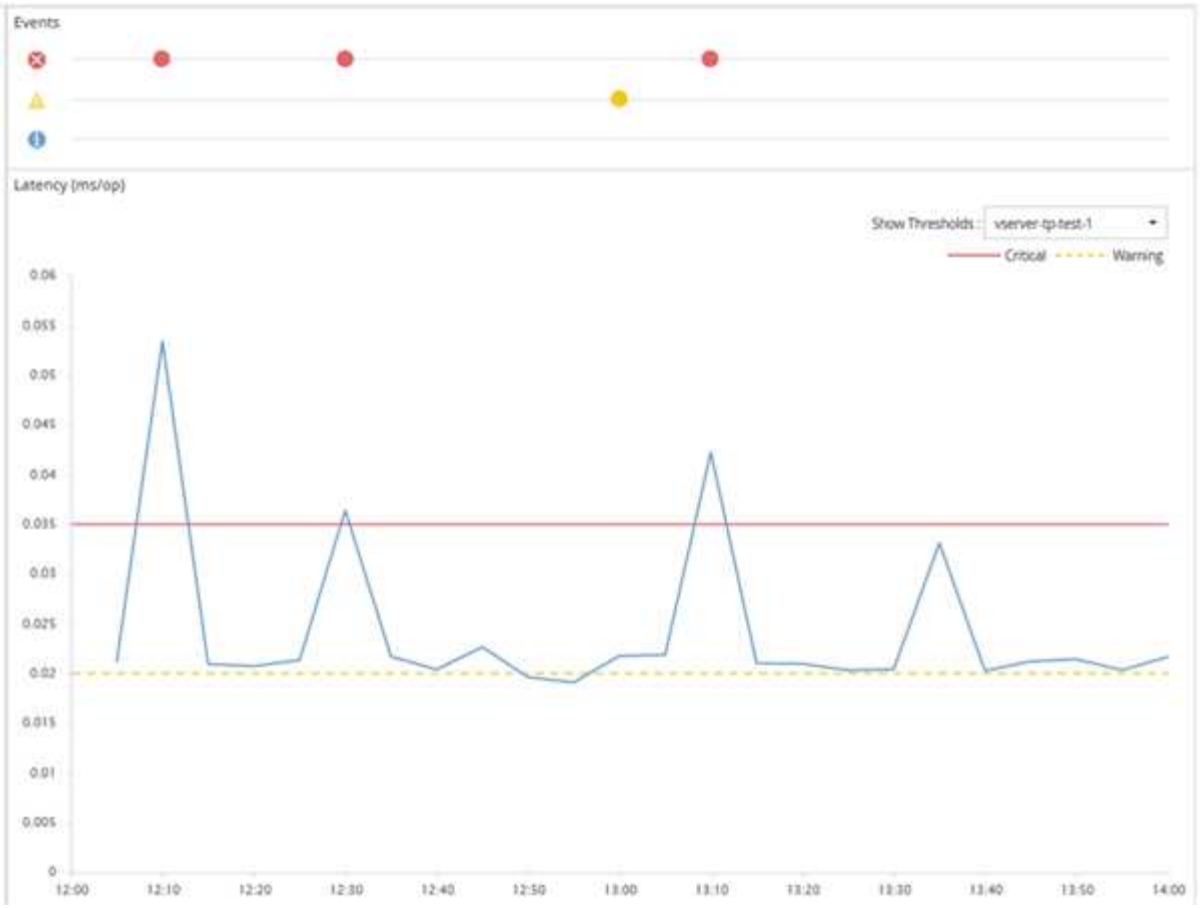
Sie erstellen eine Performance-Schwellenwertrichtlinie für ein Storage-Objekt wie folgt:

- Auswahl eines Storage-Objekts
- Auswahl eines diesem Objekt zugeordneten Performance-Zählers
- Festlegen von Werten zur Definition der oberen Grenzwerte von Performance-Zählern, die als Warn- und kritische Situationen gelten
- Festlegung eines Zeitraums, der definiert, wie lange der Zähler den oberen Grenzwert überschreiten muss

Beispielsweise können Sie für ein Volume eine Performance-Schwellenwertrichtlinie festlegen, sodass Sie eine Benachrichtigung über ein kritisches Ereignis erhalten, wenn die IOPS für dieses Volume 10 fortlaufende Minuten lang 750 Operationen pro Sekunde überschreiten. Dieselbe Schwellenwertrichtlinie kann auch vorsehen, dass Sie ein Warnereignis erhalten, wenn die IOPS 10 Minuten lang 500 Operationen pro Sekunde überschreiten.

Die aktuelle Version bietet Schwellenwerte, die Ereignisse auslösen, wenn ein Zählerwert den festgelegten Schwellenwert überschreitet. Es können keine Schwellenwerte festgelegt werden, die Ereignisse auslösen, wenn ein Zählerwert unter einen festgelegten Schwellenwert fällt.

Hier ist ein Beispiel für ein Zählerdiagramm dargestellt, das zeigt, dass ein Warnschwellenwert (gelbes Symbol) um 1:00 Uhr überschritten wurde und dass ein kritischer Schwellenwert (rotes Symbol) um 12:10 Uhr, 12:30 Uhr und 1:10 Uhr überschritten wurde:



Eine Schwellenwertüberschreitung muss über den festgelegten Zeitraum hinweg kontinuierlich erfolgen. Sinkt der Schwellenwert aus irgendeinem Grund unter die Grenzwerte, gilt eine nachfolgende Überschreitung als Beginn eines neuen Zeitraums.

Einige Clusterobjekte und Performance-Zähler ermöglichen das Erstellen einer kombinierten Schwellenwertrichtlinie, bei der zwei Performance-Zähler ihre Maximalwerte überschreiten müssen, bevor ein Ereignis generiert wird. Beispielsweise lässt sich eine Schwellenwertrichtlinie anhand der folgenden Kriterien erstellen:

Clusterobjekt	Performance-Zähler	Warnschwelle	Kritischer Schwellenwert	Dauer
Volumen	Latenz	10 Millisekunden	20 Millisekunden	15 Minuten
Aggregat	Verwendung	65%	85%	

Schwellenwertrichtlinien, die zwei Clusterobjekte verwenden, bewirken, dass ein Ereignis nur dann generiert wird, wenn beide Bedingungen verletzt werden. Zum Beispiel bei Verwendung der in der Tabelle definierten Schwellenwertrichtlinie:

Wenn die Volume-Latenz im Durchschnitt …	Und die Festplattenauslastung des Aggregats beträgt…	Dann…
15 Millisekunden	50%	Es liegt kein gemeldetes Ereignis vor.
15 Millisekunden	75%	Ein Warnereignis wird gemeldet.
25 Millisekunden	75%	Ein Warnereignis wird gemeldet.

Wenn die Volume-Latenz im Durchschnitt …	Und die Festplattenauslastung des Aggregats beträgt…	Dann…
25 Millisekunden	90%	Es wurde ein kritisches Ereignis gemeldet.

Reaktion auf Verstöße gegen Leistungsschwellenwertrichtlinien in Active IQ Unified Manager

Wenn ein Zählerwert den definierten Performance-Schwellenwert für die in der Dauer angegebene Zeitspanne überschreitet, gilt der Schwellenwert als verletzt und ein Ereignis wird gemeldet.

Das Ereignis löst folgende Aktionen aus:

- Das Ereignis wird im Dashboard, auf der Seite Performance Cluster Summary, auf der Seite Events und auf der objektspezifischen Seite Performance Inventory angezeigt.
- (Optional) Es kann eine E-Mail-Benachrichtigung über das Ereignis an einen oder mehrere E-Mail-Empfänger sowie ein SNMP-Trap an einen Trap-Empfänger gesendet werden.
- (optional) Ein Skript kann ausgeführt werden, um Storage-Objekte automatisch zu ändern oder zu aktualisieren.

Die erste Aktion wird immer ausgeführt. Auf der Seite „Alert Setup“ wird festgelegt, ob die optionalen Aktionen ausgeführt werden. Es können eindeutige Aktionen definiert werden, je nachdem, ob eine Schwellenwertrichtlinie vom Typ „Warning“ oder „Critical“ verletzt wird.

Nachdem bei einem Storage Objekt ein Verstoß gegen eine Performance-Schwellenwertrichtlinie aufgetreten ist, werden für diese Richtlinie keine weiteren Ereignisse generiert, bis der Zählerwert unter den Schwellenwert fällt. Dann wird die Dauer für diese Begrenzung zurückgesetzt. Solange der Schwellenwert weiterhin überschritten wird, wird die Endzeit des Ereignisses fortlaufend aktualisiert, um anzuzeigen, dass dieses Ereignis noch andauert.

Ein Schwellenwertereignis erfasst bzw. fixiert die Informationen zu Schweregrad und Richtliniendefinition, sodass zusammen mit dem Ereignis eindeutige Schwellenwertinformationen angezeigt werden, selbst wenn die Schwellenwertrichtlinie in Zukunft geändert wird.

Leistungsindikatoren verstehen, die mithilfe von Schwellenwerten in Active IQ Unified Manager verfolgt werden

Einige gängige Performance-Zähler, wie IOPS und MB/s, können Schwellenwerte für alle Storage-Objekte festlegen. Es gibt andere Zähler, für die sich Schwellenwerte nur für bestimmte Storage-Objekte festlegen lassen.

Verfügbare Performance-Zähler

Speicherobjekt	Performance-Zähler	Beschreibung
Cluster	IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabeoperationen, die der Cluster pro Sekunde verarbeitet.

Speicherobjekt	Performance-Zähler	Beschreibung
MB/s	Durchschnittliche Anzahl der Megabyte an Daten, die pro Sekunde zu und von diesem Cluster übertragen werden.	Node
IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabeoperationen, die der Knoten pro Sekunde verarbeitet.	MB/s
Durchschnittliche Anzahl von Megabyte an Daten, die pro Sekunde zu und von diesem Knoten übertragen werden.	Latenz	Durchschnittliche Anzahl der Millisekunden, die der Knoten benötigt, um auf Applikationsanforderungen zu reagieren.
Verwendung	Durchschnittlicher Prozentsatz der CPU- und RAM-Auslastung des Knotens.	Verwendete Performance-Kapazität
Durchschnittlicher Prozentsatz der Performance-Kapazität, die vom Knoten verbraucht wird.	Genutzte Performance-Kapazität - Takeover	Durchschnittlicher Prozentsatz der Performancekapazität, der vom Knoten verbraucht wird, zuzüglich der Performancekapazität seines Partnerknotens.
Aggregat	IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabeoperationen, die das Aggregat pro Sekunde verarbeitet.
MB/s	Durchschnittliche Anzahl der Megabyte an Daten, die pro Sekunde zu und von diesem Aggregat übertragen werden.	Latenz
Durchschnittliche Anzahl der Millisekunden, die das Aggregat benötigt, um auf Anfragen der Applikation zu antworten.	Verwendung	Durchschnittlicher Prozentsatz der im Aggregat verwendeten Festplatten.
Verwendete Performance-Kapazität	Durchschnittlicher Prozentsatz der Performancekapazität, der vom Aggregat verbraucht wird.	Speicher-VM
IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabeoperationen, die die SVM pro Sekunde verarbeitet.	MB/s
Durchschnittliche Anzahl der Megabyte an Daten, die pro Sekunde zu und von dieser SVM übertragen werden.	Latenz	Durchschnittliche Anzahl von Millisekunden, die die SVM benötigt, um auf Applikationsanforderungen zu reagieren.

Speicherobjekt	Performance-Zähler	Beschreibung
Volumen	IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabeoperationen, die das Volume pro Sekunde verarbeitet.
MB/s	Durchschnittliche Anzahl an Megabyte Daten, die pro Sekunde zu und von diesem Volume übertragen werden.	Latenz
Durchschnittliche Anzahl der Millisekunden, die das Volume für die Beantwortung von Anforderungen der Applikation benötigt.	Cache-Miss-Verhältnis	Durchschnittlicher Prozentsatz der Leseanfragen von Client-Applikationen, die vom Volume statt aus dem Cache zurückgegeben werden.
LUN	IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabeoperationen, die die LUN pro Sekunde verarbeitet.
MB/s	Durchschnittliche Anzahl der Megabyte an Daten, die pro Sekunde zu und von dieser LUN übertragen werden.	Latenz
Durchschnittliche Anzahl an Millisekunden, die die LUN benötigt, um auf Anfragen der Applikation zu reagieren.	Namensraum	IOPS
Durchschnittliche Anzahl von Eingabe-/Ausgabeoperationen, die der Namespace pro Sekunde verarbeitet.	MB/s	Durchschnittliche Anzahl an Megabyte an Daten, die pro Sekunde zu diesem Namespace und von diesem Namespace übertragen werden.
Latenz	Durchschnittliche Anzahl der Millisekunden, die der Namespace benötigt, um auf Applikationsanforderungen zu reagieren.	Port
Bandbreitenauslastung	Durchschnittlicher Prozentsatz der verfügbaren Bandbreite des Ports, der genutzt wird.	MB/s
Durchschnittliche Anzahl der Megabyte an Daten, die pro Sekunde zu und von diesem Port übertragen werden.	Netzwerkschnittstelle (LIF)	MB/s

Kombinationsschwellenwertrichtlinienobjekte und Zähler in Active IQ Unified Manager verstehen

Nur bestimmte Performance Zähler können zusammen in Kombinationsrichtlinien verwendet werden. Wenn primäre und sekundäre Performance Zähler angegeben sind,

müssen beide Performance Zähler ihre Maximalwerte überschreiten, bevor ein Ereignis generiert wird.

Primäres Storage-Objekt und Zähler	Sekundäres Storage Objekt und Zähler
Volume Latenz	Volume-IOPS
Volume MB/s	Auslastung des Aggregats
Genutzte Aggregat-Performance-Kapazität	Knotenauslastung
Genutzte Node Performance Kapazität	Ausgenutzte Knotenleistungskapazität - Übernahme
LUN Latenz	LUN-IOPS
LUN MB/s	Auslastung des Aggregats
Genutzte Aggregat-Performance-Kapazität	Knotenauslastung
Genutzte Node Performance Kapazität	Ausgenutzte Knotenleistungskapazität - Übernahme

Wenn eine Volume-Kombinationsrichtlinie auf ein FlexGroup Volume anstatt auf ein FlexVol Volume angewendet wird, können nur die Attribute „Volume IOPS“ und „Volume MB/s“ als sekundärer Zähler ausgewählt werden. Wenn die Schwellenwertrichtlinie eines der Knoten- oder Aggregatattribute enthält, wird die Richtlinie nicht auf das FlexGroup Volume angewendet, und Sie erhalten eine Fehlermeldung, in der dieser Fall beschrieben wird. Dies liegt daran, dass FlexGroup Volumes auf mehr als einem Knoten oder Aggregat vorhanden sein können.

In Active IQ Unified Manager können benutzerdefinierte Leistungsschwellenwertrichtlinien erstellt werden

Sie erstellen Performance-Schwellenwertrichtlinien für Storage-Objekte, sodass Benachrichtigungen gesendet werden, wenn ein Performance-Zähler einen bestimmten Wert überschreitet. Die Ereignisbenachrichtigung weist darauf hin, dass im Cluster ein Performanceproblem auftritt.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Sie erstellen Performance-Schwellenwertrichtlinien, indem Sie die Schwellenwerte auf der Seite „Performance-Schwellenwertrichtlinie erstellen“ eingeben. Sie können neue Richtlinien erstellen, indem Sie alle Richtlinienwerte auf dieser Seite definieren, oder eine Kopie einer vorhandenen Richtlinie erstellen und die Werte in der Kopie ändern (sogenanntes Klonen).

Gültige Schwellenwerte sind 0,001 bis 10.000.000 für Zahlen, 0,001-100 für Prozentsätze und 0,001-200 für Prozentsätze der verwendeten Performance-Kapazität.

Die aktuelle Version bietet Schwellenwerte, die Ereignisse auslösen, wenn ein Zählerwert den festgelegten Schwellenwert überschreitet. Es können keine Schwellenwerte festgelegt werden, die Ereignisse auslösen, wenn ein Zählerwert unter einen festgelegten Schwellenwert fällt.

Schritte

1. Im linken Navigationsbereich ist **Ereignisschwellenwerte** > **Performance** auszuwählen.

   Die Seite „Performance-Schwellenwerte“ wird angezeigt.

2. Die entsprechende Schaltfläche ist abhängig davon auszuwählen, ob eine neue Richtlinie erstellt oder eine ähnliche Richtlinie geklont und die geklonte Version geändert werden soll.

Zu…	Klicken…
Eine neue Richtlinie erstellen	**Erstellen**
Eine bestehende Richtlinie klonen	Eine vorhandene Richtlinie auswählen und auf **Clone** klicken

   Die Seite „Performance-Schwellenwertrichtlinie erstellen“ oder die Seite „Performance-Schwellenwertrichtlinie klonen“ wird angezeigt.

3. Die Schwellenwertrichtlinie wird durch Angabe der Schwellenwerte für Performance-Zähler definiert, die für bestimmte Storage Objekte festgelegt werden sollen:

   a. Auszuwählen sind der Storage Objekttyp sowie ein Name und eine Beschreibung für die Richtlinie.

   b. Es werden der zu überwachende Performance-Zähler und die Grenzwerte festgelegt, die Warn- und kritische Ereignisse definieren.

      Sie müssen mindestens einen Warn- oder einen kritischen Grenzwert definieren. Es ist nicht erforderlich, beide Grenzwerttypen zu definieren.

   c. Falls erforderlich, erfolgt die Auswahl eines sekundären Performance-Zählers sowie die Festlegung der Grenzwerte für Warn- und kritische Ereignisse.

      Die Einbeziehung eines sekundären Zählers erfordert, dass beide Zähler die Grenzwerte überschreiten, bevor der Schwellenwert überschritten und ein Ereignis gemeldet wird. Nur bestimmte Objekte und Zähler können mithilfe einer Kombinationsrichtlinie konfiguriert werden.

   d. Hier wird die Zeitspanne festgelegt, in der die Grenzwerte überschritten werden müssen, damit ein Ereignis gesendet wird.

   Beim Klonen einer bestehenden Richtlinie müssen Sie einen neuen Namen für die Richtlinie eingeben.

4. Mit **Speichern** speichern Sie die Richtlinie.

   Sie werden zur Seite „Performance Thresholds“ zurückgeleitet. Eine Erfolgsmeldung oben auf der Seite bestätigt, dass die Schwellenwertrichtlinie erstellt wurde, und stellt einen Link zur Seite „Inventory“ für diesen Objekttyp bereit, sodass die neue Richtlinie sofort auf Storage-Objekte angewendet werden kann.

Wenn Sie die neue Schwellenwertrichtlinie jetzt auf Storage-Objekte anwenden möchten, können Sie auf den Link **Go to object_type now** klicken, um zur Inventarseite zu gelangen.

Zuweisung von Performance-Schwellenwertrichtlinien zu Speicherobjekten in Active IQ Unified Manager

Sie weisen einem Storage Objekt eine benutzerdefinierte Performance-Schwellenwertrichtlinie zu, sodass Unified Manager ein Ereignis meldet, wenn der Wert des Performance-Zählers die Richtlinieneinstellung überschreitet.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Die Performance-Schwellenwertrichtlinie bzw. -richtlinien, die auf das Objekt angewendet werden sollen,

müssen vorhanden sein.

Sie können jeweils nur eine Performance-Richtlinie gleichzeitig auf ein Objekt oder eine Gruppe von Objekten anwenden.

Jedem Storage Objekt können maximal drei Schwellenwertrichtlinien zugewiesen werden. Beim Zuweisen von Richtlinien zu mehreren Objekten führt Unified Manager die folgenden Aktionen aus, wenn einem der Objekte bereits die maximale Anzahl an Richtlinien zugewiesen ist:

- Anwendung der Richtlinie auf alle ausgewählten Objekte, die ihr Maximum noch nicht erreicht haben
- Objekte, die die maximale Anzahl von Richtlinien erreicht haben, bleiben unberücksichtigt
- Es wird eine Meldung angezeigt, dass die Richtlinie nicht allen Objekten zugewiesen wurde

Schritte

1. Auf der Seite „Performance-Inventar“ eines beliebigen Storage-Objekts erfolgt die Auswahl des Objekts oder der Objekte, denen eine Schwellenwertrichtlinie zugewiesen werden soll:

Um Schwellenwerte zuzuweisen…	**Klicken…**
Ein einzelnes Objekt	Das Kästchen links von diesem Objekt.
Mehrere Objekte	Das Kästchen links neben jedem Objekt.
Alle Objekte auf der Seite	im ☐ Dropdown-Menü die Option **Alle Objekte auf dieser Seite auswählen** auswählen.
Alle Objekte desselben Typs	Im ☐ Dropdown-Menü wird **Alle Objekte auswählen** gewählt.

   Mithilfe der Sortier- und Filterfunktionen können Sie die Liste der Objekte auf der Inventarseite verfeinern, um die Anwendung von Schwellenwertrichtlinien auf viele Objekte zu vereinfachen.

2. Nach der Auswahl erfolgt der Klick auf **Assign Performance Threshold Policy**.

   Die Seite „Performance-Schwellenwertrichtlinie zuweisen“ wird angezeigt und zeigt eine Liste der Schwellenwertrichtlinien an, die für diesen spezifischen Storage-Objekttyp vorhanden sind.

3. Bei Auswahl jeder Richtlinie werden die Details der Einstellungen für Performance-Schwellenwerte angezeigt, sodass überprüft werden kann, ob die richtige Schwellenwertrichtlinie ausgewählt wurde.
4. Nachdem Sie die passende Schwellenwertrichtlinie ausgewählt haben, wählen Sie **Assign Policy** aus.

   Eine Erfolgsmeldung am oberen Seitenrand bestätigt, dass die Schwellenwertrichtlinie dem Objekt oder den Objekten zugewiesen wurde, und bietet einen Link zur Alarmierungsseite, damit Sie die Alarmeinstellungen für dieses Objekt und diese Richtlinie konfigurieren können.

Wenn Sie Warnmeldungen per E-Mail oder als SNMP-Trap erhalten möchten, die Sie darüber informieren, dass ein bestimmtes Performance Ereignis erzeugt wurde, müssen Sie die Warnmeldungseinstellungen auf der Seite „Alert Setup“ konfigurieren.

Leistungsschwellenwertrichtlinien in Active IQ Unified Manager anzeigen

Auf der Seite „Leistungsschwellenwerte“ können Sie alle derzeit definierten Performance-Schwellenwertrichtlinien anzeigen.

Die Liste der Schwellenwertrichtlinien ist alphabetisch nach Richtliniennamen sortiert und umfasst Richtlinien für alle Arten von Storage-Objekten. Sie können auf eine Spaltenüberschrift klicken, um die Richtlinien nach dieser Spalte zu sortieren. Falls eine bestimmte Richtlinie gesucht wird, lassen sich mit den Filter- und Suchfunktionen die in der Inventarliste angezeigten Schwellenwertrichtlinien eingrenzen.

Durch Bewegen des Mauszeigers über den Richtliniennamen und den Bedingungsnamen werden die Konfigurationsdetails der Richtlinie angezeigt. Zusätzlich können Sie mithilfe der bereitgestellten Schaltflächen benutzerdefinierte Schwellenwertrichtlinien erstellen, klonen, bearbeiten und löschen.

Schritt

1. Im linken Navigationsbereich ist **Ereignisschwellenwerte** > **Performance** auszuwählen.

   Die Seite „Performance-Schwellenwerte“ wird angezeigt.

Das Bearbeiten benutzerdefinierter Leistungsschwellenwertrichtlinien in Active IQ Unified Manager

Die Schwellenwerteinstellungen für vorhandene Performance-Schwellenwertrichtlinien können bearbeitet werden. Dies kann hilfreich sein, wenn Sie feststellen, dass Sie für bestimmte Schwellenwertbedingungen zu viele oder zu wenige Benachrichtigungen erhalten.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Bei vorhandenen Schwellenwertrichtlinien können Sie weder den Richtliniennamen noch den Typ des überwachten Storage-Objekts ändern.

Schritte

1. Im linken Navigationsbereich ist **Ereignisschwellenwerte** > **Performance** auszuwählen.

   Die Seite „Performance-Schwellenwerte“ wird angezeigt.

2. Sie wählen die Schwellenwertrichtlinie aus, die Sie ändern möchten, und klicken auf **Bearbeiten**.

   Die Seite „Performance Schwellenwertrichtlinie bearbeiten“ wird angezeigt.

3. Nach dem Vornehmen von Änderungen an der Schwellenwertrichtlinie auf **Speichern** klicken.

   Sie kehren zur Seite „Performance-Schwellenwerte“ zurück.

Nach dem Speichern werden Änderungen sofort auf allen Storage Objekten aktualisiert, die die Richtlinie verwenden.

Je nach Art der Änderungen, die Sie an der Richtlinie vorgenommen haben, kann es sinnvoll sein, die für die Objekte konfigurierten Alarmeinstellungen zu überprüfen, die die Richtlinie auf der Seite „Alert Setup“ verwenden.

Entfernen von Leistungsschwellenwertrichtlinien von Speicherobjekten in Active IQ Unified Manager

Sie können eine benutzerdefinierte Performance-Schwellenwertrichtlinie von einem

Storage Objekt entfernen, wenn Unified Manager den Wert des Performance-Zählers nicht mehr überwachen soll.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Sie können jeweils nur eine Richtlinie aus einem ausgewählten Objekt entfernen.

Sie können eine Schwellenwertrichtlinie aus mehreren Storage Objekten entfernen, indem Sie in der Liste mehr als ein Objekt auswählen.

Schritte

1. Auf der Seite **Inventar** eines beliebigen Storage-Objekts lassen sich ein oder mehrere Objekte auswählen, auf die mindestens eine Performance-Schwellenwertrichtlinie angewendet wurde.

Zum Löschen von Schwellenwerten aus…	Folgendes ist zu tun…
Ein einzelnes Objekt	Das Kästchen links neben diesem Objekt wird ausgewählt.
Mehrere Objekte	Das Kästchen links neben jedem Objekt auswählen.
Alle Objekte auf der Seite	Die Auswahl von  erfolgt in der Spaltenüberschrift.

2. Dann erfolgt die Auswahl von **Clear Performance Threshold Policy**.

   Auf der Seite „Schwellenwertrichtlinie löschen“ erscheint eine Liste der Schwellenwertrichtlinien, die den Storage-Objekten aktuell zugewiesen sind.

3. Die Schwellenwertrichtlinie, die aus den Objekten entfernt werden soll, auswählen und auf **Richtlinie löschen** klicken.

   Wenn Sie eine Schwellenwertrichtlinie auswählen, erscheinen die Details der Richtlinie, sodass Sie bestätigen können, dass Sie die richtige Richtlinie ausgewählt haben.

Änderungen an Leistungsschwellenwertrichtlinien in Active IQ Unified Manager verstehen

Wenn Sie den Zählerwert oder die Dauer einer bestehenden Performance-Schwellenwertrichtlinie anpassen, wird die Richtlinienänderung auf alle Storage-Objekte angewendet, die diese Richtlinie verwenden. Die neue Einstellung wird sofort wirksam, und Unified Manager beginnt, die Performance-Zählerwerte für alle neu erfassten Performance-Daten mit den neuen Schwellenwerteinstellungen zu vergleichen.

Falls für Objekte, die die geänderte Schwellenwertrichtlinie verwenden, noch aktive Ereignisse vorhanden sind, werden diese Ereignisse als veraltet markiert, und die Schwellenwertrichtlinie beginnt, den Zähler als neu definierte Schwellenwertrichtlinie zu überwachen.

Bei der Anzeige des Zählers, auf den der Schwellenwert angewendet wurde, in der Detailansicht der Zählerdiagramme spiegeln die Linien für kritische Schwellenwerte und Warnschwellenwerte die aktuellen Schwellenwerteinstellungen wider. Die ursprünglichen Schwellenwerteinstellungen werden auf dieser Seite nicht angezeigt, selbst wenn Sie historische Daten anzeigen, als die alte Schwellenwerteinstellung noch gültig war.

Da ältere Schwellenwerteinstellungen in der Detailansicht der Zählerdiagramme nicht angezeigt werden, sehen Sie möglicherweise historische Ereignisse, die unterhalb der aktuellen Schwellenwertlinien liegen.

Verwalten von Schwellenwertrichtlinien beim Verschieben von Objekten in Active IQ Unified Manager

Da Performance-Schwellenwertrichtlinien Storage Objekten zugewiesen werden, bleiben alle zugewiesenen Schwellenwertrichtlinien auch nach Abschluss der Verschiebung eines Objekts mit dem Objekt verknüpft. Wenn beispielsweise ein Volume oder eine LUN in ein anderes Aggregat verschoben wird, bleiben die Schwellenwertrichtlinien für das Volume oder die LUN auf dem neuen Aggregat weiterhin aktiv.

Wenn für die Schwellenwertrichtlinie eine sekundäre Zählerbedingung vorhanden ist (eine Kombinationsrichtlinie), zum Beispiel wenn einem Aggregat oder einem Knoten eine zusätzliche Bedingung zugewiesen ist, gilt die sekundäre Zählerbedingung für das neue Aggregat oder den neuen Knoten, zu dem das Volume oder die LUN verschoben wurde.

Wenn für Objekte, die die geänderte Schwellenwertrichtlinie verwenden, neue aktive Ereignisse vorhanden sind, markiert das System diese Ereignisse als veraltet, und die Schwellenwertrichtlinie überwacht den Zähler anschließend als neu definierte Schwellenwertrichtlinie.

Ein Verschiebungsvorgang für ein Volume veranlasst ONTAP, ein informatives Änderungsereignis zu senden. Ein Symbol für ein Änderungsereignis wird in der Ereigniszeitleiste auf der Seite „Performance Explorer“ und der Seite „Workload Analysis“ angezeigt, um den Zeitpunkt anzugeben, zu dem der Verschiebungsvorgang abgeschlossen wurde.

Wenn Sie ein Objekt in einen anderen Cluster verschieben, wird die benutzerdefinierte Schwellenwertrichtlinie vom Objekt entfernt. Falls erforderlich, sollten Sie dem Objekt nach Abschluss des Verschiebungsvorgangs eine Schwellenwertrichtlinie zuweisen. Dynamische und systemdefinierte Schwellenwertrichtlinien werden jedoch automatisch auf ein Objekt angewendet, nachdem es in einen neuen Cluster verschoben wurde.

Funktionalität der Schwellenwertrichtlinie während der HA-Übernahme und -Rückgabe

Bei einer Übernahme oder Rückgabe in einer Hochverfügbarkeitskonfiguration (HA) behalten Objekte, die von einem Knoten auf den anderen Knoten verschoben werden, ihre Schwellenwertrichtlinien ebenso wie bei manuellen Verschiebungsvorgängen bei. Da Unified Manager alle 15 Minuten auf Änderungen der Clusterkonfiguration prüft, wird die Auswirkung der Umschaltung auf den neuen Knoten erst bei der nächsten Abfrage der Clusterkonfiguration erkannt.

Wenn sowohl eine Übernahme- als auch eine Rückgabeoperation innerhalb des 15-minütigen Erfassungszeitraums für Konfigurationsänderungen auftreten, werden die Performance-Statistiken möglicherweise nicht von einem Knoten auf den anderen Knoten verschoben.

Funktionalität der Schwellenwertrichtlinie während der Aggregatverschiebung

Wenn Sie ein Aggregat mithilfe des `aggregate relocation start` Befehls von einem Knoten auf einen anderen Knoten verschieben, bleiben sowohl Einzel- als auch Kombinationsschwellenwertrichtlinien für alle Objekte erhalten, und der Knotenanteil der Schwellenwertrichtlinie gilt für den neuen Knoten.

Funktionalität der Schwellenwertrichtlinie während der MetroCluster Umschaltung

Objekte, die innerhalb einer MetroCluster Konfiguration von einem Cluster in einen anderen verschoben werden, behalten ihre benutzerdefinierten Schwellenwertrichtlinieneinstellungen nicht bei. Bei Bedarf lassen sich Schwellenwertrichtlinien auf die Volumes und LUNs anwenden, die in den Partnercluster verschoben wurden. Nachdem ein Objekt in seinen ursprünglichen Cluster zurückverschoben wurde, gilt die benutzerdefinierte Schwellenwertrichtlinie automatisch wieder.

Informationen finden sich unter "Volume-Verhalten bei Switchover und Switchback".

Analyse von Performance Ereignissen

Analyse von Leistungsereignissen in Active IQ Unified Manager

Sie können Performance-Ereignisse analysieren, um festzustellen, wann sie erkannt wurden, ob sie aktiv (neu oder bestätigt) oder veraltet sind, welche Workloads und Clusterkomponenten beteiligt sind und welche Möglichkeiten zur eigenständigen Behebung der Ereignisse bestehen.

Informationen zu Leistungsereignissen in Active IQ Unified Manager anzeigen

Auf der Inventarseite der Ereignisverwaltung können Sie eine Liste aller Performance Ereignisse auf den von Unified Manager überwachten Clustern anzeigen. Anhand dieser Informationen können Sie die wichtigsten Ereignisse ermitteln und anschließend detaillierte Informationen abrufen, um die Ursache des jeweiligen Ereignisses zu bestimmen.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Die Ereignisliste ist nach Erkennungszeitpunkt sortiert, wobei die neuesten Ereignisse zuerst angezeigt werden. Sie können auf eine Spaltenüberschrift klicken, um die Ereignisse nach dieser Spalte zu sortieren. Beispielsweise können Sie nach der Spalte Status sortieren, um Ereignisse nach Schweregrad anzuzeigen. Wenn Sie nach einem bestimmten Ereignis oder einem bestimmten Ereignistyp suchen, können Sie die Filter- und Suchfunktionen verwenden, um die angezeigte Ereignisliste einzugrenzen.

Auf dieser Seite werden Ereignisse aus allen Quellen angezeigt:

- Benutzerdefinierte Performance-Schwellenwertrichtlinie
- Systemdefinierte Performance-Schwellenwertrichtlinie
- Dynamischer Performance-Schwellenwert

Die Spalte „Ereignistyp“ listet die Quelle des Ereignisses auf. Sie können ein Ereignis auswählen, um Details dazu auf der Seite „Ereignisdetails“ anzuzeigen.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.
2. Im Menü „View“ ist **Active performance events** auszuwählen.

   Auf dieser Seite werden alle neuen und bestätigten Performance-Ereignisse angezeigt, die in den letzten 7

Tagen generiert wurden.

3. Wenn Sie das zu analysierende Ereignis gefunden haben, können Sie auf den Ereignisnamen klicken.

   Die Detailseite für das Ereignis wird angezeigt.

   Sie können die Detailseite eines Ereignisses auch anzeigen, indem Sie auf der Seite „Performance Explorer“ oder in einer Benachrichtigungs-E-Mail auf den Link mit dem Ereignisnamen klicken.

Analyse von Ereignissen anhand benutzerdefinierter Performance-Schwellenwerte

Analyse von Ereignissen anhand benutzerdefinierter Leistungsschwellenwerte in Active IQ Unified Manager

Ereignisse, die durch benutzerdefinierte Schwellenwerte generiert werden, zeigen an, dass ein Performance-Zähler für ein bestimmtes Storage-Objekt, beispielsweise ein Aggregat oder Volume, den in der Richtlinie definierten Schwellenwert überschritten hat. Dies weist darauf hin, dass bei dem Cluster-Objekt ein Performance-Problem vorliegt.

Die Seite mit den Ereignisdetails dient zur Analyse des Performance-Ereignisses und gegebenenfalls zur Ergreifung einer Korrekturmaßnahme, um die Performance wieder auf den Normalzustand zurückzuführen.

Reaktion auf benutzerdefinierte Leistungsschwellenwertereignisse in Active IQ Unified Manager

Mit Unified Manager können Sie Performance-Ereignisse untersuchen, die dadurch verursacht wurden, dass ein Performance-Zähler einen benutzerdefinierten Warn- oder kritischen Schwellenwert überschritten hat. Außerdem können Sie mit Unified Manager den Systemstatus der Clusterkomponente prüfen, um festzustellen, ob kürzlich auf der Komponente erkannte Systemstatusereignisse zu dem Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es muss neue oder veraltete Performance-Ereignisse geben.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. In der **Beschreibung** wird die Schwellenwertüberschreitung beschrieben, die das Ereignis verursacht hat.

   Beispielsweise zeigt die Meldung „`Der Latenzwert von 456 ms/op hat auf Grundlage des Schwellenwerts von 400 ms/op ein WARNING-Ereignis ausgelöst`“ an, dass für das Objekt ein Latenzwarnereignis aufgetreten ist.

3. Beim Bewegen des Mauszeigers über den Richtliniennamen erscheinen Details zur Schwellenwertrichtlinie, die das Ereignis ausgelöst hat.

   Dies umfasst den Namen der Richtlinie, den zu bewertenden Performance Zähler, den Wert des Zählers, der überschritten werden muss, damit dies als kritisches Ereignis oder Warnereignis gilt, und die Dauer, für die der Zähler den Wert überschreiten muss.

4. Es empfiehlt sich, den **Auslösezeitpunkt des Ereignisses** zu notieren, damit untersucht werden kann, ob gleichzeitig andere Ereignisse aufgetreten sind, die zu diesem Ereignis beigetragen haben könnten.
5. Für die weitere Untersuchung des Ereignisses und zur Feststellung, ob Maßnahmen zur Behebung des Performanceproblems erforderlich sind, steht eine der folgenden Optionen zur Verfügung:

Option	Mögliche Untersuchungsmaßnahmen
Wenn Sie auf den Namen des Quellobjekts klicken, wird die Explorer-Seite für dieses Objekt angezeigt.	Auf dieser Seite können Sie die Objektdetails anzeigen und dieses Objekt mit anderen ähnlichen Storage Objekten vergleichen, um festzustellen, ob bei anderen Storage Objekten etwa zur gleichen Zeit ein Performance Problem auftritt. So lässt sich beispielsweise feststellen, ob auch andere Volumes im selben Aggregat ein Performance Problem haben.
Wenn Sie den Clusternamen auswählen, wird die Seite mit der Clusterübersicht angezeigt.	Auf dieser Seite lassen sich die Details des Clusters anzeigen, auf dem sich dieses Objekt befindet, um festzustellen, ob ungefähr zur gleichen Zeit andere Probleme mit der Performance aufgetreten sind.

Analyse von Ereignissen anhand systemdefinierter Performance-Schwellenwerte

Analyse von Ereignissen aus systemdefinierten Leistungsschwellenwerten in Active IQ Unified Manager

Ereignisse, die durch systemdefinierte Performance Schwellenwerte generiert werden, zeigen an, dass ein Performance-Zähler oder eine Gruppe von Performance-Zählern für ein bestimmtes Storage Objekt den Schwellenwert aus einer systemdefinierten Richtlinie überschritten hat. Dies weist darauf hin, dass bei dem Storage Objekt, beispielsweise einem Aggregat oder Knoten, ein Performance-Problem vorliegt.

Die Seite mit den Ereignisdetails dient zur Analyse des Performance-Ereignisses und gegebenenfalls zur Ergreifung einer Korrekturmaßnahme, um die Performance wieder auf den Normalzustand zurückzuführen.

Systemdefinierte Schwellenwertrichtlinien sind auf Cloud Volumes ONTAP, ONTAP Edge oder ONTAP Select Systemen nicht aktiviert.

Reaktion auf systemdefinierte Leistungsschwellenereignisse in Active IQ Unified Manager

Mit Unified Manager können Sie Performance Ereignisse untersuchen, die dadurch verursacht wurden, dass ein Performance Zähler einen systemdefinierten Warnschwellenwert überschritten hat. Sie können Unified Manager auch verwenden, um den Systemstatus der Clusterkomponente zu prüfen und festzustellen, ob kürzlich auf der Komponente erkannte Ereignisse zu dem Performance Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es muss neue oder veraltete Performance-Ereignisse geben.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. In der **Beschreibung** wird die Schwellenwertüberschreitung beschrieben, die das Ereignis verursacht hat.

   Beispielsweise zeigt die Meldung „`Node utilization value of 90 % has triggered a WARNING event based on threshold setting of 85 %`“ an, dass für das Clusterobjekt ein Warnereignis zur Knotenauslastung aufgetreten ist.

3. Es empfiehlt sich, den **Auslösezeitpunkt des Ereignisses** zu notieren, damit untersucht werden kann, ob gleichzeitig andere Ereignisse aufgetreten sind, die zu diesem Ereignis beigetragen haben könnten.
4. Unter **Systemdiagnose** ist eine kurze Beschreibung der Art der Analyse angegeben, die die systemdefinierte Richtlinie für das Clusterobjekt durchführt.

   Bei manchen Ereignissen wird neben der Diagnose ein grünes oder rotes Symbol angezeigt, das angibt, ob in dieser Diagnose ein Problem festgestellt wurde. Bei anderen Arten von systemdefinierten Ereignissen zeigen Zählerdiagramme die Performance des Objekts an.

5. Unter **Vorgeschlagene Aktionen** lässt sich über den Link **Help me do this** anzeigen, welche vorgeschlagenen Aktionen Sie ausführen können, um zu versuchen, das Performance-Ereignis selbst zu beheben.

Reaktion auf Leistungsereignisse von QoS-Richtliniengruppen in Active IQ Unified Manager

Unified Manager generiert QoS-Richtlinienwarnereignisse, wenn der Workload-Durchsatz (IOPS, IOPS/TB oder MB/s) die definierte ONTAP QoS Richtlinieneinstellung überschritten hat und sich dies auf die Workload-Latenz auszuwirken beginnt. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Performance Probleme zu beheben, bevor viele Workloads von Latenz betroffen sind.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es muss neue, bestätigte oder veraltete Performance-Ereignisse geben.

Unified Manager generiert Warnereignisse bei Verstößen gegen die QoS-Richtlinie, wenn der Workload-Durchsatz während jedes Performance-Erfassungszeitraums der vergangenen Stunde die definierte QoS-Richtlinieneinstellung überschritten hat. Der Workload-Durchsatz kann den QoS-Schwellenwert während jedes Erfassungszeitraums nur kurzzeitig überschreiten, Unified Manager zeigt im Diagramm jedoch während des Erfassungszeitraums nur den “average”-Durchsatz an. Aus diesem Grund können QoS-Ereignisse auftreten, obwohl der Durchsatz eines Workloads den im Diagramm angezeigten Richtlinienschwellenwert möglicherweise nicht überschritten hat.

Sie können System Manager oder die ONTAP Befehle verwenden, um Richtliniengruppen zu managen, einschließlich der folgenden Aufgaben:

- Erstellen einer neuen Richtliniengruppe für die Workload
- Hinzufügen oder Entfernen von Workloads in einer Richtliniengruppe
- Verschieben einer Workload zwischen Richtliniengruppen
- Ändern der Durchsatzbegrenzung einer Richtliniengruppe
- Verschieben eines Workloads auf ein anderes Aggregat oder einen anderen Knoten

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. In der **Beschreibung** wird die Schwellenwertüberschreitung beschrieben, die das Ereignis verursacht hat.

   Beispielsweise zeigt die Meldung „`IOPS-Wert von 1.352 IOPS auf vol1_NFS1 hat ein WARNING-Ereignis ausgelöst, um potenzielle Performance-Probleme für die Workload zu identifizieren`“ an, dass ein QoS Max IOPS-Ereignis auf dem Volume vol1_NFS1 aufgetreten ist.

3. Der Abschnitt **Ereignisinformationen** enthält weitere Details dazu, wann das Ereignis aufgetreten ist und wie lange es bereits aktiv ist.

   Zusätzlich können Sie für Volumes oder LUNs, die sich den Durchsatz einer QoS-Richtlinie teilen, die Namen der drei Workloads sehen, die die meisten IOPS oder MBps verbrauchen.

4. Im Abschnitt **Systemdiagnose** werden zwei Diagramme angezeigt: eines für die durchschnittlichen Gesamt-IOPS oder MBps (je nach Ereignis) und eines für die Latenz. In dieser Anordnung ist erkennbar, welche Clusterkomponenten die Latenz am stärksten beeinflussen, wenn sich die Workload der maximalen QoS-Grenze nähert.

   Bei einem Event für eine gemeinsam genutzte QoS-Richtlinie werden die drei Workloads mit dem höchsten Durchsatz im Durchsatzdiagramm angezeigt. Wenn mehr als drei Workloads die QoS-Richtlinie gemeinsam nutzen, werden zusätzliche Workloads in einer Kategorie “Other workloads” zusammengefasst. Zusätzlich zeigt das Latenzdiagramm die durchschnittliche Latenz für alle Workloads, die Teil der QoS-Richtlinie sind.

   Zu beachten ist, dass bei adaptiven QoS-Richtlinienereignissen die IOPS- und MBps-Diagramme IOPS- oder MBps-Werte anzeigen, die ONTAP basierend auf der Größe des Volumes aus der zugewiesenen IOPS/TB-Schwellenwertrichtlinie umgerechnet hat.

5. Im Abschnitt **Empfohlene Maßnahmen** geht es darum, die Vorschläge zu prüfen und festzustellen, welche Maßnahmen zu ergreifen sind, um eine Erhöhung der Latenz für den Workload zu vermeiden.

   Falls erforderlich, zeigt ein Klick auf die Schaltfläche **Help** weitere Details zu den vorgeschlagenen Maßnahmen an, mit denen sich das Performance-Ereignis möglicherweise beheben lässt.

Adaptive QoS-Ereignisse mit einer definierten Blockgröße in Active IQ Unified Manager verstehen

Adaptive QoS Richtliniengruppen skalieren automatisch eine maximale oder minimale Durchsatzgrenze basierend auf der Volume-Größe und halten dabei das Verhältnis von IOPS zu TB aufrecht, wenn sich die Größe des Volume ändert. Ab ONTAP 9.5 lässt sich die Blockgröße in der QoS Richtlinie angeben, um gleichzeitig effektiv einen MB/s-Schwellenwert anzuwenden.

Die Zuweisung eines IOPS-Schwellenwerts in einer adaptiven QoS-Richtlinie begrenzt lediglich die Anzahl der Operationen pro Arbeitslast. Abhängig von der auf dem Client, der die Arbeitslasten generiert, festgelegten Blockgröße umfassen manche IOPS deutlich mehr Daten und belasten daher die Knoten, die die Operationen verarbeiten, wesentlich stärker.

Der MB/s-Wert für eine Workload wird anhand der folgenden Formel berechnet:

```
MB/s = (IOPS * Block Size) / 1000
```

Wenn eine Workload im Durchschnitt 3.000 IOPS aufweist und die Blockgröße auf dem Client auf 32 KB festgelegt ist, beträgt der effektive MB/s-Wert für diese Workload 96. Wenn dieselbe Workload im Durchschnitt 3.000 IOPS aufweist und die Blockgröße auf dem Client auf 48 KB festgelegt ist, beträgt der effektive MB/s-Wert für diese Workload 144. Sie sehen, dass der Node bei einer größeren Blockgröße 50 % mehr Daten verarbeitet.

Im Folgenden geht es um die folgende adaptive QoS-Richtlinie mit definierter Blockgröße und darum, wie Ereignisse auf Grundlage der auf dem Client festgelegten Blockgröße ausgelöst werden.

Erforderlich ist eine Richtlinie, bei der der Spitzendurchsatz auf 2.500 IOPS/TB und die Blockgröße auf 32 KB festgelegt ist. Dadurch wird der MB/s-Schwellenwert für ein Volume mit 1 TB belegter Kapazität effektiv auf 80 MB/s ((2.500 IOPS * 32 KB) / 1.000) festgelegt. Beachten Sie, dass Unified Manager ein Warnungsereignis generiert, wenn der Durchsatzwert 10 % unter dem definierten Schwellenwert liegt. Ereignisse werden in den folgenden Situationen generiert:

Verwendete Kapazität	**Ein Ereignis wird ausgelöst, wenn der Durchsatz diesen Wert überschreitet …**	
	IOPS	MB/s
1 TB	2.250 IOPS	72 MB/s
2 TB	4.500 IOPS	144 MB/s
5 TB	11.250 IOPS	360 MB/s

Wenn das Volume 2 TB des verfügbaren Speicherplatzes belegt, die IOPS 4.000 beträgt und die QoS-Blockgröße auf dem Client auf 32 KB eingestellt ist, ergibt sich ein Durchsatz von 128 MB/s ((4.000 IOPS * 32 KB) / 1.000). In diesem Szenario wird kein Ereignis generiert, da sowohl 4.000 IOPS als auch 128 MB/s unter dem Schwellenwert für ein Volume liegen, das 2 TB Speicherplatz belegt.

Wenn das Volume 2TB des verfügbaren Speicherplatzes nutzt, die IOPS 4,000 betragen und die QoS-Blockgröße auf dem Client auf 64KB festgelegt ist, beträgt der MB/s-Durchsatz 256 MB/s ((4,000 IOPS * 64 KB) / 1000). In diesem Fall erzeugen die 4,000 IOPS kein Ereignis, der MB/s-Wert von 256 MB/s liegt jedoch über dem Schwellenwert von 144 MB/s, und es wird ein Ereignis generiert.

Aus diesem Grund wird, wenn ein Ereignis durch eine Überschreitung der MB/s-Grenze für eine adaptive QoS-Richtlinie ausgelöst wird, die die Blockgröße umfasst, im Abschnitt „Systemdiagnose“ auf der Seite mit den Ereignisdetails ein MB/s-Diagramm angezeigt. Wenn das Ereignis hingegen durch eine Überschreitung der IOPS-Grenze für die adaptive QoS-Richtlinie ausgelöst wird, wird im Abschnitt „Systemdiagnose“ ein IOPS-Diagramm angezeigt. Wenn sowohl bei IOPS als auch bei MB/s eine Überschreitung auftritt, erhalten Sie zwei Ereignisse.

Weitere Informationen zur Anpassung der QoS-Einstellungen finden Sie unter "Überblick über das Performance-Management".

Reaktion auf Ereignisse der Knotenressourcenüberlastung in Active IQ Unified Manager

Unified Manager generiert Warnereignisse zu überlasteten Knotenressourcen, wenn ein einzelner Knoten über die Grenzen seiner betrieblichen Effizienz hinaus arbeitet und dadurch potenziell die Latenzzeiten von Workloads beeinträchtigt. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Performance Probleme zu korrigieren, bevor viele Workloads von Latenzproblemen betroffen sind.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es muss neue oder veraltete Performance-Ereignisse geben.

Unified Manager generiert Warnereignisse für Richtlinienverstöße bei überlasteten Knotenressourcen, indem er Knoten identifiziert, die ihre Performancekapazität länger als 30 Minuten zu mehr als 100 % nutzen.

Sie können System Manager oder die ONTAP Befehle verwenden, um diese Art von Performanceproblem zu beheben; dazu gehören unter anderem die folgenden Aufgaben:

- Erstellung und Anwendung einer QoS-Richtlinie auf alle Volumes oder LUNs, die Systemressourcen übermäßig beanspruchen
- Reduzierung der maximalen QoS Durchsatzbegrenzung einer Richtliniengruppe mit zugewiesenen Workloads
- Verschieben eines Workloads auf ein anderes Aggregat oder einen anderen Knoten
- Erhöhen der Kapazität durch Hinzufügen von Festplatten zum Knoten oder durch ein Upgrade auf einen Knoten mit schnellerer CPU und mehr RAM

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. In der **Beschreibung** wird die Schwellenwertüberschreitung beschrieben, die das Ereignis verursacht hat.

   Beispielsweise weist die Meldung „`Perf. Capacity Used value of 139% on simplicity-02 has triggered a WARNING event to identify potential performance problems in the data processing unit.`“ darauf hin, dass die Performance-Kapazität auf Node simplicity-02 überlastet ist und die Node-Performance beeinträchtigt.

3. Im Abschnitt **Systemdiagnose** sind drei Diagramme zu sehen: eines zur auf dem Knoten genutzten Performance Kapazität, eines zu den durchschnittlichen Storage IOPS, die von den wichtigsten Workloads genutzt werden, und eines zur Latenz der wichtigsten Workloads. In dieser Anordnung wird ersichtlich, welche Workloads die Ursache für die Latenz auf dem Knoten sind.

   Sie können durch Bewegen des Cursors über das IOPS-Diagramm sehen, auf welche Workloads QoS-Richtlinien angewendet werden und auf welche nicht.

4. Im Abschnitt **Empfohlene Maßnahmen** geht es darum, die Vorschläge zu prüfen und festzustellen, welche Maßnahmen zu ergreifen sind, um eine Erhöhung der Latenz für den Workload zu vermeiden.

   Falls erforderlich, zeigt ein Klick auf die Schaltfläche **Help** weitere Details zu den vorgeschlagenen Maßnahmen an, mit denen sich das Performance-Ereignis möglicherweise beheben lässt.

Reaktion auf Leistungsereignisse im Zusammenhang mit Clusterungleichgewichten in Active IQ Unified Manager

Unified Manager generiert Warnereignisse bei Cluster-Ungleichgewicht, wenn ein Knoten in einem Cluster deutlich stärker ausgelastet ist als die anderen Knoten und dadurch potenziell die Latenzzeiten von Workloads beeinträchtigt. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Performance Probleme zu beheben, bevor viele Workloads von Latenzproblemen betroffen sind.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Unified Manager generiert Warnereignisse bei Verstößen gegen die Schwellenwertrichtlinie für Cluster-Ungleichgewichte, indem er den Wert der genutzten Performance-Kapazität aller Knoten im Cluster vergleicht, um festzustellen, ob zwischen einzelnen Knoten ein Lastunterschied von 30 % besteht.

Diese Schritte helfen Ihnen, die folgenden Ressourcen zu identifizieren, damit Sie leistungsstarke Workloads auf einen weniger ausgelasteten Knoten verschieben können:

- Die weniger ausgelasteten Knoten im selben Cluster
- Die am wenigsten ausgelasteten Aggregate auf dem neuen Knoten
- Die leistungsstärksten Volumes auf dem aktuellen Knoten

Schritte

1. Die Seite **Ereignisdetails** zeigt Informationen über das Ereignis an.
2. In der **Beschreibung** wird die Schwellenwertüberschreitung beschrieben, die das Ereignis verursacht hat.

   Beispielsweise weist die Meldung „`Der Zähler für die verwendete Performance Kapazität zeigt einen Lastunterschied von 62 % zwischen den Nodes im Cluster Dallas-1-8 an und hat auf Grundlage des Systemschwellenwerts von 30 % ein WARNING Ereignis ausgelöst`“ darauf hin, dass die Performance Kapazität auf einem der Nodes überbeansprucht wird und die Node Performance beeinträchtigt.

3. Der Text unter **Vorgeschlagene Maßnahmen** enthält Informationen zum Verschieben eines leistungsstarken Volume von dem Knoten mit dem hohen Wert für die genutzte Performance-Kapazität auf einen Knoten mit dem niedrigsten Wert für die genutzte Performance-Kapazität.
4. Die Knoten mit dem höchsten und niedrigsten Wert der genutzten Performance Kapazität:
   a. Im Abschnitt **Ereignisinformationen** ist der Name des Quell-Clusters auszuwählen.
   b. Auf der Seite **Cluster / Performance Summary** erfolgt die Auswahl von **Nodes** im Bereich **Managed Objects**.
   c. Auf der Inventarseite **Nodes** erfolgt die Sortierung der Knoten nach der Spalte **Performance Capacity Used**.
   d. Zu notieren sind die Namen der Knoten mit dem höchsten und dem niedrigsten Wert der genutzten Performance-Kapazität.
5. Das Volume mit den meisten IOPS auf dem Knoten mit dem höchsten Wert für die genutzte Performance-Kapazität:
   a. Der Knoten mit dem höchsten Wert für die genutzte Performance Kapazität.
   b. Auf der Seite **Node / Performance Explorer** erfolgt die Auswahl von **Aggregates on this Node** im Menü **View and Compare**.
   c. Das Aggregat mit dem höchsten Wert für die genutzte Performance-Kapazität auswählen.
   d. Auf der Seite **Aggregate / Performance Explorer** erfolgt die Auswahl von **Volumes on this Aggregate** im Menü **View and Compare**.
   e. Die Volumes werden nach der Spalte **IOPS** sortiert, und der Name des Volumes mit den meisten IOPS sowie der Name des Aggregats, in dem sich das Volume befindet, werden notiert.
6. Gesucht ist das Aggregat mit der geringsten Auslastung auf dem Knoten mit dem niedrigsten Wert für die genutzte Performance Kapazität:
   a. **Storage** > **Aggregates** zeigt die Inventarseite **Aggregates** an.
   b. Die Ansicht **Performance: All Aggregates** wird ausgewählt.

c. Anschließend erfolgt die Auswahl der Schaltfläche **Filter** sowie das Hinzufügen eines Filters, bei dem “Node” dem in Schritt 4 notierten Namen des Knotens mit dem niedrigsten Wert für die genutzte Performance Kapazität entspricht.

d. Der Name des Aggregats mit dem niedrigsten Wert für die genutzte Performance-Kapazität ist zu notieren.

7. Das Volume wird vom überlasteten Knoten auf das Aggregat verschoben, das auf dem neuen Knoten als gering ausgelastet identifiziert wurde.

   Sie können den Verschiebevorgang mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools durchführen.

Nach einigen Tagen ist erkennbar, ob von diesem Cluster erneut dasselbe Cluster-Ungleichgewichtsereignis eingeht.

Analyse von Ereignissen anhand dynamischer Performance-Schwellenwerte

Analyse von Ereignissen aus dynamischen Leistungsschwellenwerten in Active IQ Unified Manager

Ereignisse, die durch dynamische Schwellenwerte generiert werden, weisen darauf hin, dass die tatsächliche Antwortzeit (Latenz) einer Arbeitslast im Vergleich zum erwarteten Antwortzeitbereich zu hoch oder zu niedrig ist. Sie verwenden die Seite „Ereignisdetails“, um das Performance-Ereignis zu analysieren und bei Bedarf eine Korrekturmaßnahme zu ergreifen, damit die Performance wieder den Normalzustand erreicht.

Dynamische Performance-Schwellenwerte sind auf Cloud Volumes ONTAP, ONTAP Edge oder ONTAP Select Systemen nicht aktiviert.

Betroffene Workloads in dynamischen Performance-Ereignissen in Active IQ Unified Manager identifizieren

Im Unified Manager können Sie ermitteln, welche Volume-Workloads die größte Abweichung bei der Antwortzeit (Latenz) aufweisen, die durch eine Storage-Komponente in Contention verursacht wird. Die Identifizierung dieser Workloads hilft Ihnen zu verstehen, warum die darauf zugreifenden Clientanwendungen langsamer als üblich arbeiten.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es müssen neue, bestätigte oder veraltete dynamische Performance-Ereignisse vorliegen.

Die Seite mit den Ereignisdetails zeigt eine Liste der benutzerdefinierten und systemdefinierten Workloads an, sortiert nach der größten Abweichung bei Aktivität oder Nutzung auf der Komponente oder danach, wie stark sie vom Ereignis betroffen sind. Die Werte basieren auf den Spitzenwerten, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. In den Diagrammen „Workload-Latenz“ und „Workload-Aktivität“ erfolgt die Auswahl der Option **Victim Workloads**.

3. Wenn Sie den Mauszeiger über die Diagramme bewegen, sehen Sie die wichtigsten benutzerdefinierten Workloads, die sich auf die Komponente auswirken, sowie den Namen des betroffenen Workloads.

Identifizierung überlastender Workloads in dynamischen Performance-Ereignissen in Active IQ Unified Manager

Im Unified Manager können Sie ermitteln, welche Workloads für eine Clusterkomponente mit Ressourcenkonflikt die größte Nutzungsabweichung aufweisen. Die Identifizierung dieser Workloads hilft Ihnen zu verstehen, warum bestimmte Volumes im Cluster langsame Antwortzeiten (Latenz) aufweisen.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es müssen neue, bestätigte oder veraltete dynamische Performance-Ereignisse vorliegen.

Die Seite mit den Ereignisdetails zeigt eine Liste der benutzerdefinierten und systemdefinierten Workloads, sortiert nach der höchsten Auslastung der Komponente oder der größten Beeinträchtigung durch das Ereignis. Die Werte basieren auf den Spitzenwerten, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Auf der Seite „Ereignisdetails“ können Informationen über das Ereignis angezeigt werden.
2. In den Diagrammen „Workload-Latenz“ und „Workload-Aktivität“ erfolgt die Auswahl von **Bully Workloads**.
3. Wenn Sie den Mauszeiger über die Diagramme bewegen, werden die wichtigsten benutzerdefinierten Bully Workloads angezeigt, die sich auf die Komponente auswirken.

Shark-Workloads in einem dynamischen Performance-Ereignis in Active IQ Unified Manager identifizieren

Im Unified Manager können Sie die Workloads identifizieren, die bei einer Storage Komponente mit Ressourcenkonflikt die größte Nutzungsabweichung aufweisen. Die Identifizierung dieser Workloads hilft Ihnen bei der Entscheidung, ob diese Workloads in einen weniger ausgelasteten Cluster verschoben werden sollten.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es gibt neue, bestätigte oder veraltete dynamische Performance-Ereignisse.

Die Seite mit den Ereignisdetails zeigt eine Liste der benutzerdefinierten und systemdefinierten Workloads, sortiert nach der höchsten Auslastung der Komponente oder der größten Beeinträchtigung durch das Ereignis. Die Werte basieren auf den Spitzenwerten, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. In den Diagrammen „Workload-Latenz“ und „Workload-Aktivität“ können Sie **Shark Workloads** auswählen.
3. Wenn Sie den Mauszeiger über die Diagramme bewegen, werden die wichtigsten benutzerdefinierten Workloads angezeigt, die sich auf die Komponente auswirken, sowie der Name des Shark Workloads.

Performance Ereignisanalyse für eine MetroCluster Konfiguration

Analyse von MetroCluster Leistungsereignissen mit Active IQ Unified Manager

Mit Unified Manager können Sie ein Performance-Ereignis für eine MetroCluster Konfiguration analysieren. Sie können die an dem Ereignis beteiligten Workloads identifizieren und die vorgeschlagenen Maßnahmen zur Behebung des Problems überprüfen.

MetroCluster Performance Ereignisse können auf *bully* Workloads zurückzuführen sein, die die Interswitch-Verbindungen (ISLs) zwischen den Clustern übermäßig beanspruchen, oder auf Probleme mit dem Systemstatus der Verbindungen. Unified Manager überwacht jeden Cluster in einer MetroCluster Konfiguration unabhängig, ohne Performance Ereignisse auf einem Partnercluster zu berücksichtigen.

Performance Ereignisse beider Cluster in der MetroCluster Konfiguration werden ebenfalls auf der Unified Manager Dashboard Seite angezeigt. Außerdem können die Systemstatus-Seiten von Unified Manager angezeigt werden, um den Systemstatus der einzelnen Cluster zu überprüfen und deren Beziehung anzuzeigen.

Analyse eines MetroCluster Leistungsereignisses auf einem Cluster in Active IQ Unified Manager

Mit Unified Manager lässt sich der Cluster in einer MetroCluster Konfiguration analysieren, auf dem ein Performance Ereignis erkannt wurde. Dabei lassen sich der Cluster-Name, der Zeitpunkt der Ereigniserkennung sowie die beteiligten *bully* und *victim* Workloads identifizieren.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Für eine MetroCluster Konfiguration müssen neue, bestätigte oder veraltete Performance Ereignisse vorliegen.
- Beide Cluster in der MetroCluster Konfiguration müssen von derselben Instanz des Unified Manager überwacht werden.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. Die Ereignisbeschreibung enthält die Namen der beteiligten Workloads und deren Anzahl.

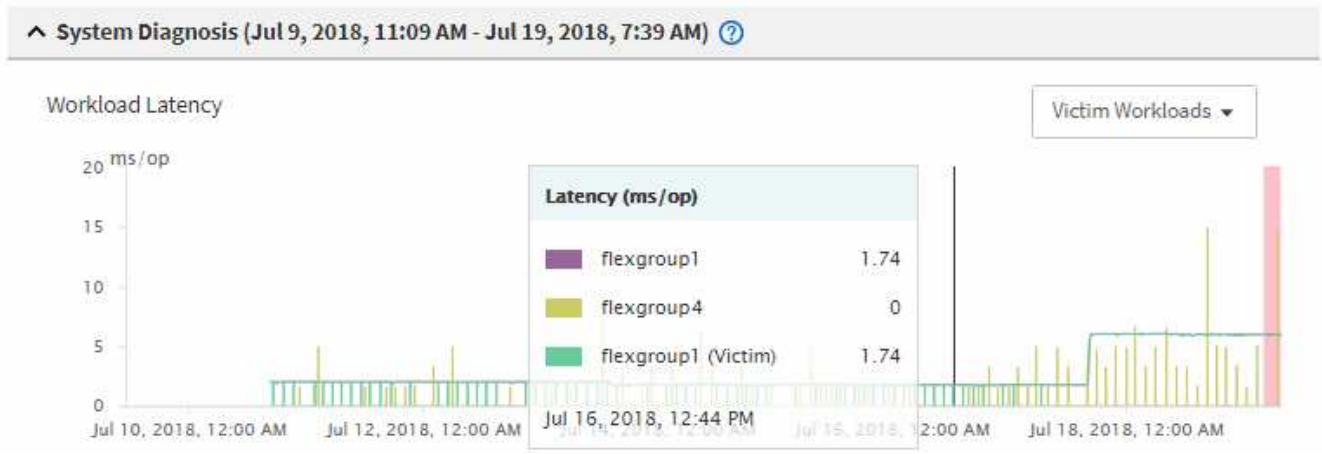
   In diesem Beispiel ist das Symbol MetroCluster Resources rot, was darauf hinweist, dass die MetroCluster Ressourcen umkämpft sind. Wenn sich der Mauszeiger über dem Symbol befindet, wird eine Beschreibung des Symbols angezeigt.



3. Der Clustername und der Zeitpunkt der Ereigniserkennung können zur Analyse von Performance Ereignissen auf dem Partnercluster verwendet werden.

4. In den Diagrammen ist zu prüfen, ob die Antwortzeiten der *victim*-Workloads über dem Performance-Schwellenwert liegen.

   In diesem Beispiel wird die betroffene Arbeitslast im Hover-Text angezeigt. Die Latenzdiagramme zeigen auf hoher Ebene ein konsistentes Latenzmuster für die betroffenen Arbeitslasten. Obwohl die anormale Latenz der betroffenen Arbeitslasten das Ereignis ausgelöst hat, könnte ein konsistentes Latenzmuster darauf hindeuten, dass die Arbeitslasten innerhalb ihres erwarteten Bereichs arbeiten, ein I/O-Spitzenwert jedoch die Latenz erhöht und das Ereignis ausgelöst hat.



   Wenn Sie kürzlich eine Applikation auf einem Client installiert haben, die auf diese Volume Workloads zugreift und diese Applikation eine hohe Anzahl von E/A-Operationen an sie sendet, ist möglicherweise mit einem Anstieg ihrer Latenzzeiten zu rechnen. Wenn die Latenz für die Workloads wieder in den erwarteten Bereich zurückkehrt, der Ereignisstatus in „veraltet“ wechselt und länger als 30 Minuten in diesem Status verbleibt, kann das Ereignis wahrscheinlich ignoriert werden. Wenn das Ereignis weiterhin besteht und im neuen Status verbleibt, kann es weiter untersucht werden, um festzustellen, ob andere Probleme das Ereignis verursacht haben.

5. Im Diagramm „Workload Throughput“ wird mit der Auswahl der Option **Bully Workloads** die Anzeige der Bully Workloads aktiviert.

   Das Vorhandensein von besonders ressourcenintensiven Workloads deutet darauf hin, dass das Ereignis möglicherweise durch einen oder mehrere Workloads im lokalen Cluster verursacht wurde, die die MetroCluster Ressourcen übermäßig beanspruchten. Diese Workloads weisen eine hohe Abweichung im Schreibdurchsatz (MB/s) auf.

   Dieses Diagramm zeigt auf hoher Ebene das Schreibdurchsatzmuster (MB/s) für die Workloads. Anhand des Schreibdurchsatzmusters in MB/s lassen sich ungewöhnliche Durchsatzraten erkennen, die darauf hindeuten können, dass ein Workload die MetroCluster Ressourcen übermäßig nutzt.

   Wenn keine rechenintensiven Workloads an dem Ereignis beteiligt sind, könnte die Ursache ein Systemstatusproblem mit der Verbindung zwischen den Clustern oder ein Performance Problem auf dem Partnercluster sein. Mit Unified Manager kann der Systemstatus beider Cluster in einer MetroCluster Konfiguration überprüft werden. Außerdem kann Unified Manager verwendet werden, um Performance Ereignisse auf dem Partnercluster zu prüfen und zu analysieren.

Analyse eines MetroCluster Leistungsereignisses auf einem Remote Cluster in Active IQ Unified Manager

Mit Unified Manager können Sie dynamische Performance-Ereignisse auf einem Remote-Cluster in einer MetroCluster Konfiguration analysieren. Die Analyse hilft Ihnen festzustellen, ob ein Ereignis auf dem Remote-Cluster ein Ereignis auf dem Partner-

Cluster verursacht hat.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Sie müssen ein Performance-Ereignis auf einem lokalen Cluster in einer MetroCluster Konfiguration analysiert und die Ereigniserkennungszeit ermittelt haben.
- Sie müssen den Systemstatus des lokalen Clusters und des Partner-Clusters, das an dem Performance-Ereignis beteiligt ist, überprüft sowie den Namen des Partner-Clusters ermittelt haben.

Schritte

1. Bei der Unified Manager Instanz, die den Partnercluster überwacht, ist eine Anmeldung erforderlich.
2. Im linken Navigationsbereich lässt sich durch Klicken auf **Ereignisse** die Ereignisliste anzeigen.
3. Im Selektor **Time Range** erfolgt die Auswahl von **Last Hour**; anschließend folgt ein Klick auf **Apply Range**.
4. Im Selektor **Filter** wird im linken Dropdown-Menü **Cluster** ausgewählt, der Name des Partnerclusters in das Textfeld eingegeben und anschließend auf **Filter anwenden** geklickt.

   Wenn für den ausgewählten Cluster in der letzten Stunde keine Ereignisse verzeichnet wurden, bedeutet dies, dass der Cluster in dem Zeitraum, in dem das Ereignis auf seinem Partner erkannt wurde, keine Performance-Probleme hatte.

5. Wenn im ausgewählten Cluster in der letzten Stunde Ereignisse erkannt wurden, ist die Ereigniserkennungszeit mit der Ereigniserkennungszeit des Ereignisses im lokalen Cluster zu vergleichen.

   Wenn diese Ereignisse ressourcenintensive Workloads betreffen, die zu Ressourcenkonflikten auf der Datenverarbeitungskomponente führen, könnten einer oder mehrere dieser Workloads das Ereignis im lokalen Cluster verursacht haben. Sie können auf das Ereignis klicken, um es zu analysieren und die vorgeschlagenen Maßnahmen zu seiner Behebung auf der Seite mit den Ereignisdetails einzusehen.

   Falls diese Ereignisse keine Bully-Workloads betreffen, haben sie das Performance-Ereignis auf dem lokalen Cluster nicht verursacht.

Reaktion auf ein dynamisches QoS-Drosselungsereignis in Active IQ Unified Manager

Mit Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch eine QoS-Richtliniengruppe verursacht wurde, die den Workload-Durchsatz (MB/s) drosselt. Die Drosselung erhöhte die Antwortzeiten (Latenz) von Volume Workloads in der Richtliniengruppe. Anhand der Ereignisinformationen können Sie feststellen, ob neue Grenzwerte für die Richtliniengruppen erforderlich sind, um die Drosselung zu stoppen.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es muss neue, bestätigte oder veraltete Performance-Ereignisse geben.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. Unter **Beschreibung** werden die Namen der von der Drosselung betroffenen Workloads angezeigt.

   Die Beschreibung kann für Opfer und Verursacher dieselbe Workload anzeigen, da die

Drosselung die Workload zu ihrem eigenen Opfer macht.

3. Der Name des Volume wird mithilfe einer Applikation wie beispielsweise einem Texteditor notiert.

   Sie können anhand des Volume-Namens suchen, um ihn später wiederzufinden.

4. In den Diagrammen „Workload-Latenz“ und „Workload-Auslastung“ wird **Bully Workloads** ausgewählt.
5. Beim Bewegen des Mauszeigers über die Diagramme werden die wichtigsten benutzerdefinierten Workloads angezeigt, die sich auf die Richtliniengruppe auswirken.

   Die Arbeitslast an oberster Stelle der Liste weist die größte Abweichung auf und hat die Drosselung verursacht. Die Aktivität gibt den prozentualen Anteil des von jeder Arbeitslast genutzten Limits der Richtliniengruppe an.

6. Im Bereich **Suggested Actions** lässt sich für die oberste Workload die Schaltfläche **Analyze Workload** auswählen.
7. Auf der Seite „Workload Analysis“ ist das Latenzdiagramm auf die Ansicht aller Cluster Components und das Durchsatzdiagramm auf Breakdown eingestellt.

   Die Aufschlüsselungsdiagramme werden unterhalb des Latenzdiagramms und des IOPS-Diagramms angezeigt.

8. Im **Latenz**-Diagramm lässt sich anhand der QoS-Grenzwerte erkennen, in welchem Ausmaß die Drosselung die Latenz zum Zeitpunkt des Ereignisses beeinflusst hat.

   Die QoS Richtliniengruppe hat einen maximalen Durchsatz von 1.000 Operationen pro Sekunde (op/sec), den die darin enthaltenen Workloads gemeinsam nicht überschreiten können. Zum Zeitpunkt des Ereignisses hatten die Workloads in der Richtliniengruppe einen kombinierten Durchsatz von über 1.200 op/sec, wodurch die Richtliniengruppe ihre Aktivität auf 1.000 op/sec drosselte.

9. Zum Vergleich dienen die Werte für die **Lese-/Schreiblatenz** und die Werte für **Lese-/Schreib-/Sonstiges**.

   Beide Diagramme zeigen eine hohe Anzahl von Leseanfragen mit hoher Latenz, während die Anzahl der Anfragen und die Latenz bei Schreibanfragen gering sind. Anhand dieser Werte lässt sich feststellen, ob ein hoher Durchsatz oder eine hohe Anzahl von Operationen die Latenz erhöht hat. Diese Werte können bei der Entscheidung verwendet werden, eine Richtliniengruppenbegrenzung für den Durchsatz oder die Operationen festzulegen.

10. Mit ONTAP System Manager kann das aktuelle Limit der Richtliniengruppe auf 1.300 Operationen/Sek. erhöht werden.
11. Nach einem Tag können Sie zu Unified Manager zurückkehren und auf der Seite **Workload Analysis** die in Schritt 3 erfasste Workload eingeben.
12. Auswahl des Diagramms „Durchsatzaufschlüsselung“.

    Das Diagramm „Lesen/Schreiben/Sonstiges“ wird angezeigt.

13. Oben auf der Seite wird der Mauszeiger auf das Symbol für das Änderungsereignis () für die Änderung der Richtliniengruppenbegrenzung bewegt.
14. Vergleich zwischen dem Diagramm **Lesen/Schreiben/Sonstiges** und dem Diagramm **Latenz**.

    Die Lese- und Schreibanfragen sind gleich, aber die Drosselung hat aufgehört und die Latenz hat sich verringert.

Reaktion auf ein Leistungsereignis, das durch einen Festplattenausfall in Active IQ Unified Manager verursacht wird

Mit Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch Workloads verursacht wurde, die ein Aggregat übermäßig auslasten. Mit Unified Manager können Sie außerdem den Systemstatus des Aggregats prüfen, um festzustellen, ob kürzlich auf dem Aggregat erkannte Systemstatusereignisse zu dem Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es muss neue, bestätigte oder veraltete Performance-Ereignisse geben.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. Die **Beschreibung** enthält die am Ereignis beteiligten Workloads und die betroffene Clusterkomponente.

   Es gibt mehrere betroffene Volumes, deren Latenz durch die Clusterkomponente mit Konfliktpotenzial beeinträchtigt wurde. Das Aggregat, das sich mitten in einer RAID Rekonstruktion befindet, um die ausgefallene Festplatte durch eine Ersatzfestplatte zu ersetzen, ist die Clusterkomponente mit Konfliktpotenzial. Unter Component in Contention ist das Aggregatssymbol rot hervorgehoben, und der Name des Aggregats wird in Klammern angezeigt.

3. Im Diagramm zur Workload Auslastung erfolgt die Auswahl von **Bully Workloads**.
4. Wenn sich der Mauszeiger über dem Diagramm befindet, werden die wichtigsten Bully-Workloads angezeigt, die sich auf die Komponente auswirken.

   Die Workloads mit der höchsten Spitzenauslastung seit Erkennung des Ereignisses werden oben im Diagramm angezeigt. Einer der wichtigsten Workloads ist der systemdefinierte Workload Disk Health, der auf eine RAID-Rekonstruktion hinweist. Eine Rekonstruktion ist der interne Prozess zum Wiederaufbau des Aggregats mit der Ersatzfestplatte. Der Workload Disk Health hat zusammen mit anderen Workloads auf dem Aggregat wahrscheinlich die Auslastungskonkurrenz auf dem Aggregat und das zugehörige Ereignis verursacht.

5. Nachdem bestätigt wurde, dass die Aktivität der Arbeitslast „Disk Health“ das Ereignis verursacht hat, ist etwa 30 Minuten zu warten, bis die Rekonstruktion abgeschlossen ist und Unified Manager das Ereignis analysiert hat und erkennt, ob das Aggregat noch in Konflikt steht.
6. Aktualisierung der **Event details**.

   Nach Abschluss der RAID-Rekonstruktion sollte der State „obsolete“ sein; daran ist erkennbar, dass das Ereignis behoben ist.

7. Im Diagramm zur Workload Auslastung werden bei Auswahl von **Bully Workloads** die Workloads auf dem Aggregat nach Spitzenauslastung angezeigt.
8. Im Bereich **Suggested Actions** lässt sich für die oberste Workload die Schaltfläche **Analyze Workload** auswählen.
9. Auf der Seite **Workload Analysis** ist der Zeitbereich auf die letzten 24 Stunden (1 Tag) festgelegt, sodass die Daten für das ausgewählte Volume angezeigt werden.

   In der Ereigniszeitleiste zeigt ein roter Punkt (🔴) an, wann der Festplattenausfall aufgetreten ist.

10. Im Diagramm „Knoten- und Aggregatauslastung“ bleibt nach dem Ausblenden der Linie für die Knotenstatistiken nur die Aggregatlinie sichtbar.
11. Hier erfolgt der Vergleich der Daten in diesem Diagramm mit den Daten zum Zeitpunkt des Ereignisses im Diagramm **Latency**.

    Zum Zeitpunkt des Ereignisses wies die Aggregatauslastung eine hohe Lese- und Schreibaktivität auf, verursacht durch die RAID-Rekonstruktionsprozesse, was die Latenz des ausgewählten Volumes erhöhte. Wenige Stunden nach dem Auftreten des Ereignisses waren sowohl die Lese- und Schreibvorgänge als auch die Latenz gesunken, was bestätigt, dass beim Aggregat kein Ressourcenkonflikt mehr besteht.

Reaktion auf ein Leistungsereignis, das durch eine HA Übernahme in Active IQ Unified Manager verursacht wurde

Mit Unified Manager können Sie ein Performance-Ereignis untersuchen, das durch hohe Data Processing auf einem Cluster-Knoten verursacht wurde, der sich in einem Hochverfügbarkeitspaar (HA) befindet. Mit Unified Manager können Sie außerdem den Systemstatus der Knoten prüfen, um festzustellen, ob kürzlich auf den Knoten erkannte Systemstatusereignisse zu dem Performance-Ereignis beigetragen haben.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Es muss neue, bestätigte oder veraltete Performance-Ereignisse geben.

Schritte

1. Die Seite **Ereignisdetails** enthält Informationen zum Ereignis.
2. Die **Beschreibung** enthält die am Ereignis beteiligten Workloads und die betroffene Clusterkomponente.

    Es gibt ein betroffenes Volume, dessen Latenz durch die Clusterkomponente in Konflikt beeinträchtigt wurde. Der Data Processing Knoten, der alle Workloads von seinem Partnerknoten übernommen hat, ist die Clusterkomponente in Konflikt. Unter „Component in Contention“ ist das Data Processing Symbol rot hervorgehoben, und der Name des Knotens, der zum Zeitpunkt des Ereignisses die Data Processing verarbeitete, wird in Klammern angezeigt.

3. In der **Beschreibung** wählen Sie den Namen des Volumes aus.

    Die Seite „Volume Performance Explorer“ wird angezeigt. Oben auf der Seite zeigt in der Zeitleiste der Ereignisse ein Symbol für ein Änderungsereignis ( ) den Zeitpunkt an, zu dem Unified Manager den Beginn der HA-Übernahme erkannt hat.

4. Wenn der Cursor auf das Änderungsereignissymbol für die HA-Übernahme zeigt, werden Details zur HA-Übernahme als Hover-Text angezeigt.

    Im Latenzdiagramm zeigt ein Ereignis an, dass das ausgewählte Volume aufgrund hoher Latenz etwa zur gleichen Zeit wie die HA-Übernahme den Performance-Schwellenwert überschritten hat.

5. Mit **Zoom View** wird das Latenzdiagramm auf einer neuen Seite angezeigt.
6. Im Menü „Ansicht“ dient **Cluster Components** zur Anzeige der Gesamtlatenz nach Clusterkomponente.
7. Wenn Sie den Mauszeiger auf das Änderungsereignissymbol für den Beginn der HA Übernahme richten, lässt sich die Latenz für Data Processing mit der Gesamtlatenz vergleichen.

    Zum Zeitpunkt der HA-Übernahme kam es aufgrund der erhöhten Workload-Anforderung auf dem Data

Processing Knoten zu einem sprunghaften Anstieg der Data Processing. Die erhöhte CPU-Auslastung führte zu einer höheren Latenz und löste das Ereignis aus.

8. Nach der Reparatur des ausgefallenen Knotens erfolgt die Durchführung einer HA-Rückführung in ONTAP System Manager, wodurch die Workloads vom Partnerknoten auf den reparierten Knoten verschoben werden.
9. Nach Abschluss des HA Giveback und nach der nächsten Konfigurationserkennung in Unified Manager (ca. 15 Minuten) lassen sich auf der Inventarseite **Event Management** das Ereignis und die Workload finden, die durch das HA Takeover ausgelöst wurden.

   Das durch die HA-Übernahme ausgelöste Ereignis hat nun den Status „veraltet“, was darauf hinweist, dass das Ereignis behoben ist. Die Latenz der Data Processing-Komponente hat sich verringert, wodurch die Gesamtlatenz gesunken ist. Der Knoten, den das ausgewählte Volume nun für Data Processing verwendet, hat das Ereignis behoben.

Performance-Ereignisse beheben

Leistungsereignisse in Active IQ Unified Manager beheben

Sie können die vorgeschlagenen Maßnahmen nutzen, um Performance-Ereignisse selbst zu beheben. Die ersten drei Vorschläge werden immer angezeigt, und die Maßnahmen unter dem vierten Vorschlag sind spezifisch für den angezeigten Ereignistyp.

Die Links „Help me do this“ bieten zusätzliche Informationen zu jeder vorgeschlagenen Aktion, einschließlich Anweisungen zur Durchführung einer bestimmten Aktion. Einige der Aktionen können die Verwendung von Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI-Befehlen oder einer Kombination dieser Tools erfordern.

Bestätigen Sie, dass die Latenz im Active IQ Unified Manager innerhalb des erwarteten Bereichs liegt

Wenn eine Clusterkomponente überlastet ist, kann dies die Antwortzeit (Latenz) der darauf zugreifenden Volume-Workloads verringern. Sie können die Latenz jedes betroffenen Workloads auf der überlasteten Komponente überprüfen, um sicherzustellen, dass sie im erwarteten Bereich liegt. Durch Klicken auf einen Volume-Namen können Sie außerdem die Verlaufsdaten für dieses Volume anzeigen.

Wenn sich das Performance-Ereignis im veralteten Zustand befindet, könnte die Latenz jedes an dem Ereignis beteiligten Opfers wieder innerhalb des erwarteten Bereichs liegen.

Bewertung, wie sich Konfigurationsänderungen auf die Workload-Performance in Active IQ Unified Manager auswirken

Konfigurationsänderungen am Cluster, wie z. B. ein ausgefallener Datenträger, ein HA Failover oder ein verschobenes Volume, können sich negativ auf die Volume Performance auswirken und zu erhöhter Latenz führen.

In Unified Manager können Sie die Seite „Workload-Analyse“ einsehen, um festzustellen, wann eine aktuelle Konfigurationsänderung erfolgt ist, und dies mit den Operationen und der Latenz (Antwortzeit) vergleichen, um zu prüfen, ob sich die Aktivität für die ausgewählte Volume-Workload geändert hat.

Die Performance Seiten von Unified Manager können nur eine begrenzte Anzahl von Änderungsereignissen erkennen. Die Systemstatus Seiten bieten Warnmeldungen für andere Ereignisse, die durch Konfigurationsänderungen verursacht werden. Sie können in Unified Manager nach dem Volume suchen, um den Ereignisverlauf anzuzeigen.

Die Workload-Performance kann durch Anpassen der Client-seitig Einstellungen in Active IQ Unified Manager verbessert werden

Sie können Ihre Client-Workloads, wie z. B. Applikationen oder Datenbanken, die E/A an Volumes senden, die an einem Performance-Ereignis beteiligt sind, überprüfen, um festzustellen, ob eine Client-seitig Änderung das Ereignis korrigieren könnte.

Wenn die Clients, die mit Volumes auf einem Cluster verbunden sind, ihre E/A-Anforderungen erhöhen, muss der Cluster mehr leisten, um die Nachfrage zu erfüllen. Wenn Sie wissen, welche Clients eine hohe Anzahl von E/A-Anforderungen an ein bestimmtes Volume auf dem Cluster stellen, können Sie die Cluster Performance verbessern, indem Sie die Anzahl der Clients anpassen, die auf das Volume zugreifen, oder die Menge der E/A-Vorgänge für das Volume verringern. Sie können außerdem ein Limit auf die QoS-Richtliniengruppe anwenden oder erhöhen, der das Volume angehört.

Sie können Clients und deren Applikationen untersuchen, um festzustellen, ob die Clients mehr E/A-Operationen als üblich senden, was zu Engpässen bei einer Clusterkomponente führen könnte. Auf der Seite „Ereignisdetails“ zeigt der Abschnitt „Systemdiagnose“ die Volume-Workloads mit der höchsten Auslastung an, die die von Engpässen betroffene Komponente verwenden. Wenn Sie wissen, welcher Client auf ein bestimmtes Volume zugreift, können Sie zum Client wechseln, um festzustellen, ob die Clienthardware oder eine Applikation nicht wie erwartet funktioniert oder mehr Arbeit als üblich ausführt.

In einer MetroCluster Konfiguration werden Schreibanforderungen an ein Volume auf einem lokalen Cluster auf ein Volume auf dem Remote-Cluster gespiegelt. Die Synchronisierung des Quell-Volumes auf dem lokalen Cluster mit dem Ziel-Volume auf dem Remote-Cluster kann in der MetroCluster Konfiguration auch die Auslastung beider Cluster erhöhen. Durch die Reduzierung der Schreibanforderungen an diese gespiegelten Volumes können die Cluster weniger Synchronisierungsvorgänge durchführen, wodurch sich die Performance-Auswirkungen auf andere Workloads verringern.

Wie sich Client- oder Netzwerkprobleme auf die Leistung in Active IQ Unified Manager auswirken

Wenn die E/A-Anforderungen der Clients, die mit Volumes in einem Cluster verbunden sind, steigen, muss der Cluster härter arbeiten, um die Nachfrage zu erfüllen. Die erhöhte Belastung des Clusters kann dazu führen, dass eine Komponente in einen Engpass gerät, die Latenz der Workloads erhöht wird, die sie verwenden, und ein Ereignis in Unified Manager ausgelöst wird.

Auf der Seite mit den Ereignisdetails zeigt der Abschnitt „Systemdiagnose“ die wichtigsten Volume-Workloads an, die die umkämpfte Komponente verwenden. Wenn Sie wissen, welcher Client auf ein bestimmtes Volume zugreift, können Sie auf dem Client feststellen, ob die Clienthardware oder eine Applikation nicht wie erwartet funktioniert oder mehr Arbeit als üblich ausführt. Gegebenenfalls ist Unterstützung durch Ihren Clientadministrator oder den Anbieter der Applikation erforderlich.

Sie können Ihre Netzwerkinfrastruktur prüfen, um festzustellen, ob Hardwareprobleme, Engpässe oder konkurrierende Workloads vorliegen, die möglicherweise dazu geführt haben, dass E/A-Anfragen zwischen dem Cluster und den verbundenen Clients langsamer als erwartet ausgeführt werden. Gegebenenfalls ist die Unterstützung durch Ihren Netzwerkadministrator erforderlich.

Analyse von Volumes mit hoher Aktivität innerhalb einer QoS-Richtliniengruppe in Active IQ Unified Manager

Sie können die Workloads in der Quality of Service (QoS)-Richtliniengruppe mit der größten Aktivitätsänderung überprüfen, um festzustellen, ob mehr als ein Workload das Ereignis verursacht hat. Außerdem können Sie prüfen, ob andere Workloads die festgelegte Durchsatzbegrenzung noch überschreiten oder ob sie sich wieder innerhalb ihres erwarteten Aktivitätsbereichs befinden.

Auf der Seite mit den Ereignisdetails können Sie im Abschnitt „Systemdiagnose“ die Workloads nach der maximalen Aktivitätsabweichung sortieren, um die Workloads mit der größten Aktivitätsänderung oben in der Tabelle anzuzeigen. Diese Workloads könnten die „`bullies`“ sein, deren Aktivität den festgelegten Grenzwert überschritten hat und das Ereignis möglicherweise verursacht hat.

Sie können für jede Volume-Workload die Seite „Workload Analysis“ aufrufen, um deren IOPS-Aktivität zu überprüfen. Falls die Workload Phasen mit sehr hoher Vorgangsaktivität aufweist, könnte dies zu dem Ereignis beigetragen haben. Sie können die Richtliniengruppeneinstellungen für die Workload ändern oder die Workload in eine andere Richtliniengruppe verschieben.

Mit ONTAP System Manager oder den ONTAP CLI-Befehlen können Sie Richtliniengruppen wie folgt managen:

- Eine Richtliniengruppe erstellen.
- Workloads in einer Richtliniengruppe hinzufügen oder entfernen.
- Eine Arbeitslast zwischen Richtliniengruppen verschieben.
- Die Durchsatzbegrenzung einer Richtliniengruppe ändern.

Verschieben von LIFs zur Verbesserung der Leistung in Active IQ Unified Manager

Das Verschieben logischer Schnittstellen (LIFs) auf einen weniger ausgelasteten Port kann dazu beitragen, die Lastverteilung zu verbessern, Wartungsarbeiten und das Performance-Tuning zu unterstützen sowie indirekte Zugriffe zu reduzieren.

Indirekter Zugriff kann die Systemeffizienz beeinträchtigen. Er tritt auf, wenn die Workload eines Volume unterschiedliche Knoten für die Netzwerkverarbeitung und die Datenverarbeitung verwendet. Um indirekten Zugriff zu reduzieren, können Sie LIFs neu anordnen. Dies umfasst das Verschieben von LIFs, sodass sie denselben Knoten für die Netzwerkverarbeitung und die Datenverarbeitung verwenden. Sie können den Lastausgleich so konfigurieren, dass ONTAP ausgelastete LIFs automatisch auf einen anderen Port verschiebt, oder Sie können eine LIF manuell verschieben.

Vorteile	Überlegungen
• Verbesserung der Lastverteilung. • Indirekten Zugriff reduzieren.	Beim Verschieben einer LIF, die mit CIFS-Freigaben verbunden ist, werden Clients, die auf die CIFS-Freigaben zugreifen, getrennt. Sämtliche Lese- und Schreibanforderungen an die CIFS-Freigaben werden unterbrochen.

Sie verwenden die ONTAP Befehle zur Konfiguration des Lastausgleichs. Weitere Informationen finden Sie in der ONTAP Networking-Dokumentation.

Sie verwenden ONTAP System Manager und die ONTAP CLI-Befehle, um LIFs manuell zu verschieben.

Ausführung von Storage Effizienzvorgängen zu weniger ausgelasteten Zeiten

Speichereffizienzvorgänge werden in Active IQ Unified Manager für Zeiten mit geringerer Auslastung geplant

Sie können die Richtlinie oder den Zeitplan, die bzw. der Storage Effizienzvorgänge steuert, so ändern, dass diese Vorgänge ausgeführt werden, wenn die Workloads der betroffenen Volumes weniger ausgelastet sind.

Storage-Effizienzvorgänge können einen hohen Anteil der CPU-Ressourcen des Clusters nutzen und die Volumes, auf denen die Vorgänge ausgeführt werden, stark belasten. Wenn die betroffenen Volumes gleichzeitig eine hohe Aktivität aufweisen, während die Storage-Effizienzvorgänge ausgeführt werden, kann sich ihre Latenz erhöhen und ein Ereignis auslösen.

Auf der Seite mit den Ereignisdetails zeigt der Abschnitt „Systemdiagnose“ die Workloads in der QoS-Richtliniengruppe anhand der Spitzenabweichung bei der Aktivität an, um die störenden Workloads zu identifizieren. Wenn „`storage efficiency`“ im oberen Bereich der Tabelle angezeigt wird, beeinträchtigen diese Vorgänge die betroffenen Workloads. Durch Anpassen der Effizienzrichtlinie oder des Zeitplans, damit diese Vorgänge ausgeführt werden, wenn diese Workloads weniger ausgelastet sind, lässt sich verhindern, dass die Vorgänge der Storage-Effizienz zu Ressourcenkonflikten im Cluster führen.

Mit ONTAP System Manager können Sie Effizienzrichtlinien managen. Mit den ONTAP Befehlen können Sie Effizienzrichtlinien und Zeitpläne managen.

Informationen zur Speichereffizienz in Active IQ Unified Manager

Storage-Effizienz ermöglicht es Ihnen, die maximale Datenmenge zu den niedrigsten Kosten zu speichern und ein schnelles Datenwachstum bei gleichzeitig geringerem Speicherplatzbedarf zu bewältigen. Die NetApp Strategie für Storage-Effizienz basiert auf der integrierten Grundlage von Storage-Virtualisierung und einheitlichem Storage, die durch das zentrale ONTAP Betriebssystem und das WAFL Dateisystem (Write Anywhere File Layout) bereitgestellt werden.

Zur Storage-Effizienz gehört der Einsatz von Technologien wie Thin Provisioning, Snapshot Kopie, Deduplizierung, Datenkomprimierung, FlexClone, Thin Replication mit SnapVault und Volume SnapMirror, RAID-DP, Flash Cache, Flash Pool Aggregat und FabricPool-fähigen Aggregaten, die dazu beitragen, die Storage-Auslastung zu erhöhen und die Storage-Kosten zu senken.

Die einheitliche Storage-Architektur ermöglicht die effiziente Konsolidierung eines SAN, eines Network Attached Storage (NAS) und von sekundärem Storage auf einer einzigen Plattform.

Hochdichte Festplattenlaufwerke, wie z. B. Serial Advanced Technology Attachment (SATA)-Laufwerke, die innerhalb eines Flash Pool Aggregats oder mit Flash Cache und RAID-DP Technologie konfiguriert sind, erhöhen die Effizienz, ohne Performance und Ausfallsicherheit zu beeinträchtigen.

Ein für FabricPool aktiviertes Aggregat umfasst ein reines SSD-Aggregat oder HDD-Aggregat (ab ONTAP 9.8) als lokalen Performance-Tier und einen Objektspeicher, den Sie als Cloud-Tier festlegen. Die Konfiguration von FabricPool unterstützt Sie beim Managen, auf welchem Storage-Tier, dem lokalen Tier oder dem Cloud-Tier, Daten gespeichert werden sollen, je nachdem, ob häufig auf sie zugegriffen wird.

Technologien wie Thin Provisionierung, Snapshot-Kopien, Deduplizierung, Datenkomprimierung, Thin-

Replikation mit SnapVault und Volume SnapMirror sowie FlexClone bieten bessere Einsparungen. Diese Technologien können einzeln oder zusammen genutzt werden, um maximale Storage-Effizienz zu erzielen.

Informationen dazu, wie sich das Hinzufügen von Festplatten auf die Datenneuverteilung in Active IQ Unified Manager auswirkt

Sie können einem Aggregat Festplatten hinzufügen, um die Storage-Kapazität und die Performance dieses Aggregats zu erhöhen. Nach dem Hinzufügen der Festplatten ist eine Verbesserung der Lese Performance erst nach der Neuverteilung der Daten auf die hinzugefügten Festplatten zu erkennen.

Diese Anweisungen gelten, wenn Unified Manager Aggregatereignisse empfangen hat, die durch dynamische Schwellenwerte oder systemdefinierte Performance-Schwellenwerte ausgelöst wurden:

- Wenn Sie ein Ereignis mit einem dynamischen Schwellenwert erhalten haben, wird auf der Seite „Ereignisdetails“ das Clusterkomponentensymbol, das das von einer Ressourcenkonkurrenz betroffene Aggregat darstellt, rot hervorgehoben.

  Unterhalb des Symbols steht in Klammern der Name des Aggregats, der kennzeichnet, zu welchem Aggregat Sie Datenträger hinzufügen können.

- Wenn Sie ein systemdefiniertes Schwellenwertereignis erhalten haben, enthält der Ereignisbeschreibungstext auf der Seite mit den Ereignisdetails den Namen des Aggregats, bei dem das Problem auftritt.

  Sie können diesem Aggregat Festplatten hinzufügen und Daten neu verteilen.

Die dem Aggregat hinzugefügten Datenträger müssen bereits im Cluster vorhanden sein. Falls im Cluster keine zusätzlichen Datenträger verfügbar sind, ist möglicherweise eine Kontaktaufnahme mit Ihrem Administrator oder der Erwerb weiterer Datenträger erforderlich. Sie können ONTAP System Manager oder die ONTAP-Befehle verwenden, um Datenträger zu einem Aggregat hinzuzufügen.

> Eine Neuzuweisung von Daten ist nur bei der Verwendung von HDD- und Flash Pool Aggregaten zu empfehlen. Auf SSD- oder FabricPool Aggregaten sollten Daten nicht neu zugewiesen werden.

Die Workload-Performance lässt sich durch das Aktivieren von Flash Cache auf einem Knoten in Active IQ Unified Manager verbessern

Die Workload Performance lässt sich verbessern, indem auf jedem Knoten im Cluster Flash Cache™ intelligentes Daten-Caching aktiviert wird.

Ein Flash Cache Modul, auch Performance Acceleration Module genannt, ein PCIe-basiertes Speichermodul, optimiert die Performance von random-read-intensiven Workloads, indem es als intelligenter externer Lesecache fungiert. Diese Hardware arbeitet mit der WAFL External Cache Softwarekomponente von ONTAP zusammen.

Im Unified Manager ist auf der Seite mit den Ereignisdetails das Symbol der Clusterkomponente, die das betroffene Aggregat darstellt, rot hervorgehoben. Unter dem Symbol steht in Klammern der Name des Aggregats, der das Aggregat identifiziert. Sie können Flash Cache auf dem Node aktivieren, auf dem sich das Aggregat befindet.

Sie können ONTAP System Manager oder die ONTAP-Befehle verwenden, um zu prüfen, ob Flash Cache installiert oder aktiviert ist, und ihn gegebenenfalls zu aktivieren. Der folgende Befehl zeigt an, ob Flash Cache auf einem bestimmten Knoten aktiviert ist: **`cluster::> run local options flexscale.enable`**

Weitere Informationen zu Flash Cache und den Anforderungen für seine Verwendung enthält der folgende technische Bericht:

"Technischer Bericht 3832: Flash Cache Best Practices-Leitfaden"

Die Workload-Performance kann durch die Aktivierung von Flash Pool auf einem Speicheraggregat in Active IQ Unified Manager verbessert werden.

Sie können die Workload Performance verbessern, indem Sie die Flash Pool Funktion auf einem Aggregat aktivieren. Ein Flash Pool ist ein Aggregat, das sowohl HDDs als auch SSDs umfasst. Die HDDs werden für den primären Storage verwendet, und die SSDs stellen einen leistungsstarken Lese- und Schreibcache bereit, um die Performance des Aggregats zu steigern.

Im Unified Manager zeigt die Seite mit den Ereignisdetails den Namen des betroffenen Aggregats an. Mithilfe von ONTAP System Manager oder den ONTAP Befehlen können Sie prüfen, ob Flash Pool für ein Aggregat aktiviert ist. Wenn SSDs installiert sind, können Sie Flash Pool über die Befehlszeilenschnittstelle aktivieren. Wenn SSDs installiert sind, können Sie den folgenden Befehl auf dem Aggregat ausführen, um zu prüfen, ob Flash Pool aktiviert ist: **`cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled`**

In diesem Befehl ist *`aggr_name`* der Name des Aggregats, z. B. des Aggregats, um das es geht.

Weitere Informationen zu Flash Pool und den Anforderungen für dessen Verwendung sind im *Clustered Data ONTAP Physical Storage Management Guide* enthalten.

Prüfen des Zustands der MetroCluster Konfiguration in Active IQ Unified Manager

Mit Unified Manager können Sie den Systemstatus der Cluster in einer MetroCluster Konfiguration über IP oder FC überprüfen. Der Systemstatus und die Ereignisse helfen Ihnen festzustellen, ob Hardware- oder Softwareprobleme vorliegen, die die Performance Ihrer Workloads beeinträchtigen könnten.

Wenn Sie Unified Manager so konfigurieren, dass E-Mail-Benachrichtigungen gesendet werden, können Sie Ihre E-Mails auf etwaige Systemstatusprobleme im lokalen oder Remote-Cluster prüfen, die möglicherweise zu einem Performance-Ereignis beigetragen haben. In der Unified Manager GUI kann eine Liste aktueller Ereignisse unter **Event Management** ausgewählt werden, und anschließend können mithilfe der Filter nur MetroCluster Konfigurationsereignisse angezeigt werden.

Weitere Informationen sind unter "Überprüfung des Systemstatus von Clustern in einer MetroCluster Konfiguration" verfügbar.

Überprüfung der MetroCluster Konfigurationen in Active IQ Unified Manager

Performanceprobleme bei gespiegelten Workloads in MetroCluster FC- und IP-Konfigurationen lassen sich vermeiden, indem sichergestellt wird, dass die MetroCluster Konfiguration korrekt eingerichtet ist. Die Performance von Workloads kann auch durch

Änderungen an der Konfiguration oder durch Upgrades von Software- oder Hardwarekomponenten verbessert werden.

Anweisungen zum Einrichten der Cluster in der MetroCluster Konfiguration, einschließlich der Fibre Channel (FC) Switches, Kabel und Inter-Switch-Links (ISLs), finden Sie in "MetroCluster Dokumentation". Außerdem unterstützt sie Sie bei der Konfiguration der MetroCluster Software, sodass die lokalen und Remote-Cluster mit gespiegelten Volume-Daten kommunizieren können. Spezifische Informationen zu Ihrer MetroCluster over IP Konfiguration finden Sie in "Installation einer MetroCluster IP Konfiguration".

Sie können Ihre MetroCluster Konfiguration mit den Anforderungen in "MetroCluster Dokumentation" vergleichen, um festzustellen, ob eine Änderung oder Aktualisierung von Komponenten in Ihrer MetroCluster Konfiguration die Workload-Performance verbessern könnte. Dieser Vergleich kann Ihnen helfen, die folgenden Fragen zu beantworten:

- Sind die Controller für Ihre Workloads geeignet?
- Müssen Sie Ihre ISL Bundles auf eine höhere Bandbreite aufrüsten, um einen höheren Durchsatz zu bewältigen?
- Können Sie die Buffer-to-Buffer-Credits (BBC) an Ihren Switches anpassen, um die Bandbreite zu erhöhen?
- Wenn Ihre Workloads einen hohen Schreibdurchsatz auf Solid-State-Drive-(SSD)-Storage aufweisen, müssen Sie dann Ihre FC-zu-SAS-Brücken aufrüsten, um den Durchsatz zu bewältigen?

Verwandte Informationen

- Informationen zum Austausch oder zur Aufrüstung von MetroCluster Komponenten finden Sie im "MetroCluster Dokumentation".
- Informationen zum Upgrade von Controllern finden Sie unter "Aktualisierung von Controllern in einer MetroCluster FC-Konfiguration mittels Switchover und Switchback" und "Aktualisierung von Controllern in einer MetroCluster IP-Konfiguration mittels Switchover und Switchback"

Workloads in Active IQ Unified Manager in ein anderes Aggregat verschieben

Mit Unified Manager können Sie ein Aggregat identifizieren, das weniger ausgelastet ist als das Aggregat, auf dem sich Ihre Workloads derzeit befinden. Anschließend können Sie ausgewählte Volumes oder LUNs auf dieses Aggregat verschieben. Durch das Verschieben leistungsstarker Workloads auf ein weniger ausgelastetes Aggregat oder auf ein Aggregat mit aktiviertem Flash Storage können die Workloads effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Sie müssen den Namen des Aggregats notiert haben, bei dem aktuell ein Performance Problem vorliegt.
- Sie müssen das Datum und die Uhrzeit protokolliert haben, zu denen das Aggregat das Ereignis erhalten hat.
- Unified Manager muss Performance-Daten von mindestens einem Monat erfasst und analysiert haben.

Diese Schritte helfen Ihnen, die folgenden Ressourcen zu identifizieren, damit Sie leistungsstarke Workloads auf ein weniger ausgelastetes Aggregat verschieben können:

- Die Aggregate im selben Cluster, die weniger ausgelastet sind
- Die Volumes mit der höchsten Performance im aktuellen Aggregat

Schritte

1. Zu identifizieren ist das im Cluster am wenigsten ausgelastete Aggregat:
   a. Auf der **Ereignis**-Detailseite erfolgt die Auswahl des Namens des Clusters, auf dem sich das Aggregat befindet.

      Auf der Seite Performance/Cluster-Startseite sind die Clusterdetails zu sehen.

   b. Auf der Seite **Zusammenfassung** erfolgt die Auswahl von **Aggregate** im Bereich **Verwaltete Objekte**.

      Die Liste der Aggregate in diesem Cluster wird angezeigt.

   c. Ein Klick auf die Spalte **Auslastung** sortiert die Aggregate nach der geringsten Auslastung.

      Sie können auch diejenigen Aggregate identifizieren, die über die größte **Free Capacity** verfügen. Dadurch erhalten Sie eine Liste potenzieller Aggregate, auf die Sie Workloads verschieben könnten.

   d. Zu notieren ist der Name des Aggregats, in das die Workloads verschoben werden sollen.
2. Leistungsstarke Volumes des Aggregats, das das Ereignis erhalten hat:
   a. Das Aggregat, bei dem das Performanceproblem auftritt, ist auszuwählen.

      Die Aggregatdetails sind auf der Seite „Performance/Aggregate Explorer“ zu sehen.

   b. Im Auswahlfeld **Zeitraum** ist die Option **Letzte 30 Tage** auszuwählen; anschließend ist auf **Bereich anwenden** zu klicken.

      Dadurch können Sie einen längeren Zeitraum des Performance Verlaufs als die standardmäßigen 72 Stunden anzeigen. Sie möchten ein Volume verschieben, das dauerhaft viele Ressourcen nutzt, nicht nur in den letzten 72 Stunden.

   c. Im Steuerelement **View and Compare** erfolgt die Auswahl von **Volumes on this Aggregate**.

      Auf diesem Aggregat wird eine Liste der FlexVol Volumes und der FlexGroup Bestandteil-Volumes angezeigt.

   d. Durch das Sortieren der Volumes nach der höchsten MB/s-Rate und anschließend nach der höchsten IOPS-Rate werden die Volumes mit der höchsten Performance angezeigt.
   e. Zu notieren sind die Namen der Volumes, die in ein anderes Aggregate verschoben werden sollen.
3. Die Volumes mit hoher Performance in das als gering ausgelastet identifizierte Aggregat verschieben.

   Sie können den Verschiebevorgang mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools durchführen.

Nach einigen Tagen lässt sich prüfen, ob Sie von diesem Knoten oder Aggregat dieselbe Art von Ereignissen erhalten.

Workloads in Active IQ Unified Manager auf einen anderen Node verschieben

Mit Unified Manager können Sie ein Aggregat auf einem anderen Knoten identifizieren, der weniger ausgelastet ist als der Knoten, auf dem Ihre Workloads derzeit ausgeführt

werden, und anschließend ausgewählte Volumes auf dieses Aggregat verschieben. Wenn leistungsstarke Workloads auf ein Aggregat auf einem weniger ausgelasteten Knoten verlagert werden, können die Workloads auf beiden Knoten effizienter arbeiten.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Sie müssen den Namen des Knotens notiert haben, bei dem derzeit ein Performance Problem auftritt.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu denen der Knoten das Performance-Ereignis empfangen hat.
- Unified Manager muss Performance-Daten über einen Zeitraum von mindestens einem Monat erfasst und analysiert haben.

Dieses Verfahren hilft Ihnen, die folgenden Ressourcen zu identifizieren, damit Sie leistungsstarke Workloads auf einen weniger ausgelasteten Knoten verschieben können:

- Die Knoten im selben Cluster mit der größten freien Performancekapazität
- Die Aggregate auf dem neuen Knoten, die über die größte freie Performancekapazität verfügen
- Die leistungsstärksten Volumes auf dem aktuellen Knoten

Schritte

1. Zu ermitteln ist der Knoten im Cluster mit der größten freien Performance-Kapazität:
   a. Auf der Seite **Ereignisdetails** erfolgt die Auswahl des Namens des Clusters, in dem sich der Knoten befindet.

      Auf der Seite Performance/Cluster-Startseite sind die Clusterdetails zu sehen.

   b. Auf der Registerkarte **Zusammenfassung** erfolgt die Auswahl von **Knoten** im Bereich **Verwaltete Objekte**.

      Die Liste der Knoten in diesem Cluster wird angezeigt.

   c. Mit einem Klick auf die Spalte **Performance Capacity Used** werden die Knoten nach dem geringsten verwendeten Prozentsatz sortiert.

      Dies bietet eine Liste potenzieller Knoten, auf die Sie Arbeitslasten verschieben könnten.

   d. Zu notieren ist der Name des Knotens, auf den Sie die Workloads verschieben möchten.
2. Das am wenigsten ausgelastete Aggregat auf dem neuen Knoten ist zu identifizieren:
   a. Im linken Navigationsbereich: **Storage** > **Aggregates**; im Menü Ansicht: **Performance** > **All Aggregates**.

      Die Ansicht „Performance: Alle Aggregate“ wird angezeigt.

   b. Unter **Filtering** wählen Sie im linken Dropdown-Menü **Node** aus, geben den Namen des Node in das Textfeld ein und klicken dann auf **Apply Filter**.

      Die Ansicht „Performance: Alle Aggregate“ wird erneut angezeigt und enthält die Liste der auf diesem Knoten verfügbaren Aggregate.

   c. Ein Klick auf die Spalte **Genutzte Performance-Kapazität** sortiert die Aggregate nach der geringsten

Auslastung.

Dies bietet eine Liste potenzieller Aggregate, auf die Sie Workloads verschieben könnten.

d. Zu notieren ist der Name des Aggregats, in das die Workloads verschoben werden sollen.

3. Identifizierung der leistungsstarken Workloads des Knotens, der das Ereignis empfangen hat:
   a. Die Seite **Event Details** für das Ereignis wird wieder angezeigt.
   b. Im Feld **Betroffene Volumes** kann der Link für die Anzahl der Volumes ausgewählt werden.

      Die Ansicht „Performance: Alle Volumes“ zeigt eine gefilterte Liste der Volumes auf diesem Knoten an.

   c. Über die Spalte **Gesamtkapazität** können Sie die Volumes nach dem größten zugewiesenen Speicherplatz sortieren.

      Dadurch erhalten Sie eine Liste potenzieller Volumes, die Sie möglicherweise verschieben möchten.

   d. Zu notieren sind die Namen der Volumes, die verschoben werden sollen, sowie die Namen der aktuellen Aggregate, auf denen sie sich befinden.
4. Die Volumes sollten auf die Aggregate verschoben werden, die Sie auf dem neuen Knoten als diejenigen mit der größten freien Performance Kapazität identifiziert haben.

   Sie können den Verschiebevorgang mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools durchführen.

Nach einigen Tagen lässt sich prüfen, ob Sie von diesem Knoten oder Aggregat dieselbe Art von Ereignissen erhalten.

Verschieben von Workloads auf ein Aggregat auf einem anderen Node in Active IQ Unified Manager

Mit Unified Manager kann ein Aggregat auf einem anderen Knoten identifiziert werden, der weniger ausgelastet ist als der Knoten, auf dem Ihre Workloads derzeit ausgeführt werden. Anschließend können ausgewählte Volumes auf dieses Aggregat verschoben werden. Durch das Verschieben leistungsstarker Workloads auf ein Aggregat auf einem weniger ausgelasteten Knoten können die Workloads auf beiden Knoten effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Sie müssen den Namen des Knotens notiert haben, bei dem derzeit ein Performance Problem auftritt.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu denen der Knoten das Performance-Ereignis empfangen hat.
- Unified Manager muss Performance-Daten von mindestens einem Monat erfasst und analysiert haben.

Diese Schritte helfen Ihnen, die folgenden Ressourcen zu identifizieren, damit Sie leistungsstarke Workloads auf einen weniger ausgelasteten Knoten verschieben können:

- Die weniger ausgelasteten Knoten im selben Cluster
- Die am wenigsten ausgelasteten Aggregate auf dem neuen Knoten

- Die leistungsstärksten Volumes auf dem aktuellen Knoten

Schritte

1. Identifizierung des am wenigsten ausgelasteten Knotens im Cluster:
   a. Auf der **Ereignis**-Detailseite wählen Sie den Namen des Clusters aus, in dem sich der Knoten befindet.

      Auf der Seite Performance/Cluster-Startseite sind die Clusterdetails zu sehen.

   b. Auf der Seite **Übersicht** erfolgt die Auswahl von **Knoten** im Bereich **Verwaltete Objekte**.

      Die Liste der Knoten in diesem Cluster wird angezeigt.

   c. Ein Klick auf die Spalte **Auslastung** sortiert die Knoten nach der geringsten Auslastung.

      Sie können auch diejenigen Knoten identifizieren, die über die größte **Free Capacity** verfügen. Dadurch erhalten Sie eine Liste potenzieller Knoten, auf die Sie Arbeitslasten verschieben könnten.

   d. Zu notieren ist der Name des Knotens, auf den Sie die Workloads verschieben möchten.
2. Das am wenigsten ausgelastete Aggregat auf dem neuen Knoten ist zu identifizieren:
   a. Im linken Navigationsbereich: **Storage** > **Aggregates**; im Menü Ansicht: **Performance** > **All Aggregates**.

      Die Ansicht „Performance: Alle Aggregate“ wird angezeigt.

   b. Unter **Filtering** wählen Sie im linken Dropdown-Menü **Node** aus, geben den Namen des Node in das Textfeld ein und klicken dann auf **Apply Filter**.

      Die Ansicht „Performance: Alle Aggregate“ wird erneut angezeigt und enthält die Liste der auf diesem Knoten verfügbaren Aggregate.

   c. Ein Klick auf die Spalte **Auslastung** sortiert die Aggregate nach der geringsten Auslastung.

      Sie können auch diejenigen Aggregate identifizieren, die über die größte **Free Capacity** verfügen. Dadurch erhalten Sie eine Liste potenzieller Aggregate, auf die Sie Workloads verschieben könnten.

   d. Zu notieren ist der Name des Aggregats, in das die Workloads verschoben werden sollen.
3. Identifizierung der leistungsstarken Workloads des Knotens, der das Ereignis empfangen hat:
   a. Zur **Event**-Detailseite für das Event zurückkehren.
   b. Im Feld **Betroffene Volumes** kann der Link für die Anzahl der Volumes ausgewählt werden.

      Die Ansicht „Performance: Alle Volumes“ zeigt eine gefilterte Liste der Volumes auf diesem Knoten an.

   c. Über die Spalte **Gesamtkapazität** können Sie die Volumes nach dem größten zugewiesenen Speicherplatz sortieren.

      Dadurch erhalten Sie eine Liste potenzieller Volumes, die Sie möglicherweise verschieben möchten.

   d. Zu notieren sind die Namen der Volumes, die verschoben werden sollen, sowie die Namen der aktuellen Aggregate, auf denen sie sich befinden.
4. Die Volumes werden auf die Aggregate verschoben, die Sie auf dem neuen Knoten als gering ausgelastet identifiziert haben.

Sie können den Verschiebevorgang mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools durchführen.

Nach einigen Tagen lässt sich prüfen, ob Sie von diesem Knoten oder Aggregat dieselbe Art von Ereignissen erhalten.

Verschieben von Workloads auf einen Knoten in einem anderen HA-Paar in Active IQ Unified Manager

Mit Unified Manager lässt sich ein Aggregat auf einem Knoten in einem anderen Hochverfügbarkeitspaar (HA-Paar) identifizieren, das über mehr freie Performance-Kapazität verfügt als das HA-Paar, auf dem Ihre Workloads derzeit ausgeführt werden. Anschließend lassen sich ausgewählte Volumes auf Aggregate im neuen HA-Paar verschieben.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Ihr Cluster muss aus mindestens zwei HA-Paaren bestehen

  Dieses Sanierungsverfahren ist nicht geeignet, wenn in Ihrem Cluster nur ein HA-Paar vorhanden ist.
- Die Namen der beiden Knoten im HA-Paar, bei denen derzeit ein Performanceproblem auftritt, müssen erfasst worden sein.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu denen die Knoten das Performance-Ereignis empfangen haben.
- Unified Manager muss Performance-Daten über einen Zeitraum von mindestens einem Monat erfasst und analysiert haben.

Durch die Verlagerung leistungsstarker Workloads auf ein Aggregat auf einem Knoten mit mehr freier Performance-Kapazität können Workloads auf beiden Knoten effizienter arbeiten. Dieses Verfahren hilft Ihnen dabei, die folgenden Ressourcen zu identifizieren, damit Sie leistungsstarke Workloads auf einen Knoten mit mehr freier Performance-Kapazität in einem anderen HA-Paar verschieben können:

- Die Knoten in einem anderen HA-Paar auf demselben Cluster, die über die größte freie Performancekapazität verfügen
- Die Aggregate auf den neuen Knoten mit der größten freien Performancekapazität
- Die leistungsstärksten Volumes auf den aktuellen Knoten

Schritte

1. Knoten identifizieren, die Teil eines anderen HA-Paars im selben Cluster sind:
   a. Auf der Seite **Ereignisdetails** wird der Name des Clusters ausgewählt, in dem sich die Knoten befinden.

      Auf der Seite Performance/Cluster-Startseite sind die Clusterdetails zu sehen.

   b. Auf der Seite **Übersicht** erfolgt die Auswahl von **Knoten** im Bereich **Verwaltete Objekte**.

      Die Liste der Knoten in diesem Cluster wird in der Ansicht „Performance: Alle Knoten“ angezeigt.

   c. Zu notieren sind die Namen der Knoten, die sich in anderen HA-Paaren befinden als in dem HA-Paar,

bei dem derzeit ein Performance-Problem auftritt.

2. Es ist der Knoten im neuen HA-Paar mit der größten freien Performancekapazität zu identifizieren:
   a. In der Ansicht **Performance: All Nodes** lässt sich durch Klicken auf die Spalte **Performance Capacity Used** eine Sortierung der Knoten nach der niedrigsten prozentualen Auslastung vornehmen.

      Dies bietet eine Liste potenzieller Knoten, auf die Sie Arbeitslasten verschieben könnten.

   b. Sie notieren den Namen des Knotens in einem anderen HA-Paar, auf den Sie die Workloads verschieben möchten.
3. Es ist ein Aggregat auf dem neuen Knoten mit der größten freien Performance-Kapazität zu ermitteln:
   a. In der Ansicht **Performance: Alle Knoten** erfolgt die Auswahl des Knotens.

      Die Knotendetails sind auf der Seite „Performance/Node Explorer“ zu sehen.

   b. Im Menü **Anzeigen und Vergleichen** steht **Aggregate auf diesem Knoten** zur Auswahl.

      Die Aggregate dieses Knotens sind im Raster aufgeführt.

   c. Ein Klick auf die Spalte **Genutzte Performance-Kapazität** sortiert die Aggregate nach der geringsten Auslastung.

      Dies bietet eine Liste potenzieller Aggregate, auf die Sie Workloads verschieben könnten.

   d. Zu notieren ist der Name des Aggregats, in das die Workloads verschoben werden sollen.
4. Leistungsstarke Workloads der Knoten, die das Ereignis empfangen haben:
   a. Zur **Event**-Detailseite für das Event zurückkehren.
   b. Im Feld **Betroffene Volumes** erfolgt die Auswahl des Links für die Anzahl der Volumes des ersten Knotens.

      Die Ansicht „Performance: Alle Volumes“ zeigt eine gefilterte Liste der Volumes auf diesem Knoten an.

   c. Über die Spalte **Gesamtkapazität** können Sie die Volumes nach dem größten zugewiesenen Speicherplatz sortieren.

      Dies bietet eine Liste potenzieller Volumes, die Sie möglicherweise verschieben möchten.

   d. Zu notieren sind die Namen der Volumes, die verschoben werden sollen, sowie die Namen der aktuellen Aggregate, auf denen sie sich befinden.
   e. Die Schritte 4c und 4d sind auch für den zweiten Knoten auszuführen, der Teil dieses Ereignisses war, um mögliche Volumes zu identifizieren, die ebenfalls von diesem Knoten verschoben werden sollen.
5. Die Volumes sollten auf die Aggregate verschoben werden, die Sie auf dem neuen Knoten als diejenigen mit der größten freien Performance Kapazität identifiziert haben.

   Sie können den Verschiebevorgang mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools durchführen.

Nach einigen Tagen lässt sich prüfen, ob Sie von diesem Knoten oder Aggregat dieselbe Art von Ereignissen erhalten.

Verschieben von Workloads auf einen anderen Knoten in einem anderen HA-Paar in Active IQ Unified Manager

Mit Unified Manager können Sie ein Aggregat auf einem Knoten in einem anderen HA-Paar identifizieren, das weniger ausgelastet ist als das HA-Paar, auf dem Ihre Workloads derzeit ausgeführt werden. Anschließend können Sie ausgewählte Volumes auf Aggregate im neuen HA-Paar verschieben. Wenn leistungsstarke Workloads auf ein Aggregat auf einem weniger ausgelasteten Knoten verschoben werden, können die Workloads auf beiden Knoten effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Ihr Cluster muss aus mindestens zwei HA-Paaren bestehen; dieser Behebungsprozess kann nicht verwendet werden, wenn Ihr Cluster nur ein HA-Paar hat.
- Sie müssen die Namen der beiden Knoten im HA-Paar notiert haben, bei denen derzeit das Performanceproblem besteht.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu denen die Knoten das Performance-Ereignis empfangen haben.
- Unified Manager muss Performance-Daten von mindestens einem Monat erfasst und analysiert haben.

Diese Schritte helfen Ihnen, die folgenden Ressourcen zu identifizieren, damit Sie leistungsstarke Workloads auf einen weniger ausgelasteten Knoten eines anderen HA-Paares verschieben können:

- Die Knoten in einem anderen HA-Paar auf demselben Cluster, die weniger ausgelastet sind
- Die am wenigsten ausgelasteten Aggregate auf den neuen Knoten
- Die leistungsstärksten Volumes auf den aktuellen Knoten

Schritte

1. Knoten identifizieren, die Teil eines anderen HA-Paars im selben Cluster sind:
   a. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Clusters**; im Menü Ansicht die von **Performance** > **All Clusters**.

      Die Ansicht „Performance: All Clusters“ wird angezeigt.

   b. Für den aktuellen Cluster die Zahl im Feld **Knotenanzahl** auswählen.

      Die Ansicht „Performance: Alle Knoten“ wird angezeigt.

   c. Zu notieren sind die Namen der Knoten, die sich in anderen HA-Paaren befinden als in dem HA-Paar, bei dem aktuell das Performance Problem auftritt.
2. Im neuen HA-Paar ist der am wenigsten ausgelastete Knoten zu identifizieren:
   a. Ein Klick auf die Spalte **Auslastung** sortiert die Knoten nach der geringsten Auslastung.

      Sie können auch diejenigen Knoten identifizieren, die über die größte **Free Capacity** verfügen. Dadurch erhalten Sie eine Liste potenzieller Knoten, auf die Sie Arbeitslasten verschieben könnten.

   b. Zu notieren ist der Name des Knotens, auf den Sie die Workloads verschieben möchten.
3. Das am wenigsten ausgelastete Aggregat auf dem neuen Knoten ist zu identifizieren:

a. Im linken Navigationsbereich: **Storage** > **Aggregates**; im Menü Ansicht: **Performance** > **All Aggregates**.

   Die Ansicht „Performance: Alle Aggregate“ wird angezeigt.

b. Unter **Filtering** wählen Sie im linken Dropdown-Menü **Node** aus, geben den Namen des Node in das Textfeld ein und klicken dann auf **Apply Filter**.

   Die Ansicht „Performance: Alle Aggregate“ wird erneut angezeigt und enthält die Liste der auf diesem Knoten verfügbaren Aggregate.

c. Ein Klick auf die Spalte **Auslastung** sortiert die Aggregate nach der geringsten Auslastung.

   Sie können auch diejenigen Aggregate identifizieren, die über die größte **Free Capacity** verfügen. Dadurch erhalten Sie eine Liste potenzieller Aggregate, auf die Sie Workloads verschieben könnten.

d. Zu notieren ist der Name des Aggregats, in das die Workloads verschoben werden sollen.

4. Leistungsstarke Workloads der Knoten, die das Ereignis empfangen haben:
   a. Zur **Event**-Detailseite für das Event zurückkehren.
   b. Im Feld **Betroffene Volumes** erfolgt die Auswahl des Links für die Anzahl der Volumes des ersten Knotens.

      Die Ansicht „Performance: Alle Volumes“ zeigt eine gefilterte Liste der Volumes auf diesem Knoten an.

   c. Über die Spalte **Gesamtkapazität** können Sie die Volumes nach dem größten zugewiesenen Speicherplatz sortieren.

      Dies bietet eine Liste potenzieller Volumes, die Sie möglicherweise verschieben möchten.

   d. Zu notieren sind die Namen der Volumes, die verschoben werden sollen, sowie die Namen der aktuellen Aggregate, auf denen sie sich befinden.
   e. Die Schritte 4c und 4d sind auch für den zweiten Knoten auszuführen, der Teil dieses Ereignisses war, um mögliche Volumes zu identifizieren, die ebenfalls von diesem Knoten verschoben werden sollen.
5. Die Volumes werden auf die Aggregate verschoben, die Sie auf dem neuen Knoten als gering ausgelastet identifiziert haben.

   Sie können den Verschiebevorgang mit ONTAP System Manager, OnCommand Workflow Automation, ONTAP Befehlen oder einer Kombination dieser Tools durchführen.

Nach einigen Tagen lässt sich prüfen, ob Sie von diesem Knoten oder Aggregat dieselbe Art von Ereignissen erhalten.

QoS Richtlinieneinstellungen können zur Priorisierung von Node Workloads in Active IQ Unified Manager verwendet werden.

Sie können für eine QoS-Richtliniengruppe ein Limit festlegen, um die E/A-Leistung pro Sekunde (IOPS) oder die MBps-Durchsatzbegrenzung für die darin enthaltenen Workloads zu steuern. Befinden sich Workloads in einer Richtliniengruppe ohne festgelegtes Limit, z. B. der Standardrichtliniengruppe, oder entspricht das festgelegte Limit nicht Ihren Anforderungen, können Sie das Limit erhöhen oder die Workloads in eine neue oder vorhandene Richtliniengruppe mit dem gewünschten Limit verschieben.

Wenn ein Performance Ereignis auf einem Knoten dadurch verursacht wird, dass Workloads die Knotenressourcen übermäßig nutzen, wird in der Ereignisbeschreibung auf der Seite „Ereignisdetails“ ein Link zur Liste der beteiligten Volumes angezeigt. Auf der Seite „Performance/Volumes“ lassen sich die betroffenen Volumes nach IOPS und MBps sortieren, sodass erkennbar wird, welche Workloads die höchste Auslastung aufweisen und möglicherweise zu dem Ereignis beigetragen haben.

Durch die Zuweisung der Volumes, die die Knotenressourcen übermäßig beanspruchen, zu einer restriktiveren Richtliniengruppeneinstellung drosselt die Richtliniengruppe die Workloads und schränkt damit deren Aktivität ein, wodurch sich die Ressourcennutzung auf diesem Knoten verringern kann.

Sie können ONTAP System Manager oder die ONTAP Befehle verwenden, um Richtliniengruppen zu verwalten, einschließlich der folgenden Aufgaben:

- Erstellen einer Richtliniengruppe
- Hinzufügen oder Entfernen von Workloads in einer Richtliniengruppe
- Verschieben einer Workload zwischen Richtliniengruppen
- Ändern der Durchsatzbegrenzung einer Richtliniengruppe

Entfernen inaktiver Volumes und LUNs in Active IQ Unified Manager

Wenn freier Speicherplatz im Aggregat als Problem erkannt wurde, können Sie nach ungenutzten Volumes und LUNs suchen und diese aus dem Aggregat löschen. Dies kann dazu beitragen, das Problem des geringen Festplattenspeichers zu entschärfen.

Wenn ein Performance-Ereignis auf einem Aggregat durch niedrigen Festplattenspeicher verursacht wird, gibt es mehrere Möglichkeiten, um festzustellen, welche Volumes und LUNs nicht mehr verwendet werden.

Zur Identifizierung ungenutzter Volumes:

- Auf der Seite mit den Ereignisdetails enthält das Feld **Anzahl der betroffenen Objekte** einen Link, der die Liste der betroffenen Volumes anzeigt.

  Über den Link werden die Volumes in der Ansicht „Performance: All Volumes“ angezeigt. Von dort aus lassen sich die betroffenen Volumes nach **IOPS** sortieren, sodass erkennbar ist, welche Volumes nicht aktiv waren.

Identifizierung ungenutzter LUNs:

1. Auf der Seite mit den Ereignisdetails ist der Name des Aggregats, auf dem das Ereignis aufgetreten ist, zu notieren.
2. Im linken Navigationsbereich wählen Sie **Storage** > **LUNs** aus und dann im Menü Ansicht **Performance** > **Alle LUNs**.
3. Unter **Filtering** wird im linken Dropdown-Menü **Aggregate** ausgewählt, der Name des Aggregats in das Textfeld eingegeben und anschließend auf **Apply Filter** geklickt.
4. Zur Anzeige der inaktiven LUNs lässt sich die resultierende Liste der betroffenen LUNs nach **IOPS** sortieren.

Nachdem Sie die nicht verwendeten Volumes und LUNs identifiziert haben, können Sie diese Objekte mit ONTAP System Manager oder den ONTAP Befehlen löschen.

Grundlegende Informationen dazu, wie sich das Hinzufügen von Datenträgern auf das Aggregatlayout in Active IQ Unified Manager auswirkt

Sie können einem Aggregat Festplatten hinzufügen, um die Storage Kapazität und die Performance dieses Aggregats zu erhöhen. Nach dem Hinzufügen der Festplatten zeigt sich eine Verbesserung der Performance erst nach der Rekonstruktion des Aggregats.

Wenn auf der Seite „Ereignisdetails“ ein systemdefiniertes Schwellenwertereignis angezeigt wird, enthält die Ereignisbeschreibung den Namen des betroffenen Aggregats. Sie können Datenträger hinzufügen und die Daten auf diesem Aggregat rekonstruieren.

Die dem Aggregat hinzugefügten Datenträger müssen bereits im Cluster vorhanden sein. Falls im Cluster keine zusätzlichen Datenträger verfügbar sind, ist möglicherweise eine Kontaktaufnahme mit Ihrem Administrator oder der Erwerb weiterer Datenträger erforderlich. Sie können ONTAP System Manager oder die ONTAP-Befehle verwenden, um Datenträger zu einem Aggregat hinzuzufügen.

"Technischer Bericht 3838: Konfigurationsleitfaden für das Speichersubsystem"

Einrichten einer Verbindung zwischen einem Unified Manager Server und einem externen Datenanbieter

Einrichten einer Verbindung zwischen Active IQ Unified Manager und einem externen Datenanbieter

Eine Verbindung zwischen einem Unified Manager Server und einem externen Datenanbieter ermöglicht es Ihnen, Cluster Performance-Daten an einen externen Server zu senden, sodass Storage Manager die Performance-Kennzahlen mithilfe von Drittanbietersoftware grafisch darstellen können.

Eine Verbindung zwischen einem Unified Manager Server und einem externen Daten-Provider wird über die Menüoption „`External Data Provider`“ in der Wartungs-Managementplattform eingerichtet.

Übertragung von Active IQ Unified Manager Leistungsdaten an einen externen Server

Unified Manager erfasst eine Vielzahl von Performance-Daten von allen Clustern, die es überwacht. Bestimmte Datengruppen können an einen externen Server gesendet werden.

Je nachdem, welche Performance Daten Sie grafisch darstellen möchten, können Sie auswählen, eine der folgenden Gruppen von Statistiken zu senden:

Statistikengruppe	Enthaltene Daten	Details
Performance Monitor	Übergeordnete Performance Statistiken für die folgenden Objekte: • LUNs • Volumes	Diese Gruppe liefert die Gesamt-IOPS oder die Latenz für alle LUNs und Volumes in allen überwachten Clustern. Diese Gruppe liefert die geringste Anzahl an Statistiken.
Ressourcennutzung	Statistiken zur Ressourcenauslastung für die folgenden Objekte: • Nodes • Aggregate	Diese Gruppe liefert Nutzungsstatistiken für die Knoten und die physischen Ressourcen der Aggregate in allen überwachten Clustern. Es liefert außerdem die in der Gruppe „Performance Monitor“ erfassten Statistiken.
Detailanalyse	Niedrigstufige Statistiken zu lesen/schreiben und pro Protokoll für alle verfolgten Objekte: • Nodes • Aggregate • LUNs • Volumes • Festplatten • LIFs • Anschlüsse/Netzwerkkarten	Diese Gruppe liefert lesen/schreiben- und Aufschlüsselungen nach Protokoll für alle sieben verfolgten Objekttypen in allen überwachten Clustern. Außerdem stellt es die Statistiken bereit, die in der Gruppe „Performance Monitor“ und in der Gruppe „Ressourcennutzung“ erfasst werden. Diese Gruppe liefert die größte Anzahl von Statistiken.

Wenn der Name eines Clusters oder Clusterobjekts auf dem Storage-System geändert wird, enthalten sowohl das alte als auch das neue Objekt Performance-Daten auf dem externen Server (als “metric_path” bezeichnet). Die beiden Objekte gelten nicht als dasselbe Objekt. Wenn beispielsweise der Name eines Volumes von “volume1_acct” in “acct_vol1” geändert wird, sind die alten Performance-Daten für das alte Volume und die neuen Performance-Daten für das neue Volume zu sehen.

Die Liste aller Performance-Zähler, die an einen externen Datenanbieter gesendet werden können, ist im Knowledge Base Artikel 30096 aufgeführt.

"Unified Manager Performance-Zähler, die zu einem External Data Provider exportiert werden können"

Graphite so konfigurieren, dass Leistungsdaten von Active IQ Unified Manager empfangen werden

Graphite ist ein offenes Softwaretool zur Erfassung und grafischen Darstellung von Performancedaten aus Computersystemen. Ihr Graphite Server und Ihre Software müssen korrekt konfiguriert sein, um statistische Daten von Unified Manager zu

empfangen.

NetApp testet oder verifiziert keine spezifischen Versionen von Graphite oder anderen Tools von Drittanbietern.

Der Graphite Server empfängt keine Performance-Daten für Volumes von Unified Manager.

Nachdem Sie Graphite gemäß der Installationsanleitung installiert haben, müssen Sie die folgenden Änderungen vornehmen, um den statistischen Datentransfer von Unified Manager zu unterstützen:

- In der `/opt/graphite/conf/carbon.conf`Datei muss die maximale Anzahl der Dateien, die pro Minute auf dem Graphite-Server erstellt werden können, auf *200* (**MAX_CREATES_PER_MINUTE = 200**`) festgelegt werden.

  Abhängig von der Anzahl der Cluster in Ihrer Konfiguration und den Statistikobjekten, die Sie zum Senden ausgewählt haben, müssen möglicherweise zunächst Tausende neuer Dateien erstellt werden. Bei 200 Dateien pro Minute kann es 15 Minuten oder länger dauern, bis alle Metrikdateien zunächst erstellt sind. Sobald alle eindeutigen Metrikdateien erstellt wurden, ist dieser Parameter nicht mehr relevant.

- Wenn Sie Graphite auf einem Server ausführen, der mit einer IPv6-Adresse bereitgestellt wurde, muss der Wert für LINE_RECEIVER_INTERFACE in der `/opt/graphite/conf/carbon.conf` Datei von "0.0.0.0" in "::" geändert werden (**`LINE_RECEIVER_INTERFACE = ::`**)
- In der Datei `/opt/graphite/conf/storage-schemas.conf` muss der Parameter `retentions` verwendet werden, um die Frequenz auf 5 Minuten und die Aufbewahrungsdauer auf die für Ihre Umgebung relevante Anzahl von Tagen einzustellen.

  Die Aufbewahrungsdauer kann so lang sein, wie es Ihre Umgebung zulässt, aber für mindestens eine Aufbewahrungseinstellung muss als Häufigkeitswert 5 Minuten festgelegt sein. Im folgenden Beispiel wird ein Abschnitt für Unified Manager mithilfe des `pattern` Parameters definiert, und die Werte legen die anfängliche Häufigkeit auf 5 Minuten und die Aufbewahrungsdauer auf 100 Tage fest: **`[OPM]`**

  ```
  pattern = ^netapp-performance\..

  retentions = 5m:100d
  ```

  Wenn das Standard-Vendor-Tag von "netapp-performance" in ein anderes geändert wird, muss diese Änderung auch im `pattern` Parameter berücksichtigt werden.

Wenn der Graphite-Server nicht verfügbar ist, während der Unified Manager Server versucht, Performance-Daten zu senden, werden die Daten nicht gesendet, und es entsteht eine Lücke in den erfassten Daten.

Eine Verbindung zwischen Active IQ Unified Manager und einem externen Datenanbieter wird konfiguriert.

Unified Manager kann Cluster Performance Daten an einen externen Server senden. Sie können die Art der gesendeten Statistikdaten und das Sendeintervall festlegen.

Bevor Sie beginnen

- Sie benötigen eine Benutzerkennung, die zur Anmeldung an der Wartungs-Managementplattform des Unified Manager Servers berechtigt.

- Sie benötigen folgende Informationen über den externen Datenanbieter:
  - Servername oder IP-Adresse (IPv4 oder IPv6)
  - Standardport des Servers (falls nicht der Standardport 2003 verwendet wird)
- Sie müssen den Remote-Server und die Drittanbietersoftware so konfiguriert haben, dass sie statistische Daten vom Unified Manager Server empfangen können.
- Wichtig ist, welche Gruppe von Statistiken gesendet werden soll:
  - PERFORMANCE_INDICATOR: Performance Monitor Statistiken
  - RESSOURCENNUTZUNG: Ressourcennutzung und Performance Monitor Statistiken
  - DRILL_DOWN: Alle Statistiken
- Sie müssen das Zeitintervall kennen, in dem Sie Statistiken übertragen möchten: 5, 10 oder 15 Minuten.

  Unified Manager erfasst standardmäßig Statistiken im 5-Minuten-Takt. Wenn Sie das Übertragungsintervall auf 10 (oder 15) Minuten einstellen, ist die Datenmenge, die bei jeder Übertragung gesendet wird, zwei- bzw. dreimal so groß wie bei Verwendung des standardmäßigen 5-Minuten-Intervalls.

  Wenn Sie das Unified Manager Performance-Erfassungsintervall auf 10 oder 15 Minuten ändern, müssen Sie das Übertragungsintervall so ändern, dass es dem Unified Manager Erfassungsintervall entspricht oder größer ist.

Sie können eine Verbindung zwischen einem Unified Manager Server und einem externen Datenprovider-Server konfigurieren.

Schritte

1. Die Anmeldung an der Managementplattform des Unified Manager Servers erfolgt als Wartungsbenutzer.

   Die Eingabeaufforderungen der Unified Manager Wartungsmanagementplattform werden angezeigt.

2. Geben Sie in der Wartungs-Managementplattform die Nummer der Menüoption **External Data Provider** ein.

   Das Menü „External Server Connection“ wird angezeigt.

3. Die Nummer der Menüoption **Add/Modify Server Connection** eingeben.

   Die aktuellen Serververbindungsinformationen werden angezeigt.

4. Bei entsprechender Aufforderung `y` eingeben, um fortzufahren.
5. Bei Aufforderung erfolgt die Eingabe der IP-Adresse oder des Namens des Zielservers sowie der Informationen zum Server-Port, sofern diese vom Standardport 2003 abweichen.
6. Wenn Sie dazu aufgefordert werden, können Sie `y` eingeben, um zu überprüfen, dass die eingegebenen Informationen korrekt sind.
7. Mit einer beliebigen Taste kehren Sie zum Menü „Externe Serververbindung“ zurück.
8. Eingabe der Nummer der Menüoption **Serverkonfiguration ändern**.

   Die Informationen zur aktuellen Serverkonfiguration werden angezeigt.

9. Bei entsprechender Aufforderung `y` eingeben, um fortzufahren.
10. Wenn eine entsprechende Aufforderung angezeigt wird, geben Sie den Typ der zu sendenden Statistiken,

das Zeitintervall, in dem die Statistiken gesendet werden, sowie an, ob die Übertragung der Statistiken jetzt aktiviert werden soll:

Für..	Eingeben…
Statistikengruppe-ID	`0` - PERFORMANCE_INDICATOR (Standard) `1` - RESSOURCENNUTZUNG `2` - DRILL_DOWN
Anbieter-Tag	Ein aussagekräftiger Name für den Ordner, in dem die Statistiken auf dem externen Server gespeichert werden. “netapp-performance” ist der Standardname, Sie können aber auch einen anderen Wert eingeben. Mithilfe der Punktnotation lässt sich eine hierarchische Ordnerstruktur definieren. Beispielsweise befinden sich die Statistiken nach der Eingabe **`stats.performance.netapp`** unter **stats** > **performance** > **netapp**.
Sendeintervall	`5` (Standardeinstellung), `10`, oder `15` Minuten
Aktivieren/Deaktivieren	`0` - Deaktivieren `1` - Aktivieren (Standard)

11. Wenn Sie dazu aufgefordert werden, können Sie **`y`** eingeben, um zu überprüfen, dass die eingegebenen Informationen korrekt sind.
12. Mit einer beliebigen Taste kehren Sie zum Menü „Externe Serververbindung“ zurück.
13. Zum Verlassen der Wartungs-Managementplattform **`x`** eingeben.

Nachdem Sie die Verbindung konfiguriert haben, werden die ausgewählten Performance-Daten in dem von Ihnen angegebenen Zeitintervall an den Zielserver gesendet. Es dauert einige Minuten, bis die Metriken im externen Tool angezeigt werden. Möglicherweise müssen Sie Ihren Browser aktualisieren, um die neuen Metriken in der Metrikhierarchie zu sehen.

Überwachen und Managen des Cluster-Systemstatus

Einführung in die Systemstatusüberwachung von Active IQ Unified Manager

Informationen zur Zustandsüberwachung von Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) ermöglicht die Überwachung einer großen Anzahl von Systemen mit ONTAP-Software über eine zentrale Benutzeroberfläche. Die Unified Manager Serverinfrastruktur bietet Skalierbarkeit, Supportfähigkeit sowie erweiterte Überwachungs- und Benachrichtigungsfunktionen.

Zu den wichtigsten Funktionen des Unified Manager gehören Überwachung, Alarmierung, das Managen der Verfügbarkeit und Kapazität von Clustern, das Managen der Schutzfunktionen sowie die Bündelung von Diagnosedaten und deren Weiterleitung an den technischen Support.

Mit Unified Manager können Sie Ihre Cluster überwachen. Wenn Probleme im Cluster auftreten, benachrichtigt Sie Unified Manager über Ereignisse mit detaillierten Informationen zu diesen Problemen. Einige Ereignisse bieten Ihnen auch Abhilfemaßnahmen, mit denen Sie die Probleme beheben können. Sie können Warnmeldungen für Ereignisse konfigurieren, sodass Sie bei Problemen per E-Mail und SNMP-Traps benachrichtigt werden.

Mit Unified Manager können Sie Storage Objekte in Ihrer Umgebung managen, indem Sie sie mit Annotationen verknüpfen. Sie können benutzerdefinierte Annotationen erstellen und Cluster, Storage Virtual Machines (SVMs) und Volumes dynamisch über Regeln mit den Annotationen verknüpfen.

Sie können auch die Storage-Anforderungen Ihrer Clusterobjekte anhand der Informationen in den Kapazitäts- und Systemstatusdiagrammen für das jeweilige Clusterobjekt planen.

Physische und logische Kapazität

Unified Manager verwendet für ONTAP Storage Objekte die Konzepte des physischen und logischen Speicherplatzes.

- Physische Kapazität: Der physische Speicherplatz bezieht sich auf die physischen Blöcke des Storage, die im Volume verwendet werden. „Genutzte physische Kapazität“ ist typischerweise kleiner als die genutzte logische Kapazität, da Daten durch Storage-Effizienzfunktionen (wie Deduplizierung und Komprimierung) reduziert werden.
- Logische Kapazität: Logischer Speicherplatz bezeichnet den nutzbaren Speicherplatz (die logischen Blöcke) in einem Volume. Logischer Speicherplatz bezieht sich darauf, wie theoretischer Speicherplatz genutzt werden kann, ohne die Ergebnisse von Deduplizierung oder Komprimierung zu berücksichtigen. „Genutzter logischer Speicherplatz“ ist der genutzte physische Speicherplatz zuzüglich der Einsparungen durch konfigurierte Storage-Effizienzfunktionen (wie Deduplizierung und Komprimierung). Dieser Wert erscheint oft höher als die genutzte physische Kapazität, da er die Datenkomprimierung und andere Verringerungen des physischen Speicherplatzes nicht widerspiegelt. Daher könnte die gesamte logische Kapazität höher sein als der bereitgestellte Speicherplatz.

Kapazitätsmaßeinheiten

Unified Manager berechnet die Storage-Kapazität auf der Grundlage binärer Einheiten von 1024 (2^{10}) Byte. In ONTAP 9.10.0 und früheren Versionen wurden diese Einheiten als KB, MB, GB, TB und PB angezeigt. Ab ONTAP 9.10.1 werden sie in Unified Manager als KiB, MiB, GiB, TiB und PiB angezeigt.

Die für den Datendurchsatz verwendeten Einheiten sind weiterhin Kilobyte pro Sekunde (Kbps), Megabyte pro Sekunde (Mbps), Gigabyte pro Sekunde (Gbit/s), Terabyte pro Sekunde (Tbps) usw. für alle Releases von ONTAP.

Im Unified Manager für ONTAP 9.10.0 und frühere Versionen angezeigte Kapazitätseinheit	In Unified Manager für ONTAP 9.10.1 angezeigte Kapazitätseinheit	Berechnung	Wert in Bytes
KB	KiB	1024	1024 Bytes
MB	MiB	1024 * 1024	1.048.576 Bytes
GB	GiB	1024 * 1024 * 1024	1.073.741.824 Bytes
TB	TiB	1024 * 1024 * 1024 * 1024	1.099.511.627.776 Bytes

Die Funktionen zur Zustandsüberwachung von Active IQ Unified Manager verstehen

Unified Manager basiert auf einer Serverinfrastruktur, die Skalierbarkeit, Supportfähigkeit sowie erweiterte Überwachungs- und Benachrichtigungsfunktionen bietet. Unified Manager unterstützt die Überwachung von Systemen, auf denen ONTAP-Software ausgeführt wird.

Unified Manager umfasst folgende Funktionen:

- Identifizierung, Überwachung und Benachrichtigungen für Systeme, auf denen ONTAP Software installiert ist:
  - Physische Objekte: Knoten, Festplatten, Shelves, SFO-Paare, Ports und Flash Cache
  - Logische Objekte: Cluster, Storage Virtual Machines (SVMs), Aggregate, Volumes, LUNs, Namespaces, Qtrees, LIFs, Snapshot-Kopien, Verbindungspfade, NFS-Freigaben, SMB-Freigaben, Benutzer- und Gruppenquoten, QoS-Richtliniengruppen und Initiatorgruppen
  - Protokolle: CIFS, NFS, FC, iSCSI, NVMe und FCoE
  - Storage-Effizienz: SSD-Aggregate, Flash Pool Aggregate, FabricPool Aggregate, Deduplizierung und Komprimierung
  - Schutz: SnapMirror Beziehungen (synchron und asynchron) und SnapVault Beziehungen
- Anzeige des Cluster-Identifizierungs- und Überwachungsstatus
- MetroCluster über FC- und IP-Konfigurationen: Anzeige und Überwachung der Konfiguration, von Problemen und des Verbindungsstatus der Clusterkomponenten. MetroCluster Switches und Bridges für MetroCluster über FC-Konfigurationen
- Erweiterte Infrastruktur für Warnmeldungen, Ereignisse und Schwellenwerte

- LDAP-, LDAPS- und SAML-Authentifizierung sowie Unterstützung für lokale Benutzer
- RBAC (für einen vordefinierten Satz von Rollen)
- AutoSupport und Support Bundle
- Verbessertes Dashboard zur Anzeige des Kapazitäts-, Verfügbarkeits-, Schutz- und Performance-Systemstatus der Umgebung
- Interoperabilität von Volume-Verschiebungen, Verlauf von Volume-Verschiebungen und Änderungsverlauf von Verbindungspfaden
- Der Bereich „Scope of Impact“ zeigt grafisch die Ressourcen an, die von Ereignissen wie Some Failed Disks, MetroCluster Aggregate Mirroring Degraded und MetroCluster Spare Disks Left Behind betroffen sind
- Bereich „Mögliche Auswirkungen“, der die Auswirkungen der MetroCluster Ereignisse anzeigt
- Der Bereich „Vorgeschlagene Korrekturmaßnahmen“ zeigt die Aktionen an, die zur Behebung von Ereignissen wie Einige ausgefallene Festplatten, MetroCluster Verschlechterte Aggregatspiegelung und MetroCluster Zurückgelassene Ersatzfestplatten durchgeführt werden können
- Der Bereich „Möglicherweise betroffene Ressourcen“ zeigt die Ressourcen an, die bei Ereignissen wie dem „Volume Offline“-Ereignis, dem „Volume Restricted“-Ereignis und dem Ereignis „Thin-Provisioned Volume Space At Risk“ betroffen sein könnten.
- Unterstützung für SVMs mit FlexVol oder FlexGroup Volumes
- Unterstützung für die Überwachung von Knoten-Root-Volumes
- Erweiterte Überwachung von Snapshot Kopien, einschließlich der Berechnung des wiederverwendbaren Speicherplatzes und des Löschens von Snapshot Kopien
- Anmerkungen für Storage-Objekte
- Erstellung und Verwaltung von Berichten über Informationen zu Storage Objekten wie physische und logische Kapazität, Auslastung, Speicherplatzeinsparungen, Performance und zugehörige Ereignisse
- Integration mit OnCommand Workflow Automation zur Ausführung von Workflows

  "WFA-Download"

Active IQ Unified Manager Schnittstellen dienen zur Verwaltung des Zustands des Speichersystems.

Diese Abschnitte enthalten Informationen zu den beiden Benutzeroberflächen, die Active IQ Unified Manager zur Fehlerbehebung bei Problemen mit Datenspeicherkapazität, Verfügbarkeit und Schutz bereitstellt. Die beiden Benutzeroberflächen sind die Unified Manager Weboberfläche und die Managementplattform.

Wenn Sie die Schutzfunktionen in Unified Manager nutzen möchten, müssen Sie auch OnCommand Workflow Automation (WFA) installieren und konfigurieren.

Unified Manager Web-Benutzeroberfläche

Die Web-Benutzeroberfläche von Unified Manager ermöglicht es einem Administrator, Clusterprobleme im Zusammenhang mit Storage-Kapazität, Verfügbarkeit und Schutz von Daten zu überwachen und zu beheben.

In diesen Abschnitten werden einige gängige Arbeitsabläufe beschrieben, denen ein Administrator folgen kann, um Probleme mit der Storage-Kapazität, der Datenverfügbarkeit oder dem Schutz zu beheben, die in der Unified Manager Weboberfläche angezeigt werden.

Managementplattform

Die Managementplattform von Unified Manager ermöglicht es Administratoren, Betriebssystemprobleme, Probleme bei Versionsaktualisierungen, Benutzerzugriffsprobleme und Netzwerkprobleme im Zusammenhang mit dem Unified Manager Server zu überwachen, zu diagnostizieren und zu beheben. Wenn die Web-Benutzeroberfläche von Unified Manager nicht verfügbar ist, ist die Managementplattform die einzige Zugriffsmöglichkeit auf Unified Manager.

Mithilfe dieser Informationen können Sie auf die Wartungs-Managementplattform zugreifen und damit Probleme im Zusammenhang mit der Funktionsweise des Unified Manager-Servers beheben.

Management und Überwachung von Clustern und des Systemstatus von Clusterobjekten

Clusterüberwachung verstehen

Clusterüberwachung in Active IQ Unified Manager verstehen

Sie können der Unified Manager Datenbank Cluster hinzufügen, um Cluster hinsichtlich Verfügbarkeit, Kapazität und anderer Details wie CPU-Auslastung, Schnittstellenstatistiken, freiem Festplattenspeicher, qtree Nutzung und Umgebungsdaten des Chassis zu überwachen.

Ereignisse werden generiert, wenn der Status anormal ist oder ein vordefinierter Schwellenwert überschritten wird. Sofern dies konfiguriert ist, sendet Unified Manager eine Benachrichtigung an einen festgelegten Empfänger, wenn ein Ereignis eine Warnung auslöst.

Informationen zu Node Root Volumes in Active IQ Unified Manager

Sie können das Root-Volume des Knotens mit Unified Manager überwachen. Es empfiehlt sich, dass das Root-Volume des Knotens über ausreichend Kapazität verfügt, um einen Ausfall des Knotens zu verhindern.

Wenn die genutzte Kapazität des Node-Root-Volumes 80 Prozent der gesamten Kapazität des Node-Root-Volumes überschreitet, wird das Ereignis „Node Root Volume Space Nearly Full“ generiert. Sie können eine Warnung für das Ereignis konfigurieren, um eine Benachrichtigung zu erhalten. Sie können mithilfe von ONTAP System Manager oder der ONTAP CLI geeignete Maßnahmen ergreifen, um zu verhindern, dass der Node ausfällt.

Die Funktionalität zur Überwachung von Knoten-Root-Volumes ist nicht verfügbar, wenn Cluster ONTAP Version 9.14.1 oder höher ausführen.

Ereignisse und Schwellenwerte für Node-Root-Aggregate in Active IQ Unified Manager

Sie können das Root-Aggregat des Knotens mit Unified Manager überwachen. Es empfiehlt sich, das Root-Volume im Root-Aggregat per Thick Provisioning zu provisionieren, um zu verhindern, dass der Knoten angehalten wird.

Standardmäßig werden für Root-Aggregate keine Kapazitäts- und Performance-Ereignisse generiert. Auch die von Unified Manager verwendeten Schwellenwerte gelten nicht für die Root-Aggregate der Nodes. Nur ein

Mitarbeiter des technischen Supports kann die Einstellungen für die Generierung dieser Ereignisse ändern. Wenn die Einstellungen von einem Mitarbeiter des technischen Supports geändert werden, werden die Kapazitätsschwellenwerte auf das Root-Aggregat des Nodes angewendet.

Sie können geeignete Maßnahmen ergreifen, um ein Anhalten des Knotens zu verhindern, indem Sie entweder ONTAP System Manager oder die ONTAP CLI verwenden.

Die Funktionalität zur Überwachung von Knoten-Root-Aggregaten ist nicht verfügbar, wenn Cluster mit ONTAP Version 9.14.1 oder höher ausgeführt werden.

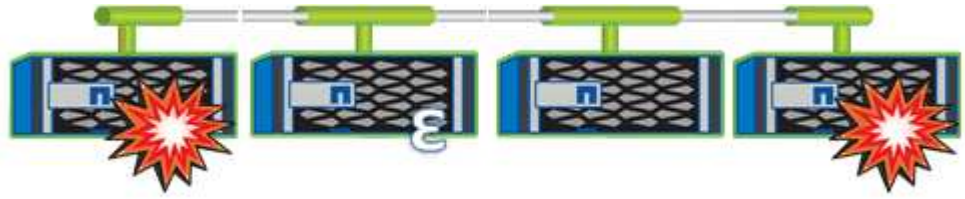
Quorum und Epsilon in ONTAP Clustern in Active IQ Unified Manager verstehen

Quorum und Epsilon sind wichtige Kennzahlen für die Gesundheit und Funktionsfähigkeit eines Clusters, die zusammen angeben, wie Cluster potenzielle Kommunikations- und Konnektivitätsherausforderungen adressieren.

Quorum ist eine Grundvoraussetzung für einen voll funktionsfähigen Cluster. Befindet sich ein Cluster im Quorum, ist die einfache Mehrheit der Knoten fehlerfrei und kann miteinander kommunizieren. Geht das Quorum verloren, verliert der Cluster die Fähigkeit, normale Clusteroperationen durchzuführen. Nur eine Knotengruppe kann zu einem bestimmten Zeitpunkt ein Quorum aufweisen, da alle Knoten gemeinsam eine einheitliche Datensicht nutzen. Wenn daher zwei nicht kommunizierende Knoten die Daten auf unterschiedliche Weise verändern, ist es nicht mehr möglich, die Daten zu einer einheitlichen Datensicht zusammenzuführen.

Jeder Knoten im Cluster nimmt an einem Abstimmungsprotokoll teil, das einen Knoten zum Master wählt; jeder verbleibende Knoten ist ein sekundärer Knoten. Der Masterknoten ist für die Synchronisierung der Informationen im gesamten Cluster verantwortlich. Sobald ein Quorum gebildet ist, wird es durch kontinuierliche Abstimmung aufrechterhalten. Wenn der Masterknoten offline geht und das Cluster weiterhin im Quorum ist, wird von den Knoten, die online bleiben, ein neuer Master gewählt.

Da in einem Cluster mit einer geraden Anzahl von Knoten ein Stimmengleichstand möglich ist, erhält ein Knoten ein zusätzliches, bruchstückhaftes Stimmgewicht, genannt Epsilon. Fällt die Verbindung zwischen zwei gleich großen Teilen eines großen Clusters aus, bleibt die Gruppe der Knoten mit *epsilon* beschlussfähig, vorausgesetzt, alle Knoten sind funktionsfähig. Die folgende Abbildung zeigt beispielsweise ein Vier-Node-Cluster, in dem zwei der Knoten ausgefallen sind. Da jedoch einer der verbleibenden Knoten *epsilon* hält, bleibt der Cluster beschlussfähig, obwohl keine einfache Mehrheit funktionsfähiger Knoten vorhanden ist.



Epsilon wird beim Erstellen des Clusters automatisch dem ersten Knoten zugewiesen. Wenn der Knoten, der Epsilon enthält, fehlerhaft wird, seinen Hochverfügbarkeitspartner übernimmt oder von seinem Hochverfügbarkeitspartner übernommen wird, wird Epsilon automatisch einem fehlerfreien Knoten in einem anderen HA-Paar neu zugewiesen.

Das Offline-Nehmen eines Knotens kann die Fähigkeit des Clusters beeinträchtigen, im Quorum zu bleiben. Daher gibt ONTAP eine Warnmeldung aus, wenn Sie einen Vorgang ausführen, der entweder den Cluster aus dem Quorum bringt oder bei einem weiteren Ausfall zum Verlust des Quorums führen würde. Sie können die Quorum-Warnmeldungen deaktivieren, indem Sie den Befehl cluster quorum-service options modify auf der

erweiterten Berechtigungsebene verwenden.

Im Allgemeinen gilt: Bei zuverlässiger Verbindung zwischen den Knoten des Clusters ist ein größerer Cluster stabiler als ein kleinerer. Die Quorumsanforderung einer einfachen Mehrheit (die Hälfte der Knoten plus Epsilon) lässt sich in einem Cluster mit 24 Knoten leichter erfüllen als in einem Zwei-Node-Cluster.

Ein Zwei-Node-Cluster stellt besondere Herausforderungen für die Aufrechterhaltung des Quorums dar. Zwei-Node-Cluster nutzen Cluster HA, bei der keiner der Nodes Epsilon hält. Stattdessen werden beide Nodes kontinuierlich abgefragt, um sicherzustellen, dass bei einem Ausfall eines Node der andere vollen Lese- und Schreibzugriff auf die Daten sowie Zugriff auf logische Schnittstellen und Managementfunktionen hat.

Die Clusterliste und Details sind im Active IQ Unified Manager verfügbar

In der Ansicht „Systemstatus: Alle Cluster“ können Sie Ihren Bestand an Clustern einsehen. Die Ansicht „Kapazität: Alle Cluster“ zeigt zusammengefasste Informationen zur Storage-Kapazität und -Auslastung aller Cluster an.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Details zu einzelnen Clustern, wie dem Systemstatus des Clusters, der Kapazität, der Konfiguration, den LIFs, den Nodes und den Datenträgern in diesem Cluster, können auch auf der Seite „Cluster / Systemstatusdetails“ angezeigt werden.

Die Details in der Ansicht „Systemstatus: Alle Cluster“, der Ansicht „Kapazität: Alle Cluster“ und auf der Seite „Cluster/Systemstatus-Details“ helfen Ihnen bei der Planung Ihres Storage. Beispielsweise können Sie vor der Provisionierung eines neuen Aggregats einen bestimmten Cluster in der Ansicht „Systemstatus: Alle Cluster“ auswählen und die Kapazitätsdetails abrufen, um festzustellen, ob der Cluster über den erforderlichen Speicherplatz verfügt.

Schritte

1. Im linken Navigationsbereich wird **Storage** > **Cluster** ausgewählt.
2. Im Menü „Ansicht“ steht die Ansicht **Systemstatus: Alle Cluster** zum Anzeigen von Informationen zum Systemstatus sowie die Ansicht **Kapazität: Alle Cluster** zum Anzeigen von Details zur Storage-Kapazität und -Auslastung in allen Clustern zur Verfügung.
3. Durch Klicken auf den Namen eines Clusters können Sie die vollständigen Details des Clusters auf der Detailseite **Cluster / Systemstatus** anzeigen.

Verwandte Informationen

- "Cluster-/Systemstatusdetailseite"
- "Leistung: Ansicht „Alle Cluster“"
- "Überwachung von MetroCluster Konfigurationen"
- "Anzeigen des Sicherheitsstatus für Cluster und Storage VMs"
- "Welche Sicherheitskriterien werden bewertet"

Der Zustand der Cluster in einer MetroCluster Konfiguration in Active IQ Unified Manager kann überprüft werden

Mit Active IQ Unified Manager (Unified Manager) kann der Systemstatus von Clustern

und ihren Komponenten in MetroCluster over FC und MetroCluster over IP Konfigurationen überprüft werden. Wenn die Cluster an einem von Unified Manager erkannten Performance-Ereignis beteiligt waren, kann der Systemstatus dabei helfen festzustellen, ob ein Hardware- oder Softwareproblem zu dem Ereignis beigetragen hat.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Sie müssen ein Performance-Ereignis für eine MetroCluster Konfiguration analysiert und den Namen des beteiligten Clusters ermittelt haben.
- Beide Cluster in der MetroCluster Konfiguration über FC und IP müssen von derselben Instanz des Unified Manager überwacht werden.

Bestimmen des Cluster-Systemstatus in der MetroCluster over FC Konfiguration

Mit den folgenden Schritten lässt sich der Systemstatus in einer MetroCluster over FC Konfiguration ermitteln.

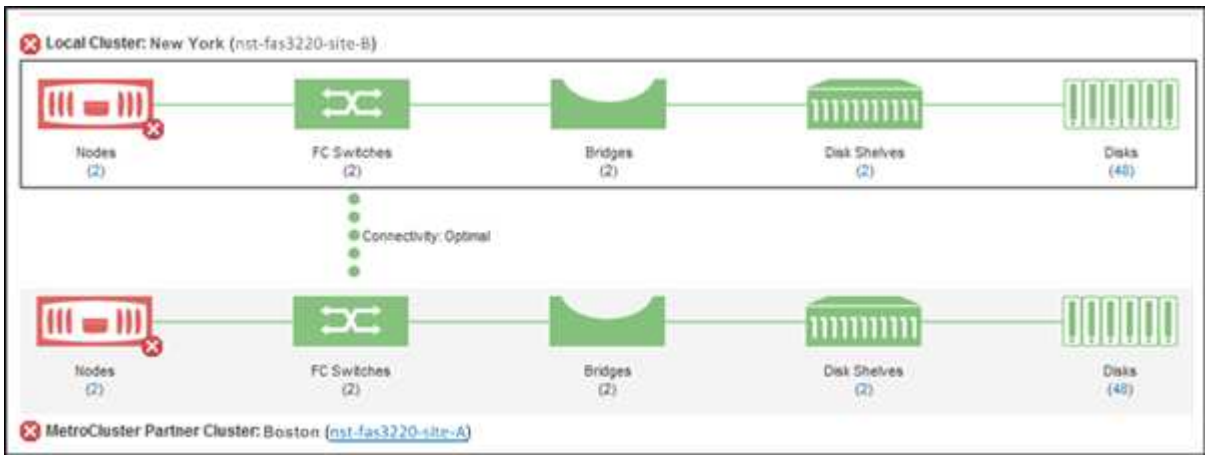
Schritte

1. Im linken Navigationsbereich zeigt ein Klick auf **Event Management** die Ereignisliste an.
2. Im Filterbereich können unter der Kategorie **Source Type** alle MetroCluster Filter ausgewählt werden. Sie sehen alle Ereignisse, die in Ihrer Umgebung für alle MetroCluster Konfigurationen ausgelöst wurden.
3. Neben einem MetroCluster Ereignis auf den Namen des Clusters klicken.

   Falls keine MetroCluster Ereignisse angezeigt werden, können Sie die Suchleiste verwenden, um nach dem Namen des Clusters zu suchen, der an dem Ereignis beteiligt ist, das Ihre MetroCluster over FC Konfiguration betrifft.

   Die Ansicht „Systemstatus: Alle Cluster“ zeigt detaillierte Informationen zum Ereignis an.

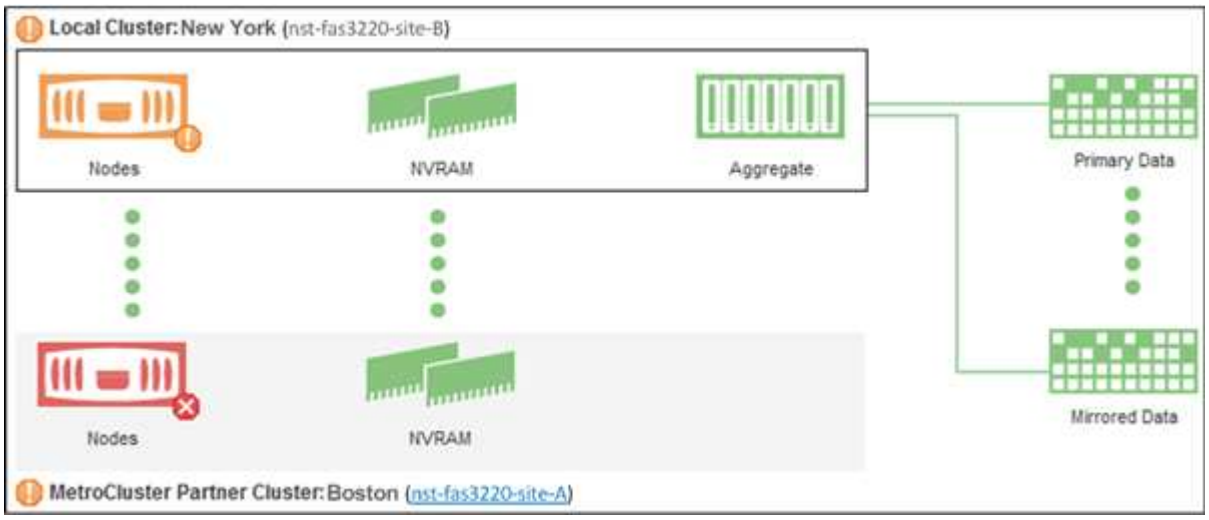
4. Die Registerkarte **MetroCluster Connectivity** zeigt den Systemstatus der Verbindung zwischen dem ausgewählten Cluster und seinem Partnercluster an.



   In diesem Beispiel sind die Namen und die Komponenten des lokalen Clusters und seines Partnerclusters zu sehen. Ein gelbes oder rotes Symbol weist auf ein Systemstatusereignis für die hervorgehobene Komponente hin. Das Konnektivitätssymbol stellt die Verbindung zwischen den Clustern dar. Wenn Sie den Mauszeiger auf ein Symbol bewegen, werden Ereignisinformationen angezeigt, oder durch Klicken auf das Symbol lassen sich die Ereignisse anzeigen. Ein Systemstatusproblem in einem der beiden Cluster könnte zu dem Performance-Ereignis beigetragen haben.

Unified Manager überwacht die NVRAM Komponente der Verbindung zwischen den Clustern. Wenn das Symbol FC Switches auf dem lokalen oder Partnercluster oder das Verbindungssymbol rot ist, könnte ein Problem mit dem Systemstatus der Verbindung das Performance-Ereignis verursacht haben.

5. Die Registerkarte **MetroCluster Replication** auswählen.



In diesem Beispiel könnte, wenn das NVRAM-Symbol auf dem lokalen oder dem Partner-Cluster gelb oder rot ist, ein Systemstatusproblem mit dem NVRAM das Performance-Ereignis verursacht haben. Wenn auf der Seite keine roten oder gelben Symbole vorhanden sind, könnte ein Performance-Problem auf dem Partner-Cluster das Performance-Ereignis verursacht haben.

Cluster-Systemstatus in MetroCluster over IP Konfiguration bestimmen

Die folgenden Schritte dienen zum Ermitteln des Systemstatus in einer MetroCluster over IP Konfiguration.

Schritte

1. Im linken Navigationsbereich zeigt ein Klick auf **Event Management** die Ereignisliste an.
2. Im Filterbereich wird unter der Kategorie **Quelltyp** der `MetroCluster Relationship` Filter ausgewählt. Es werden alle Ereignisse angezeigt, die in Ihrer Umgebung für alle MetroCluster Konfigurationen ausgelöst wurden.

> Falls die gemeldeten MetroCluster Ereignisse nicht angezeigt werden, ist eine Suche über die Suchleiste nach dem Namen des Clusters möglich, das an dem Ereignis beteiligt ist, das Ihre MetroCluster over IP Konfiguration betrifft.

3. Neben dem entsprechenden MetroCluster Ereignis können Sie auf den Namen des Clusters klicken. Die Seite „Clusters“ wird mit den Details dieses Clusters angezeigt. Informationen zum Ermitteln von Systemstatusproblemen finden Sie unter "Überwachung von Verbindungsproblemen in der MetroCluster over IP Konfiguration".

Der Gesundheits- und Kapazitätsstatus aller All SAN Array Cluster in Active IQ Unified Manager kann angezeigt werden

Auf den Cluster-Inventarseiten können Sie den Systemstatus und den Kapazitätsstatus Ihrer All SAN Array Cluster anzeigen.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Übersichtsinformationen zu allen SAN Array Clustern finden Sie in den Ansichten „Systemstatus: Alle Cluster“ und „Kapazität: Alle Cluster“. Außerdem finden Sie Details auf der Seite „Cluster/Systemstatusdetails“.

Schritte

1. Im linken Navigationsbereich wird **Storage** > **Cluster** ausgewählt.
2. Es muss sichergestellt sein, dass die Spalte “Personality” in der Ansicht **Systemstatus: Alle Cluster** angezeigt wird, oder dass sie über das Steuerelement **Ein-/Ausblenden** hinzugefügt wird.

   In dieser Spalte wird „`All SAN Array`“ für Ihre All SAN Array Cluster angezeigt.
3. Informationen prüfen.
4. Informationen zur Storage Kapazität in diesen Clustern werden in der Ansicht „Kapazität: Alle Cluster“ angezeigt.
5. Detaillierte Informationen über Systemstatus und Storage-Kapazität in diesen Clustern sind nach Auswahl des Namens eines All SAN Array Clusters verfügbar.

   Die Details sind auf den Registerkarten „Systemstatus“, „Kapazität“ und „Knoten“ auf der Seite „Cluster / Systemstatusdetails“ zu sehen.

Die Knotenliste und Details in Active IQ Unified Manager

In der Ansicht „Systemstatus: Alle Knoten“ können Sie die Liste der Knoten in Ihren Clustern anzeigen. Auf der Seite „Cluster / Systemstatusdetails“ finden Sie detaillierte Informationen zu den Knoten des überwachten Clusters.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Sie können Details wie den Knotenstatus, den Cluster, der den Knoten enthält, Details zur Aggregatkapazität (genutzt und insgesamt) sowie Details zur Bruttokapazität (nutzbar, Reserve und insgesamt) einsehen. Außerdem erhalten Sie Informationen zu HA-Paaren, Disk Shelves und Ports.

Schritte

1. Im linken Navigationsbereich können Sie **Storage** > **Nodes** auswählen.
2. In der Ansicht **Systemstatus: Alle Knoten** kann der Knoten ausgewählt werden, dessen Details angezeigt werden sollen.

   Die detaillierten Informationen für den ausgewählten Knoten werden auf der Seite „Cluster/Systemstatusdetails“ angezeigt. Im linken Bereich wird die Liste der HA-Paare angezeigt. Standardmäßig ist die Ansicht „HA Details“ geöffnet, in der Statusdetails und Ereignisse angezeigt werden, die dem ausgewählten HA-Paar zugeordnet sind.
3. Weitere Details zum Knoten lassen sich über die entsprechende Aktion anzeigen:

Zum Anzeigen…	Klicken…
Details zu den Disk Shelves	**Platten-Shelves**.
Port-bezogene Informationen	**Ports**.

Weitere Informationen:

- "Performance: Ansicht „Alle Knoten“"
- "Anzeige der verfügbaren IOPS-Werte auf Knoten- und Aggregatebene"
- "Anzeigen der Werte der genutzten Performance-Kapazität von Nodes und Aggregaten"

Generieren eines Hardwareinventarberichts für die Vertragsverlängerung in Active IQ Unified Manager

Sie können einen Bericht erstellen, der eine vollständige Liste der Cluster- und Node-Informationen enthält, z. B. Hardware-Modellnummern und Seriennummern, Festplattentypen und -anzahlen, installierte Lizenzen und mehr. Dieser Bericht ist für die Vertragsverlängerung an sicheren Standorten (“dark” Sites) hilfreich, die nicht mit der NetAppActive IQ Plattform verbunden sind.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritte

1. Im linken Navigationsbereich können Sie **Storage** > **Nodes** auswählen.
2. Der nächste Schritt ist der Wechsel zur Ansicht **Zustand: Alle Knoten** oder **Performance: Alle Knoten**.
3. Die Auswahl erfolgt über **Berichte** > ***** > Hardware-Inventarbericht*.

   Der Hardwareinventarbericht steht als .csv-Datei mit vollständigen Informationen zum aktuellen Datum zum Herunterladen bereit.

4. Diese Informationen sind für Ihren NetApp Support-Ansprechpartner zur Vertragsverlängerung bestimmt.

Die Liste und Details der Storage-VMs in Active IQ Unified Manager anzeigen

In der Ansicht „Systemstatus: Alle Storage VMs“ können Sie Ihren Bestand an Storage Virtual Machines (SVMs) überwachen. Die Detailseite „Storage VM / Systemstatus“ enthält detaillierte Informationen zu den überwachten SVMs.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Sie können SVM-Details wie Kapazität, Effizienz und Konfiguration einer SVM einsehen. Außerdem können Sie Informationen zu den zugehörigen Geräten und Warnmeldungen für diese SVM abrufen.

Schritte

1. Die Auswahl erfolgt im linken Navigationsbereich über **Storage** > **Storage VMs**.
2. Eine der folgenden Möglichkeiten kann verwendet werden, um die SVM-Details anzuzeigen:
   - Informationen über den Systemstatus aller SVMs in allen Clustern sind über das Menü „Ansicht“ in der Ansicht „Systemstatus: Alle Storage VMs“ verfügbar.
   - Die vollständigen Details lassen sich durch Klicken auf den Namen der Storage VM anzeigen.

     Sie können die vollständigen Details auch einsehen, indem Sie im Dialogfeld „Minimale Details“ auf

Details anzeigen klicken.

3. Im Dialogfeld „Minimale Details“ können die mit der SVM verknüpften Objekte durch Klicken auf **Verwandte Objekte anzeigen** angezeigt werden.

Verwandte Informationen

- "Storage VM: Seite mit Systemstatusdetails"
- "Performance: Ansicht aller Storage VMs"
- "Sicherheit: Anti-Ransomware-Ansicht"
- "Anzeigen des Sicherheitsstatus für Cluster und Storage VMs"
- "Beziehung: Ansicht Alle Beziehungen"

Die Aggregatliste und Details sind in Active IQ Unified Manager verfügbar

In der Ansicht „Systemstatus: Alle Aggregate“ können Sie Ihren Bestand an Aggregaten überwachen. Die Ansicht „Kapazität: Alle Aggregate“ ermöglicht es Ihnen, Informationen über die Kapazität und Auslastung der Aggregate in allen Clustern anzuzeigen.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Auf der Seite „Aggregat-/Systemstatusdetails“ können Sie Details wie Aggregatkapazität und -konfiguration sowie Festplatteninformationen einsehen. Diese Informationen können Sie bei Bedarf vor der Konfiguration der Schwellenwerteinstellungen verwenden.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Aggregates**.
2. Eine der folgenden Möglichkeiten kann verwendet werden, um die Aggregatdetails anzuzeigen:
   - Informationen zum Systemstatus aller Aggregate in allen Clustern sind im Menü „Ansicht“ in der Ansicht „Systemstatus: Alle Aggregate“ verfügbar.
   - Informationen über die Kapazität und Auslastung aller Aggregate in allen Clustern lassen sich anzeigen, indem im Menü „Ansicht“ die Ansicht „Kapazität: Alle Aggregate“ ausgewählt wird.
   - Die vollständigen Details lassen sich durch Klicken auf den Namen des Aggregats anzeigen.

     Sie können die vollständigen Details auch einsehen, indem Sie im Dialogfeld „Minimale Details“ auf **Details anzeigen** klicken.
3. Im Dialogfeld „Minimale Details“ können die dem Aggregat zugeordneten Objekte über **View Related** angezeigt werden.

Verwandte Informationen

- "Seite „Aggregate / Systemstatus-Details“"
- "Performance: Ansicht „Alle Aggregate“"
- "Erstellung eines Berichts zum Anzeigen von Aggregaten, die in Active IQ Unified Manager ihre volle Kapazität erreichen"

Kapazitätsinformationen zu FabricPool in Active IQ Unified Manager anzeigen

Sie können Kapazitätsinformationen zu FabricPool für Cluster, Aggregate und Volumes auf den Inventar- und Detailseiten für Kapazität und Performance dieser Objekte anzeigen. Auf diesen Seiten werden auch Informationen zur FabricPool Spiegelung angezeigt, wenn eine Spiegelungsebene konfiguriert wurde.

Auf diesen Seiten werden Informationen angezeigt, z. B. die verfügbare Kapazität auf der lokalen Performance-Ebene und auf der Cloud-Ebene, wie viel Kapazität auf beiden Ebenen genutzt wird, welche Aggregate an eine Cloud-Ebene angehängt sind und welche Volumes die FabricPool Funktionen nutzen, indem sie bestimmte Informationen auf die Cloud-Ebene verschieben.

Wenn ein Cloud-Tier auf einen anderen Cloud-Provider gespiegelt wird (das “mirror tier”), werden beide Cloud-Tiers auf der Seite „Aggregat-/Systemstatusdetails“ angezeigt.

Schritte

1. Einer der folgenden Schritte kann durchgeführt werden:

Zum Anzeigen von Kapazitätsinformationen für…	Folgendes ist zu tun…
Cluster	a. In der Ansicht „Kapazität: Alle Cluster“ erfolgt die Auswahl eines Clusters. b. Auf der Seite „Cluster / Systemstatusdetails“ wählen Sie die Registerkarte **Konfiguration** aus. Die Anzeige zeigt die Namen aller Cloud-Tiers, mit denen dieser Cluster verbunden ist.
Aggregate	a. In der Ansicht „Kapazität: Alle Aggregate“ wird ein Aggregat ausgewählt, bei dem im Feld „Typ“ „`SSD (FabricPool)`“ oder „`HDD (FabricPool)`“ angegeben ist. b. Auf der Seite „Aggregat-/Systemstatusdetails“ wird die Registerkarte **Kapazität** ausgewählt. Die Anzeige zeigt die gesamte im Cloud-Tier genutzte Kapazität an. c. Die Registerkarte **Festplatteninformationen** auswählen. Die Anzeige zeigt den Namen des Cloud-Tiers und die verwendete Kapazität an. d. Dann folgt die Auswahl der Registerkarte **Configuration**. Auf dem Display werden der Name der Cloud-Ebene und weitere detaillierte Informationen zur Cloud-Ebene angezeigt.

Zum Anzeigen von Kapazitätsinformationen für…	Folgendes ist zu tun…
Volumes	a. In der Ansicht „Kapazität: Alle Volumes“ wählen Sie ein Volume aus, bei dem im Feld “Tiering Policy” ein Richtlinienname angezeigt wird. b. Auf der Seite „Volume / Health Details“ erfolgt die Auswahl der Registerkarte **Konfiguration**. Auf dem Display wird der Name der dem Volume zugewiesenen FabricPool Tiering-Richtlinie angezeigt.

2. Auf der Seite **Workload-Analyse** können Sie im Bereich **Capacity Trend** „`Cloud Tier View`“ auswählen, um die im lokalen Performance Tier und im Cloud Tier im Vormonat genutzte Kapazität anzuzeigen.

Weitere Informationen zu FabricPool Aggregaten sind unter "Übersicht über Festplatten und Aggregate" verfügbar.

Speicherpooldetails in Active IQ Unified Manager anzeigen

Sie können die Details des Storage Pools einsehen, um den Systemstatus des Storage Pools, den gesamten und verfügbaren Cache sowie die verwendeten und verfügbaren Zuweisungen zu überwachen.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Aggregates**.
2. Einen Aggregatnamen auswählen.

   Die Details des ausgewählten Aggregats werden angezeigt.

3. Die Registerkarte **Festplatteninformationen** auswählen.

   Es werden detaillierte Datenträgerinformationen angezeigt.

   Die Cache-Tabelle wird nur angezeigt, wenn das ausgewählte Aggregat einen Storage Pool verwendet.

4. In der Cache-Tabelle befindet sich der Zeiger über dem Namen des erforderlichen Storage-Pools.

   Die Details des Storage Pools werden angezeigt.

Die Volumenliste und Details in Active IQ Unified Manager anzeigen

In der Ansicht „Systemstatus: Alle Volumes“ können Sie Ihren Bestand an Volumes überwachen. Die Ansicht „Kapazität: Alle Volumes“ ermöglicht es Ihnen, Informationen über die Kapazität und Auslastung der Volumes in einem Cluster anzuzeigen.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Auf der Seite „Volume/Systemstatusdetails“ können Sie detaillierte Informationen zu überwachten Volumes anzeigen, darunter Kapazität, Effizienz, Konfiguration und Schutz der Volumes. Außerdem können Sie Informationen zu den zugehörigen Geräten und zugehörigen Warnmeldungen für ein bestimmtes Volume anzeigen.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Eine der folgenden Möglichkeiten steht zum Anzeigen der Volumendetails zur Verfügung:
   - Zur Anzeige detaillierter Informationen über den Systemstatus von Volumes in einem Cluster wählen Sie im Menü „Ansicht“ die Ansicht „Systemstatus: Alle Volumes“.
   - Für detaillierte Informationen über die Kapazität und Auslastung der Volumes in einem Cluster steht im Menü „Ansicht“ die Ansicht „Kapazität: Alle Volumes“ zur Verfügung.
   - Die vollständigen Details lassen sich durch Klicken auf den Volumennamen anzeigen.

     Sie können die vollständigen Details auch einsehen, indem Sie im Dialogfeld „Minimale Details“ auf **Details anzeigen** klicken.
3. **Optional:** Durch Klicken auf **Zugehörige Objekte anzeigen** im Dialogfeld „Minimale Details“ lassen sich die Objekte anzeigen, die mit dem Volume in Verbindung stehen.

Verwandte Informationen

- "Volume: Seite mit Systemstatusdetails"
- "Performance: Ansicht „Alle Volumes“"
- "Sicherheit: Anti-Ransomware-Ansicht"
- "Anzeigen von Volume-Schutzbeziehungen"
- "Erstellen eines Berichts zur Anzeige verfügbarer Volume-Kapazitätsdiagramme"

Details zu NFS-Freigaben in Active IQ Unified Manager

Sie können Details zu allen NFS-Freigaben anzeigen, z. B. ihren Status, den dem Volume zugeordneten Pfad (FlexGroup Volumes oder FlexVol Volumes), die Zugriffsebenen von Clients auf die NFS-Freigaben und die für die exportierten Volumes definierte Exportrichtlinie. In der Ansicht „Systemstatus: Alle NFS-Freigaben“ werden alle NFS-Freigaben auf allen überwachten Clustern angezeigt, und auf der Seite „Storage VM / Systemstatusdetails“ werden alle NFS-Freigaben auf einer bestimmten Storage Virtual Machine (SVM) angezeigt.

Bevor Sie beginnen

- Die NFS-Lizenz muss auf dem Cluster aktiviert sein.
- Die Netzwerkschnittstellen für die NFS-Freigaben müssen konfiguriert sein.
- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritt

1. Im linken Navigationsbereich hängen die folgenden Schritte davon ab, ob alle NFS-Freigaben oder nur die NFS-Freigaben für eine bestimmte SVM angezeigt werden sollen.

Zu…	Folgen Sie diesen Schritten…
Anzeige aller NFS-Freigaben	Unter **Storage** > **NFS Shares**
NFS-Freigaben für einzelne SVM anzeigen	a. **Storage** > **Storage VMs** auswählen b. Auswahl der SVM, für die die NFS-Freigabedetails angezeigt werden sollen. c. Auf der Seite „Storage VM / Systemstatusdetails“ wählen Sie die Registerkarte **NFS-Freigaben** aus.

Weitere Informationen finden Sie unter "Provisionierung von Dateifreigabe-Volumes" und "Provisionierung von CIFS- und NFS-Dateifreigaben mithilfe von APIs".

Details zu SMB/CIFS Freigaben in Active IQ Unified Manager

Sie können Details zu allen SMB/CIFS-Freigaben anzeigen, z. B. den Freigabenamen, den Verbindungspfad, enthaltene Objekte, Sicherheitseinstellungen und für die Freigabe definierte Exportrichtlinien. In der Ansicht „Systemstatus: Alle SMB-Freigaben“ sind alle SMB-Freigaben auf allen überwachten Clustern zu sehen, und auf der Seite „Storage VM / Systemstatusdetails“ sind alle SMB-Freigaben auf einer bestimmten Storage Virtual Machine (SVM) zu sehen.

Bevor Sie beginnen

- CIFS-Lizenz muss auf dem Cluster aktiviert sein.
- Für die SMB/CIFS-Freigaben müssen die Netzwerkschnittstellen konfiguriert sein.
- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Freigaben in Ordnern werden nicht angezeigt.

Schritt

1. Im linken Navigationsbereich richten sich die folgenden Schritte danach, ob alle SMB/CIFS-Freigaben oder nur die Freigaben für eine bestimmte SVM angezeigt werden sollen.

Zu…	Folgen Sie diesen Schritten…
Alle SMB/CIFS-Freigaben	Auf **Storage** > **SMB-Freigaben** klicken
Anzeigen von SMB/CIFS-Freigaben für eine einzelne SVM	a. **Storage** > **Storage VMs** auswählen b. Wählen Sie die SVM aus, deren SMB/CIFS-Freigabedetails angezeigt werden sollen. c. Die Registerkarte **SMB Shares** befindet sich auf der Seite „Storage VM / Systemstatusdetails“.

Weitere Informationen sind unter "Provisionierung von CIFS- und NFS-Dateifreigaben mithilfe von APIs" verfügbar.

Die Liste der Snapshot-Kopien in Active IQ Unified Manager

Sie können die Liste der Snapshot-Kopien für ein ausgewähltes Volume anzeigen. Mithilfe der Liste der Snapshot-Kopien können Sie berechnen, wie viel Speicherplatz freigegeben werden kann, wenn eine oder mehrere Snapshot-Kopien gelöscht werden, und Sie können die Snapshot-Kopien bei Bedarf löschen.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Das Volume, das die Snapshot Kopien enthält, muss online sein.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. In der Ansicht **Systemstatus: Alle Volumes** erfolgt die Auswahl des Volumes, das die anzuzeigenden Snapshot Kopien enthält.
3. Auf der Detailseite **Volume / Systemstatus** ist die Registerkarte **Kapazität** auszuwählen.
4. Im Bereich **Details** der Registerkarte **Capacity** wird im Abschnitt „Weitere Details“ der Link neben **Snapshot Copies** ausgewählt.

   Die Anzahl der Snapshot-Kopien ist ein Link, der die Liste der Snapshot-Kopien anzeigt.

Verwandte Informationen

"Seite „Systemstatus/Volumes“"

Löschen von Snapshot Kopien in Active IQ Unified Manager

Sie können eine Snapshot-Kopie löschen, um Speicherplatz zu sparen oder Festplattenspeicher freizugeben, oder wenn sie nicht mehr benötigt wird.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Das Volume muss online sein.

Zum Löschen einer Snapshot Kopie, die belegt oder gesperrt ist, muss die Snapshot Kopie von der Applikation freigegeben worden sein, die sie verwendet hat.

- Sie können die Basis-Snapshot-Kopie in einem übergeordneten Volume nicht löschen, wenn ein FlexClone Volume diese Snapshot-Kopie verwendet.

  Die Basis Snapshot Kopie ist die Snapshot Kopie, die zum Erstellen des FlexClone Volume verwendet wird und den Status `Busy` und die Anwendungsabhängigkeit als `Busy, Vclone` im übergeordneten Volume anzeigt.

- Eine gesperrte Snapshot-Kopie, die in einer SnapMirror Beziehung verwendet wird, kann nicht gelöscht werden.

  Die Snapshot-Kopie ist gesperrt und wird für das nächste Update benötigt.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. In der Ansicht **Systemstatus: Alle Volumes** erfolgt die Auswahl des Volumes, das die anzuzeigenden Snapshot Kopien enthält.

   Die Liste der Snapshot-Kopien wird angezeigt.

3. Auf der Detailseite **Volume / Systemstatus** ist die Registerkarte **Kapazität** auszuwählen.
4. Im Bereich **Details** der Registerkarte **Capacity** wird im Abschnitt „Weitere Details“ der Link neben **Snapshot Copies** ausgewählt.

   Die Anzahl der Snapshot-Kopien ist ein Link, der die Liste der Snapshot-Kopien anzeigt.

5. In der Ansicht **Snapshot Copies** können Sie die Snapshot-Kopien auswählen, die Sie löschen möchten, und anschließend auf **Delete Selected** klicken.

Berechnung des zurückforderbaren Speicherplatzes für Snapshot Kopien in Active IQ Unified Manager

Sie können berechnen, wie viel Speicherplatz freigegeben werden kann, wenn eine oder mehrere Snapshot-Kopien gelöscht werden.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Das Volume muss online sein.
- Das Volume muss ein FlexVol volume sein; diese Funktion wird bei FlexGroup Volumes nicht unterstützt.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. In der Ansicht **Systemstatus: Alle Volumes** erfolgt die Auswahl des Volumes, das die anzuzeigenden Snapshot Kopien enthält.

   Die Liste der Snapshot-Kopien wird angezeigt.

3. Auf der Detailseite **Volume / Systemstatus** ist die Registerkarte **Kapazität** auszuwählen.
4. Im Bereich **Details** der Registerkarte **Capacity** wird im Abschnitt „Weitere Details“ der Link neben **Snapshot Copies** ausgewählt.

   Die Anzahl der Snapshot-Kopien ist ein Link, der die Liste der Snapshot-Kopien anzeigt.

5. In der Ansicht **Snapshot Copies** erfolgt die Auswahl der Snapshot-Kopien, für die der zurückforderbare Speicherplatz berechnet werden soll.
6. Anschließend ist **Berechnen** auszuwählen.

   Der zurückgewinnbare Speicherplatz (in Prozent sowie in KB, MB, GB usw.) auf dem Volume wird angezeigt.

7. Zur Neuberechnung des zurückgewinnbaren Speicherplatzes werden die erforderlichen Snapshot Kopien ausgewählt und auf **Recalculate** geklickt.

Informationen zu Clusterobjektfenstern und Dialogfeldern in Active IQ Unified Manager

Sie können alle Ihre Cluster und Clusterobjekte auf der jeweiligen Seite für das Storage-Objekt anzeigen. Sie können die Details auch auf der entsprechenden Detailseite für das Storage-Objekt anzeigen. Die System Manager Benutzeroberfläche kann nun über die folgenden Abschnitte STORAGE und PROTECTION in INVENTORY gestartet werden.

- Seiten für Clusterinventar, Clusterstatus und Cluster Performance
- Seiten Aggregate Inventory, Aggregate Health und Aggregate Performance
- Seiten zu Volume-Inventar, Volume-Systemstatus und Volume-Performance
- Seiten „Knoteninventar“ und „Knoten-Performance“
- Seiten „StorageVM Inventar“, „StorageVM Systemstatus“ und „StorageVM Performance“
- Seiten für Schutzbeziehungen

Allgemeine Systemstatus-Workflows und -Aufgaben in Unified Manager

Verständnis gängiger Active IQ Unified Manager Arbeitsabläufe und Aufgaben im Zusammenhang mit dem Zustand

Zu den gängigen administrativen Workflows und Aufgaben im Zusammenhang mit Unified Manager gehören die Auswahl der zu überwachenden Storage-Cluster, die Diagnose von Zuständen, die sich nachteilig auf Datenverfügbarkeit, Kapazität und Datenschutz auswirken, die Wiederherstellung verlorener Daten, die Konfiguration und Verwaltung von Volumes sowie das Bündeln und Senden von Diagnosedaten an den technischen Support, falls erforderlich.

Unified Manager ermöglicht es Storage-Administratoren, ein Dashboard anzuzeigen, die Gesamtkapazität, Verfügbarkeit und den Schutzstatus der verwalteten Storage-Cluster zu bewerten und anschließend eventuell auftretende spezifische Probleme schnell zu identifizieren, zu lokalisieren, zu diagnostizieren und zur Behebung zuzuweisen.

Die wichtigsten Probleme im Zusammenhang mit einem Cluster, einer Storage Virtual Machine (SVM), einem Volume oder einem FlexGroup Volume, die sich auf die Storage-Kapazität oder Datenverfügbarkeit Ihrer verwalteten Storage-Objekte auswirken, werden in den Systemstatusdiagrammen und Ereignissen auf der Dashboard-Seite angezeigt. Bei kritischen Problemen bietet diese Seite Links zur Unterstützung geeigneter Fehlerbehebungs-Workflows.

Unified Manager kann auch in Arbeitsabläufe eingebunden werden, die verwandte Verwaltungstools wie OnCommand Workflow Automation (WFA) umfassen, um die direkte Konfiguration von Storage-Ressourcen zu unterstützen.

In diesem Dokument werden gängige Arbeitsabläufe im Zusammenhang mit den folgenden administrativen Aufgaben beschrieben:

- Diagnose und Management von Verfügbarkeitsproblemen

  Wenn Hardwareausfälle oder Konfigurationsprobleme bei Storage-Ressourcen dazu führen, dass auf der

Dashboard-Seite Ereignisse zur Datenverfügbarkeit angezeigt werden, können Storage-Administratoren über die eingebetteten Links Verbindungsinformationen zur betroffenen Storage-Ressource und Hinweise zur Fehlerbehebung anzeigen sowie die Problemlösung anderen Administratoren zuweisen.

- Konfiguration und Überwachung von Performance-Vorfällen

  Der Administrator kann die Performance der überwachten Ressourcen des Storage-Systems überwachen und managen. Weitere Informationen enthält "Einführung in die Performance-Überwachung mit Active IQ Unified Manager".

- Diagnose und Management von Kapazitätsproblemen bei Volumes

  Bei Problemen mit der Storage-Kapazität eines Volumes, die auf der Dashboard-Seite angezeigt werden, können Storage-Administratoren den eingebetteten Links folgen, um die aktuellen und historischen Trends in Bezug auf die Storage-Kapazität des betroffenen Volumes anzuzeigen, Hinweise zur Fehlerbehebung einzusehen und die Behebung des Problems anderen Administratoren zuzuweisen.

- Konfigurieren, Überwachen und Diagnostizieren von Problemen mit Schutzbeziehungen

  Nach dem Erstellen und Konfigurieren von Schutzbeziehungen können Speicheradministratoren potenzielle Probleme im Zusammenhang mit Schutzbeziehungen, den aktuellen Status der Schutzbeziehungen, Informationen über den aktuellen und bisherigen Erfolg von Schutzaufträgen für die betroffenen Beziehungen sowie Hinweise zur Fehlerbehebung einsehen. Weitere Informationen finden Sie in "Informationen zur Verwaltung und Überwachung von Schutzbeziehungen".

- Erstellen von Sicherungsdateien und Wiederherstellen von Daten aus Sicherungsdateien.
- Zuordnung von Storage-Objekten zu Annotationen

  Durch die Verknüpfung von Speicherobjekten mit Annotationen können Speicheradministratoren die Ereignisse filtern und anzeigen, die mit den Speicherobjekten in Zusammenhang stehen. Dadurch können Speicheradministratoren die mit den Ereignissen verbundenen Probleme priorisieren und beheben.

- Mithilfe von REST-APIs können Sie Ihre Cluster managen, indem Sie die von Unified Manager erfassten Informationen zu Systemstatus, Kapazität und Performance anzeigen. Weitere Informationen finden Sie in "Erste Schritte mit Active IQ Unified Manager REST APIs".
- Senden eines Support Bundles an den technischen Support

  Storage-Administratoren können über die Managementplattform ein Support-Paket abrufen und an den technischen Support senden. Support-Pakete müssen an den technischen Support gesendet werden, wenn das Problem eine detailliertere Diagnose und Fehlerbehebung erfordert, als eine AutoSupport Meldung bieten kann.

Überwachen und Beheben von Problemen mit der Datenverfügbarkeit

Überwachung und Fehlerbehebung der Datenverfügbarkeit in Active IQ Unified Manager

Unified Manager überwacht die Zuverlässigkeit, mit der autorisierte Benutzer auf Ihre gespeicherten Daten zugreifen können, benachrichtigt Sie über Bedingungen, die diesen Zugriff blockieren oder behindern, und ermöglicht es Ihnen, diese Bedingungen zu diagnostizieren sowie deren Behebung zuzuweisen und zu verfolgen.

Die Workflow-Themen zur Datenverfügbarkeit in diesem Abschnitt beschreiben Beispiele dafür, wie ein Storage-Administrator mithilfe der Unified Manager Weboberfläche Hardware- und Softwarezustände

identifizieren, diagnostizieren und zur Behebung zuweisen kann, die sich nachteilig auf die Datenverfügbarkeit auswirken.

Erkennung und Behebung von Ausfallzuständen der Interconnect-Verbindung für Storage Failover

Suche und Behebung von Link-Down-Zuständen der Storage Failover Interconnect Verbindung in Active IQ Unified Manager

Dieser Workflow bietet ein Beispiel dafür, wie Sie ausgefallene Verbindungen der Storage Failover-Interconnect-Links erkennen, bewerten und beheben können. In diesem Szenario sind Sie ein Administrator, der Unified Manager verwendet, um vor dem Start eines ONTAP Versions Upgrades auf Ihren Nodes nach Storage Failover-Risiken zu suchen.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Wenn die Storage Failover Verbindungen zwischen den HA-Paar-Nodes während eines Versuchs für ein unterbrechungsfreies Upgrade ausfallen, schlägt das Upgrade fehl. Daher überwacht und bestätigt der Administrator üblicherweise vor Beginn eines Upgrades die Zuverlässigkeit von Storage Failover auf den für das Upgrade vorgesehenen Cluster-Nodes.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.
2. Auf der Inventarseite **Event Management** erfolgt die Auswahl von **Active Availability events**.
3. Oben auf der Inventarseite **Event Management** in der Spalte **Name** erfolgt ein Klick auf , und im Textfeld wird `*failover` eingegeben, um die Anzeige auf Ereignisse im Zusammenhang mit Storage Failover zu beschränken.

   Alle vergangenen Ereignisse im Zusammenhang mit Storage Failover-Bedingungen werden angezeigt.

   In diesem Szenario zeigt der Unified Manager das Ereignis „`Storage Failover Interconnect One or More Links Down`“ im Abschnitt „Availability Incidents“ an.

4. Wenn auf der **Event Management** Inventarseite ein oder mehrere Ereignisse im Zusammenhang mit Storage Failover angezeigt werden, sind die folgenden Schritte erforderlich:

   a. Über den Link mit dem Ereignistitel werden die Ereignisdetails für dieses Ereignis angezeigt.

      In diesem Beispiel wird der Ereignistitel „`Storage Failover Interconnect One or More Links Down`“ ausgewählt.

   Die Seite mit den Ereignisdetails für dieses Ereignis wird angezeigt.

   a. Auf der Seite mit den Ereignisdetails können Sie eine oder mehrere der folgenden Aufgaben ausführen:
      - Eine Überprüfung der Fehlermeldung im Feld „Ursache“ und eine Beurteilung des Problems ist erforderlich.
      - Zuweisung des Ereignisses an einen Administrator.
      - Quittierung des Ereignisses.

Verwandte Informationen

"Seite mit Ereignisdetails"

"Unified Manager Benutzerrollen und -Funktionen"

Durchführen der Korrekturmaßnahme bei einem Ausfall einer Storage Failover Interconnect-Verbindung in Active IQ Unified Manager

Wenn Sie die Seite mit den Ereignisdetails eines mit Storage Failover zusammenhängenden Ereignisses anzeigen, können Sie die zusammenfassenden Informationen auf der Seite prüfen, um die Dringlichkeit des Ereignisses, die mögliche Ursache des Problems und eine mögliche Lösung für das Problem zu ermitteln.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

In diesem Beispielszenario enthält die auf der Seite „Ereignisdetails“ bereitgestellte Ereigniszusammenfassung die folgenden Informationen über den Zustand einer ausgefallenen Storage Failover Interconnect-Verbindung:

```
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)
```

Die Beispielereignisinformationen zeigen, dass eine Storage Failover Interconnect-Verbindung, Link1, zwischen den HA-Paarknoten aardvark und bonobo ausgefallen ist, Link0 zwischen Apple und Boy jedoch aktiv ist. Da eine Verbindung aktiv ist, funktioniert der Remote Dynamic Memory Access (RDMA) weiterhin, und ein Storage Failover Auftrag kann dennoch erfolgreich sein.

Um jedoch sicherzustellen, dass nicht beide Verbindungen ausfallen und der Storage Failover-Schutz vollständig deaktiviert wird, beschließen Sie, die Ursache für den Ausfall von Link1 genauer zu diagnostizieren.

Schritte

1. Auf der Seite mit den **Ereignisdetails** kann über den Link zu dem im Feld „Quelle“ angegebenen Ereignis auf weitere Details zu anderen Ereignissen zugegriffen werden, die möglicherweise mit dem Zustand eines ausgefallenen Storage Failover Verbindungslinks zusammenhängen.

   In diesem Beispiel ist der Knoten mit dem Namen „aardvark“ die Quelle des Ereignisses. Beim Klicken auf

diesen Node-Name werden die HA Details für das betroffene HA Paar, aardvark und bonobo, auf der Registerkarte „Nodes“ der Seite „Cluster / Health details“ angezeigt, außerdem werden weitere Ereignisse angezeigt, die kürzlich auf dem betroffenen HA Paar aufgetreten sind.

2. Weitere Informationen zu dem Ereignis finden Sie unter **HA Details**.

   In diesem Beispiel befinden sich die relevanten Informationen in der Tabelle „Events“. Die Tabelle zeigt das Ereignis „`Storage Failover Connection One or More Link Down`“, den Zeitpunkt, zu dem das Ereignis generiert wurde, und erneut den Node, von dem dieses Ereignis ausgegangen ist.

Mithilfe der Knotenstandortinformationen in den HA Details kann für die betroffenen Nodes des HA-Paars eine physische Inspektion und Behebung des Storage Failover Problems angefordert oder persönlich durchgeführt werden.

Verwandte Informationen

"Seite mit Ereignisdetails"

"Unified Manager Benutzerrollen und -Funktionen"

Behebung von Offline-Problemen bei Volumes

Beheben von Offline-Volume-Problemen in Active IQ Unified Manager

Dieser Workflow zeigt beispielhaft, wie ein Volume-offline-Ereignis bewertet und behoben werden kann, das Unified Manager möglicherweise auf der Inventarseite für das Event Management anzeigt. In diesem Szenario sind Sie als Administrator mit Unified Manager damit befasst, ein oder mehrere Volume-offline-Ereignisse zu beheben.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Es kann mehrere Gründe geben, warum Volumes als offline gemeldet werden:

- Der SVM-Administrator hat das Volume absichtlich offline genommen.
- Der Clusterknoten, auf dem das Volume gehostet wird, ist ausgefallen, und auch das Storage Failover auf seinen HA-Paar-Partner ist fehlgeschlagen.
- Die Storage Virtual Machine (SVM), die das Volume hostet, wurde angehalten, weil der Knoten, der das Root-Volume dieser SVM hostet, ausgefallen ist.
- Das hostende Aggregat des Volumes ist aufgrund des gleichzeitigen Ausfalls von zwei RAID-Festplatten ausgefallen.

Mithilfe der Inventarseite „Event Management“ sowie der Detailseiten „Cluster/Health“, „Storage VM/Health“ und „Volume/Health“ können Sie eine oder mehrere dieser Möglichkeiten bestätigen oder ausschließen.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.
2. Auf der Inventarseite **Event Management** erfolgt die Auswahl von **Active Availability events**.
3. Für das Ereignis „Volume Offline“ ist der angezeigte Hypertext-Link auszuwählen.

   Die Seite mit den Ereignisdetails für den Verfügbarkeits-Incident wird angezeigt.

4. Auf dieser Seite geben die Hinweise Aufschluss darüber, ob der SVM-Administrator das betreffende Volume offline genommen hat.
5. Auf der Seite **Event**-Details können Sie die Informationen zu einer oder mehreren der folgenden Aufgaben einsehen:
   - Eine Überprüfung der im Feld „Ursache“ angezeigten Informationen kann mögliche Hinweise für die Diagnose liefern.

     In diesem Beispiel informiert die Angabe im Feld Cause nur darüber, dass das Volume offline ist.

   - Im Bereich „Notizen und Aktualisierungen“ sollte geprüft werden, ob es Hinweise darauf gibt, dass der SVM-Administrator das betreffende Volume absichtlich offline genommen hat.
   - Durch Klicken auf die Quelle des Ereignisses, in diesem Fall das als offline gemeldete Volume, erhalten Sie weitere Informationen zu diesem Volume.
   - Zuweisung des Ereignisses an einen Administrator.
   - Das Ereignis kann bestätigt oder gegebenenfalls als gelöst markiert werden.

Diagnoseaktionen für Volume-Offline-Zustände in Active IQ Unified Manager durchführen

Nachdem Sie die Seite „Volume / Health details“ eines als offline gemeldeten Volumes geöffnet haben, können Sie nach zusätzlichen Informationen suchen, die für die Diagnose des Offline-Zustands des Volumes hilfreich sind.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Wenn das als offline gemeldete Volume nicht absichtlich offline gesetzt wurde, kann dies mehrere Gründe haben.

Ausgehend von der Seite „Volume / Health details“ des Offline-Volumes können Sie zu anderen Seiten und Bereichen navigieren, um mögliche Ursachen zu bestätigen oder auszuschließen:

- Anhand der Links auf der **Volume / Health** Detailseite lässt sich feststellen, ob das Volume offline ist, weil sein Host-Node ausgefallen ist und auch das Storage Failover zu seinem HA-Paar-Partner fehlgeschlagen ist.

  Weitere Informationen finden Sie unter "Feststellen, ob ein Offline-Zustand des Volumes durch einen ausgefallenen Knoten verursacht wird".

- Über die Links auf der Detailseite **Volume / Health** lässt sich feststellen, ob das Volume offline ist und ob die zugehörige Storage Virtual Machine (SVM) angehalten wurde, weil der Node, der das Root-Volume dieser SVM hostet, ausgefallen ist.

  Weitere Informationen finden Sie unter "Feststellen, ob ein Volume offline ist und die SVM gestoppt wurde, weil ein Node ausgefallen ist".

- Über die Links auf der Detailseite **Volume / Health** lässt sich feststellen, ob das Volume aufgrund defekter Festplatten in seinem Host-Aggregat offline ist.

  Weitere Informationen finden Sie unter "Feststellen, ob ein Volume aufgrund defekter Festplatten in einem Aggregat offline ist".

Verwandte Informationen

"Unified Manager Benutzerrollen und -Funktionen"

Ermitteln, ob ein Volume in Active IQ Unified Manager offline ist, weil sein Hostknoten ausgefallen ist

Mithilfe der Unified Manager Weboberfläche können Sie bestätigen oder ausschließen, dass ein Volume offline ist, weil sein Host-Knoten ausgefallen ist und das Storage Failover zu seinem HA-Paarpartner fehlgeschlagen ist.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Zur Feststellung, ob der Offline-Zustand des Volumes durch einen Ausfall des Host-Knotens und ein anschließendes erfolgloses Storage Failover verursacht wird, sind die folgenden Schritte erforderlich:

Schritte

1. Der unter SVM im Bereich **Verwandte Geräte** auf der Detailseite **Volume / Systemstatus** des Offline-Volumes angezeigte Hypertext-Link ist zu suchen und anzuklicken.

   Die Detailseite „Storage VM / Systemstatus“ zeigt Informationen über die hostende Storage Virtual Machine (SVM) des Offline-Volume an.

2. Im Bereich **Related Devices** der Detailseite **Storage VM / Health** ist der unter Volumes angezeigte Hypertext-Link auszuwählen.

   Die Ansicht „Systemstatus: Alle Volumes“ zeigt eine Tabelle mit Informationen zu allen auf der SVM gehosteten Volumes an.

3. In der Ansicht **Health: All Volumes** können Sie in der Spaltenüberschrift Status auf das Filtersymbol klicken und anschließend die Option **Offline** auswählen.

   In der Liste erscheinen nur die SVM-Volumes im Offline-Status.

4. In der Ansicht „Systemstatus: Alle Volumes“ lässt sich nach einem Klick auf das Rastersymbol die Option **Cluster Nodes** auswählen.

   Möglicherweise ist im Auswahlfeld des Rasters ein Bildlauf erforderlich, um die Option **Cluster Nodes** zu finden.

   Im Volume-Inventar gibt es jetzt die Spalte „Clusterknoten“, in der der Name des Knotens angezeigt wird, der das jeweilige Offline-Volume hostet.

5. In der Ansicht **Systemstatus: Alle Volumes** den Eintrag für das Offline-Volume suchen und in der Spalte „Cluster-Knoten“ auf den Namen des hostenden Knotens klicken.

   Auf der Registerkarte „Knoten“ auf der Seite „Cluster/Systemstatusdetails“ wird der Status des HA-Knotenpaars angezeigt, zu dem der hostende Knoten gehört. Der Status des hostenden Knotens und der Erfolg eines etwaigen Cluster Failover Vorgangs werden ebenfalls in der Anzeige angegeben.

Nachdem Sie bestätigt haben, dass der Zustand „Volume offline“ vorliegt, weil sein Host-Knoten ausgefallen ist und das Storage Failover zum HA-Paar-Partner fehlgeschlagen ist, sollten Sie sich an den zuständigen Administrator oder Operator wenden, um den ausgefallenen Knoten manuell neu zu starten und das Storage Failover Problem zu beheben.

Ermitteln Sie, ob ein Volume offline ist, weil seine SVM in Active IQ Unified Manager angehalten wurde

Mithilfe der Unified Manager Weboberfläche können Sie bestätigen oder ausschließen, dass ein Volume offline ist, weil seine Host Storage Virtual Machine (SVM) gestoppt wurde, da der Knoten, auf dem sich das Root-Volume dieser SVM befindet, ausgefallen ist.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Die folgenden Schritte dienen dazu, festzustellen, ob der Offline-Zustand des Volumes darauf zurückzuführen ist, dass die zugehörige Host-SVM gestoppt wurde, weil der Knoten, auf dem das Root-Volume dieser SVM gehostet wird, ausgefallen ist:

Schritte

1. Auf der Detailseite **Volume / Systemstatus** des Offline-Volumes befindet sich unter der SVM im Bereich **Zugehörige Geräte** ein Hypertext-Link, der auszuwählen ist.

   Die Seite „Storage VM / Systemstatus-Details“ zeigt den Status „`running`“ oder „`stopped`“ der hostenden SVM an. Wenn der SVM-Status „`running`“ lautet, wird der Offline-Zustand des Volumes nicht durch einen Ausfall des Knotens verursacht, der das Root-Volume dieser SVM hostet.

2. Wenn der SVM-Status „Gestoppt“ lautet, lässt sich über **View SVMs** die Ursache dafür genauer ermitteln, dass die hostende SVM gestoppt wurde.
3. In der Ansicht **Systemstatus: Alle Storage VMs** kann in der Spaltenüberschrift SVM auf das Filtersymbol geklickt und anschließend der Name der gestoppten SVM eingegeben werden.

   Die Informationen zu dieser SVM sind in einer Tabelle aufgeführt.

4. In der Ansicht **Systemstatus: Alle Storage VMs** folgt auf einen Klick auf die Auswahl der Option **Root Volume**.

   Die Spalte „Root Volume“ wird dem SVM-Inventar hinzugefügt und zeigt den Namen des Root-Volumes der gestoppten SVM an.

5. In der Spalte „Root Volume“ öffnet ein Klick auf den Namen des Root-Volumes die Detailseite **Storage VM / Health** für dieses Volume.

   Wenn der Status des SVM Root-Volumes (Online) lautet, ist der ursprüngliche Offline-Zustand des Volumes nicht darauf zurückzuführen, dass der Knoten, der das Root-Volume dieser SVM hostet, ausgefallen ist.

6. Wenn der Status des SVM Root-Volumes „(Offline)“ ist, ist auf der Seite „Volume / Systemstatusdetails“ des SVM Root-Volumes im Bereich „Related Devices“ unter „Aggregate“ der angezeigte Hypertext-Link auszuwählen.
7. Auf der Detailseite „Aggregat / Systemstatus“ des Aggregats erfolgt die Auswahl des unter „Knoten“ im Bereich „Verwandte Geräte“ angezeigten Hypertext-Links.

   Auf der Registerkarte „Knoten“ der Cluster-/Systemstatusdetailseite wird der Status des HA-Knotenpaares angezeigt, zu dem der Host-Knoten des SVM-Root-Volumes gehört. Der Status des Knotens wird in der Anzeige dargestellt.

Nachdem bestätigt wurde, dass der Offline-Zustand des Volumes durch den Offline-Zustand der Host-SVM

dieses Volumes verursacht wird, der wiederum darauf zurückzuführen ist, dass der Knoten ausgefallen ist, der das Root-Volume dieser SVM hostet, ist der zuständige Administrator oder Operator zu kontaktieren, damit der ausgefallene Knoten manuell neu gestartet wird.

Ermitteln, ob ein Volume in Active IQ Unified Manager aufgrund defekter Festplatten offline ist

Mithilfe der Unified Manager Weboberfläche können Sie bestätigen oder ausschließen, dass ein Volume offline ist, weil RAID-Festplattenprobleme das zugehörige Host-Aggregat offline genommen haben.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Mit den folgenden Schritten lässt sich feststellen, ob der Offline-Zustand des Volumes durch RAID-Festplattenprobleme verursacht wird, die das hostende Aggregat offline schalten:

Schritte

1. Die unter „Aggregat“ im Bereich „Zugehörige Geräte“ auf der Detailseite „Volume / Systemstatus“ angezeigte Hypertext-Verknüpfung ist auszuwählen.

   Die Detailseite „Aggregate / Systemstatus“ zeigt den Online- oder Offline-Status des hostenden Aggregats an. Wenn der Aggregatstatus online ist, sind RAID-Festplattenprobleme nicht die Ursache dafür, dass das Volume offline ist.

2. Falls der Aggregatstatus offline ist, erfolgt die Auswahl von **Disk Information**; anschließend ist auf der Registerkarte **Disk Information** in der Liste **Events** nach Ereignissen für defekte Datenträger zu suchen.
3. Zur weiteren Identifizierung der defekten Datenträger dient der Hypertext-Link, der im Bereich **Related Devices** unter Node angezeigt wird.

   Die Seite mit den Details zu Cluster/Systemstatus wird angezeigt.

4. Nach einem Klick auf **Disks** und der Auswahl von **Broken** im Bereich **Filters** werden alle Disks im Status **Broken** aufgelistet.

   Wenn die defekten Festplatten den Offline-Status des Host-Aggregats verursacht haben, wird der Name des Aggregats in der Spalte Impacted Aggregate angezeigt.

Nach der Bestätigung, dass der Offline-Zustand des Volume durch defekte RAID-Festplatten und das daraus resultierende Offline-Host-Aggregat verursacht wird, ist eine Kontaktaufnahme mit dem zuständigen Administrator oder Bediener erforderlich, damit die defekten Festplatten manuell ausgetauscht und das Aggregat wieder online gebracht werden können.

Kapazitätsprobleme lösen

Kapazitätsprobleme in Active IQ Unified Manager beheben

Dieser Workflow enthält ein Beispiel dafür, wie Sie ein Kapazitätsproblem beheben können. In diesem Szenario sind Sie Administrator oder Operator und greifen auf die Unified ManagerDashboard Seite zu, um zu prüfen, ob bei den überwachten Storage Objekten Kapazitätsprobleme vorliegen. Sie möchten die mögliche Ursache des Problems und dessen Lösung ermitteln.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Auf der Dashboard-Seite ist im Bereich „Kapazität“ unter der Dropdown-Liste „Ereignisse“ nach einem Fehlerereignis mit der Meldung „`Volume Space Full`“ zu suchen.

Schritte

1. Im **Capacity**-Bereich der **Dashboard**-Seite den Namen des Fehlerereignisses „Volume Space Full“ auswählen.

   Die Seite mit den Ereignisdetails zum Fehler erscheint.

2. Auf der Detailseite **Event** können Sie eine oder mehrere der folgenden Aufgaben ausführen:
   - Im Feld „Ursache“ kann die Fehlermeldung geprüft werden; die Vorschläge unter „Vorgeschlagene Abhilfemaßnahmen“ führen zu Beschreibungen möglicher Abhilfemaßnahmen.
   - Wenn Sie im Feld „Quelle“ auf den Objektnamen, in diesem Fall ein Volume, klicken, werden Details zum Objekt angezeigt.
   - Möglicherweise wurden diesem Ereignis Notizen hinzugefügt.
   - Dem Ereignis eine Notiz hinzufügen.
   - Die Zuweisung des Ereignisses an einen anderen Benutzer ist möglich.
   - Quittierung des Ereignisses.
   - Das Ereignis als erledigt markieren.

Verwandte Informationen

"Seite mit Ereignisdetails"

Vorgeschlagene Korrekturmaßnahmen für ein volles Volume in Active IQ Unified Manager

Nach Erhalt eines Fehlerereignisses „`Volume Space Full`“ prüfen Sie die auf der Seite mit den Ereignisdetails vorgeschlagenen Abhilfemaßnahmen und entscheiden sich dafür, eine der vorgeschlagenen Maßnahmen auszuführen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Ein Benutzer mit einer beliebigen Rolle kann alle Aufgaben in diesem Workflow ausführen, bei denen Unified Manager verwendet wird.

In diesem Beispiel haben Sie auf der Unified ManagerEvent Management-Inventarseite ein Fehlerereignis „Volume Space Full“ gesehen und auf den Namen des Ereignisses geklickt.

Mögliche Abhilfemaßnahmen, die Sie für ein volles Volume durchführen könnten, umfassen unter anderem folgende:

- Aktivieren von automatischem Wachstum, Deduplizierung oder Komprimierung auf dem Volume
- Ändern der Größe oder Verschieben des Volumens
- Löschen oder Verschieben von Daten aus dem Volume

Obwohl alle diese Aktionen entweder über ONTAP System Manager oder die ONTAP CLI durchgeführt werden müssen, können Sie Unified Manager verwenden, um Informationen zu finden, die Sie möglicherweise benötigen, um zu entscheiden, welche Aktionen zu ergreifen sind.

Schritte

1. Auf der Detailseite **Event** lassen sich durch Klicken auf den Volume-Namen im Feld „Source“ Details zum betroffenen Volume anzeigen.
2. Auf der Detailseite **Volume / Health** ist unter **Configuration** zu sehen, dass Deduplizierung und Komprimierung für das Volume bereits aktiviert sind.

   Sie entscheiden sich, das Volume in der Größe anzupassen.
3. Im Bereich **Zugehörige Geräte** wählen Sie den Namen des Hosting-Aggregats aus, um zu prüfen, ob das Aggregat ein größeres Volume aufnehmen kann.
4. Auf der Detailseite **Aggregate / Health** sehen Sie, dass das Aggregat, das das volle Volume hostet, über genügend nicht zugesicherte Kapazität verfügt, sodass Sie ONTAP System Manager verwenden, um die Größe des Volume zu erhöhen und ihm mehr Kapazität zuzuweisen.

Verwandte Informationen

"Seite mit Ereignisdetails"

Systemstatusschwellenwerte verwalten

Informationen zu den Schwellenwerten für die Speicherkapazität in Active IQ Unified Manager

Ein Systemstatus-Schwellenwert für die Storage-Kapazität ist der Punkt, an dem der Unified Manager Server Ereignisse generiert, um Kapazitätsprobleme bei Storage-Objekten zu melden. Sie können Warnmeldungen so konfigurieren, dass bei jedem Auftreten solcher Ereignisse eine Benachrichtigung gesendet wird.

Die Systemstatus-Schwellenwerte für die Storage-Kapazität aller Aggregate, Volumes und qtrees sind auf Standardwerte eingestellt. Sie können die Einstellungen nach Bedarf für ein Objekt oder eine Gruppe von Objekten ändern.

Globale Einstellungen für Systemstatus-Schwellenwerte konfigurieren

Konfiguration der globalen Integritätsschwellenwerteinstellungen in Active IQ Unified Manager

Globale Systemstatus-Schwellenwertbedingungen für Kapazität, Wachstum, Snapshot-Reserve, Kontingente und Inodes können konfiguriert werden, um die Größe von Aggregaten, Volumes und qtrees effektiv zu überwachen. Außerdem lassen sich die Einstellungen für die Generierung von Ereignissen beim Überschreiten von Verzögerungsschwellenwerten bearbeiten.

Globale Systemstatus-Schwellenwerteinstellungen gelten für alle Objekte, denen sie zugeordnet sind, z. B. Aggregate, Volumes usw. Wenn Schwellenwerte überschritten werden, wird ein Ereignis generiert und, falls Warnungen konfiguriert sind, eine Warnungsbenachrichtigung gesendet. Für Schwellenwerte sind standardmäßig empfohlene Werte festgelegt, die Sie jedoch ändern können, damit in Intervallen Ereignisse generiert werden, die Ihren spezifischen Anforderungen entsprechen. Wenn Schwellenwerte geändert werden, werden Ereignisse im nächsten Überwachungszyklus generiert oder als veraltet markiert.

Globale Einstellungen für Systemstatus-Schwellenwerte sind im Abschnitt „Ereignisschwellenwerte“ des linken Navigationsmenüs verfügbar. Sie können die Schwellenwerteinstellungen auch für einzelne Objekte auf der Inventarseite oder auf der Detailseite des jeweiligen Objekts ändern.

- Informationen finden sich unter "Konfiguration globaler Schwellenwerte für den Aggregate-Systemstatus".

  Sie können die Systemstatus-Schwellenwerteinstellungen für Kapazität, Wachstum und Snapshot-Kopien für alle Aggregate konfigurieren, um jede Schwellenwertüberschreitung nachzuverfolgen.

- Informationen finden sich unter "Konfiguration globaler Schwellenwerte für den Volume-Systemstatus".

  Sie können die Einstellungen für die Systemstatusschwellenwerte für Kapazität, Snapshot Kopien, qtree Kontingente, Volume Wachstum, Reserveplatz für Überschreibungen und Inodes für alle Volumes bearbeiten, um jede Schwellenwertüberschreitung nachzuverfolgen.

- Informationen finden sich unter "Konfiguration globaler qtree Systemstatus-Schwellenwerte".

  Sie können die Systemstatus-Schwellenwerteinstellungen für die Kapazität aller qtrees bearbeiten, um jede Schwellenwertüberschreitung zu verfolgen.

- Informationen finden sich unter "Bearbeiten der Einstellungen für Systemstatusschwellenwerte der Verzögerung für nicht verwaltete Schutzbeziehungen".

  Sie können den Prozentsatz für die Verzögerungszeit bei Warnungen oder Fehlern erhöhen oder verringern, sodass Ereignisse in Intervallen auftreten, die besser Ihren Anforderungen entsprechen.

Konfiguration globaler Integritätsschwellenwerte für Aggregate in Active IQ Unified Manager

Sie können globale Systemstatus-Schwellenwerte für alle Aggregate konfigurieren, um jede Schwellenwertverletzung zu überwachen. Bei Schwellenwertverletzungen werden entsprechende Ereignisse generiert, auf deren Grundlage Präventivmaßnahmen möglich sind. Die globalen Werte lassen sich anhand bewährter Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten Aggregate gelten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Wenn Sie die Optionen global konfigurieren, werden die Standardwerte der Objekte geändert. Wenn die Standardwerte jedoch auf Objektebene geändert wurden, bleiben die globalen Werte unverändert.

Die Schwellenwertoptionen haben Standardwerte für eine bessere Überwachung, Sie können die Werte jedoch an die Anforderungen Ihrer Umgebung anpassen.

Wenn Autogrow auf Volumes aktiviert ist, die sich auf dem Aggregat befinden, gelten die Kapazitätsschwellenwerte des Aggregats anhand der von Autogrow festgelegten maximalen Volume-Größe als überschritten und nicht anhand der ursprünglichen Volume-Größe.

Die Systemstatus-Schwellenwerte gelten nicht für das Root-Aggregat des Knotens.

Schritte

1. Im linken Navigationsbereich ist **Ereignisschwellenwerte** > **Aggregat** auszuwählen.
2. Konfiguration der entsprechenden Schwellenwerte für Kapazität, Wachstum und Snapshot-Kopien.

3. Auf **Speichern** klicken.

Verwandte Informationen

"Hinzufügen von Benutzern"

Konfiguration globaler Schwellenwerte für den Volume-Integritätsstatus in Active IQ Unified Manager

Sie können die globalen Schwellenwerte für den Systemstatus aller Volumes konfigurieren, um jede Schwellenwertüberschreitung zu verfolgen. Überschreitungen der Systemstatus-Schwellenwerte lösen entsprechende Ereignisse aus, auf deren Grundlage Präventivmaßnahmen möglich sind. Sie können die globalen Werte anhand bewährter Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten Volumes gelten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die meisten Schwellenwertoptionen verfügen über Standardwerte für eine bessere Überwachung. Sie können die Werte jedoch an die Anforderungen Ihrer Umgebung anpassen.

Bei einem Volume mit aktiviertem Autogrow gelten Kapazitätsschwellenwerte auf Grundlage der durch Autogrow festgelegten maximalen Volume-Größe als überschritten, nicht auf Grundlage der ursprünglichen Volume-Größe.

> Der Standardwert von 1000 Snapshot-Kopien gilt nur für FlexVol Volumes, wenn die ONTAP-Version 9.4 oder höher ist, und für FlexGroup Volumes, wenn die ONTAP-Version 9.8 oder höher ist. Bei Clustern, auf denen ältere Versionen der ONTAP-Software installiert sind, beträgt die maximale Anzahl 250 Snapshot-Kopien pro Volume. Für diese älteren Versionen interpretiert Unified Manager die Zahl 1000 (und jede Zahl zwischen 1000 und 250) als 250; das bedeutet, dass Sie weiterhin Ereignisse erhalten, wenn die Anzahl der Snapshot-Kopien 250 erreicht. Wenn dieser Schwellenwert für diese älteren Versionen auf weniger als 250 gesetzt werden soll, muss der Schwellenwert hier in der Ansicht „Systemstatus: Alle Volumes“ oder auf der Detailseite „Volume / Systemstatus“ auf 250 oder weniger gesetzt werden.

Schritte

1. Auswahl im linken Navigationsbereich: **Event Thresholds** > **Volume**.
2. Konfiguration der entsprechenden Schwellenwerte für Kapazität, Snapshot Kopien, qtree Quotas, Volume-Wachstum und Inodes.
3. Auf **Speichern** klicken.

Verwandte Informationen

"Hinzufügen von Benutzern"

Konfiguration globaler Qtree-Integritätsschwellenwerte in Active IQ Unified Manager

Sie können die globalen Systemstatus-Schwellenwerte für alle qtrees konfigurieren, um jede Schwellenwertüberschreitung nachzuverfolgen. Bei Überschreitungen von Systemstatus-Schwellenwerten werden entsprechende Ereignisse generiert, auf deren Grundlage Sie Präventivmaßnahmen ergreifen können. Sie können die globalen Werte auf der Grundlage der Best-Practice-Einstellungen für Schwellenwerte konfigurieren, die

für alle überwachten qtrees gelten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die Schwellenwertoptionen haben Standardwerte für eine bessere Überwachung, Sie können die Werte jedoch an die Anforderungen Ihrer Umgebung anpassen.

Ereignisse werden für einen qtree nur dann generiert, wenn für den qtree ein Qtree-Kontingent oder ein Standardkontingent festgelegt wurde. Ereignisse werden nicht generiert, wenn der in einem Benutzer- oder Gruppenkontingent definierte Speicherplatz den Schwellenwert überschritten hat.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Ereignisschwellenwerte** > **Qtree**.
2. Die entsprechenden Kapazitätsschwellenwerte werden konfiguriert.
3. Auf **Speichern** klicken.

Konfiguration von Verzögerungsschwellenwerten für nicht verwaltete Schutzbeziehungen in Active IQ Unified Manager

Sie können die globalen Standard-Schwellenwerte für den Systemstatus von Verzögerungswarnungen und -fehlern für nicht verwaltete Schutzbeziehungen bearbeiten, sodass Ereignisse in Intervallen generiert werden, die Ihren Anforderungen entsprechen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die Verzögerungszeit darf das definierte Intervall des Übertragungszeitplans nicht überschreiten. Wenn der Übertragungszeitplan beispielsweise stündlich ist, darf die Verzögerungszeit nicht mehr als eine Stunde betragen. Der Verzögerungsschwellenwert gibt einen Prozentsatz an, den die Verzögerungszeit nicht überschreiten darf. Beim Beispiel von einer Stunde gilt: Wenn der Verzögerungsschwellenwert auf 150 % festgelegt ist, wird ein Ereignis ausgegeben, sobald die Verzögerungszeit mehr als 1,5 Stunden beträgt.

Die in dieser Aufgabe beschriebenen Einstellungen gelten global für alle nicht verwalteten Schutzbeziehungen. Sie können nicht exklusiv für eine einzelne nicht verwaltete Schutzbeziehung festgelegt und angewendet werden.

Schritte

1. Im linken Navigationsbereich können Sie **Event Thresholds** > **Relationship** auswählen.
2. Bei Bedarf lässt sich der globale Standardprozentsatz für die Warn- oder Fehlerverzögerungszeit erhöhen oder verringern.
3. Damit bei keinem Verzögerungsschwellenwert ein Warn- oder Fehlerereignis ausgelöst wird, muss das Kontrollkästchen neben **Enabled** deaktiviert sein.
4. Auf **Speichern** klicken.

Verwandte Informationen

"Hinzufügen von Benutzern"

Bearbeitung individueller Einstellungen für Integritätsgrenzwerte von Aggregaten in Active IQ Unified Manager

Sie können die Systemstatus-Schwellenwerteinstellungen für Aggregatkapazität, Wachstum und Snapshot-Kopien eines oder mehrerer Aggregate bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen generiert, und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, auf Grundlage des generierten Ereignisses Präventivmaßnahmen zu ergreifen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Auf Grundlage von Änderungen der Schwellenwerte werden Ereignisse im nächsten Überwachungszyklus generiert oder als veraltet markiert.

Wenn Autogrow auf Volumes aktiviert ist, die sich auf dem Aggregat befinden, gelten die Kapazitätsschwellenwerte des Aggregats anhand der von Autogrow festgelegten maximalen Volume-Größe als überschritten und nicht anhand der ursprünglichen Volume-Größe.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Aggregates**.
2. In der Ansicht **Systemstatus: Alle Aggregate** ist die Auswahl eines oder mehrerer Aggregate möglich; anschließend kann auf **Schwellenwerte bearbeiten** geklickt werden.
3. Im Dialogfeld **Edit Aggregate Thresholds** können Sie die Schwellenwerteinstellungen für eine der folgenden Kategorien bearbeiten: Kapazität, Wachstum oder Snapshot-Kopien, indem Sie das entsprechende Kästchen auswählen und anschließend die Einstellungen ändern.
4. Auf **Speichern** klicken.

Verwandte Informationen

"Hinzufügen von Benutzern"

Bearbeiten einzelner Einstellungen für Integritätsschwellenwerte von Volumes in Active IQ Unified Manager

Sie können die Systemstatus-Schwellenwerteinstellungen für Volume-Kapazität, Wachstum, Kontingent und Speicherplatzreserve eines oder mehrerer Volumes bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen generiert, und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, auf der Grundlage des generierten Ereignisses präventive Maßnahmen zu ergreifen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Auf Grundlage von Änderungen der Schwellenwerte werden Ereignisse im nächsten Überwachungszyklus generiert oder als veraltet markiert.

Bei einem Volume mit aktiviertem Autogrow gelten Kapazitätsschwellenwerte auf Grundlage der durch Autogrow festgelegten maximalen Volume-Größe als überschritten, nicht auf Grundlage der ursprünglichen Volume-Größe.

Der Standardwert von 1000 Snapshot-Kopien gilt nur für FlexVol Volumes, wenn die ONTAP-Version 9.4 oder höher ist, und für FlexGroup Volumes, wenn die ONTAP-Version 9.8 oder höher ist. Bei Clustern, auf denen ältere Versionen der ONTAP-Software installiert sind, beträgt die maximale Anzahl 250 Snapshot-Kopien pro Volume. Für diese älteren Versionen interpretiert Unified Manager die Zahl 1000 (und jede Zahl zwischen 1000 und 250) als 250; das bedeutet, dass Sie weiterhin Ereignisse erhalten, wenn die Anzahl der Snapshot-Kopien 250 erreicht. Wenn dieser Schwellenwert für diese älteren Versionen auf weniger als 250 gesetzt werden soll, muss der Schwellenwert hier in der Ansicht „Systemstatus: Alle Volumes“ oder auf der Detailseite „Volume / Systemstatus“ auf 250 oder weniger gesetzt werden.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. In der Ansicht **Systemstatus: Alle Volumes** lassen sich ein oder mehrere Volumes auswählen; anschließend kann auf **Schwellenwerte bearbeiten** geklickt werden.
3. Im Dialogfeld **Volume-Schwellenwerte bearbeiten** können Sie die Schwellenwerteinstellungen für eine der folgenden Optionen bearbeiten: Kapazität, Snapshot Kopien, qtree-Kontingent, Wachstum oder Inodes, indem Sie das entsprechende Kästchen auswählen und anschließend die Einstellungen ändern.
4. Auf **Speichern** klicken.

Verwandte Informationen

"Hinzufügen von Benutzern"

Individuelle qtree Integritätsschwellenwerte in Active IQ Unified Manager bearbeiten

Sie können die Systemstatus-Schwellenwerteinstellungen für die qtree-Kapazität für einen oder mehrere qtrees bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnmeldungen generiert, und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, anhand des generierten Ereignisses Präventivmaßnahmen zu ergreifen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Auf Grundlage von Änderungen der Schwellenwerte werden Ereignisse im nächsten Überwachungszyklus generiert oder als veraltet markiert.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Qtrees**.
2. In der Ansicht **Kapazität: Alle Qtrees** werden ein oder mehrere Qtrees ausgewählt, und anschließend wird auf **Schwellenwerte bearbeiten** geklickt.
3. Im Dialogfeld **Qtree-Schwellenwerte bearbeiten** lassen sich die Kapazitätsschwellenwerte für den ausgewählten qtree bzw. die ausgewählten qtrees ändern und anschließend **Speichern** auswählen.

Auch auf der Registerkarte „Qtrees“ der Seite „Storage VM / Systemstatusdetails“ lassen sich individuelle qtree-Schwellenwerte festlegen.

Cluster-Sicherheitsziele managen

Verwalten von Cluster-Sicherheitszielen in Active IQ Unified Manager

Unified Manager bietet ein Dashboard, das identifiziert, wie sicher Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes auf Basis der im *NetApp Security Hardening Guide for ONTAP 9* definierten Empfehlungen sind.

Ziel des Sicherheits-Dashboards ist es, alle Bereiche anzuzeigen, in denen Ihre ONTAP Cluster nicht mit den von NetApp empfohlenen Richtlinien übereinstimmen, sodass diese potenziellen Probleme behoben werden können. In den meisten Fällen werden die Probleme mithilfe von ONTAP System Manager oder der ONTAP CLI behoben. Ihr Unternehmen befolgt möglicherweise nicht alle Empfehlungen, sodass in manchen Fällen keine Änderungen erforderlich sind.

Ausführliche Empfehlungen und Lösungen finden Sie im "NetApp Security Hardening Guide für ONTAP 9" (TR-4569).

Zusätzlich zur Meldung des Sicherheitsstatus generiert Unified Manager auch Sicherheitsereignisse für jeden Cluster oder jede SVM mit Sicherheitsverstößen. Sie können diese Probleme auf der Bestandsseite der Ereignisverwaltung verfolgen und Warnmeldungen für diese Ereignisse konfigurieren, sodass Ihr Storage-Administrator benachrichtigt wird, wenn neue Sicherheitsereignisse auftreten.

Weitere Informationen sind unter "Welche Sicherheitskriterien werden bewertet" verfügbar.

Welche Sicherheitskriterien werden bewertet

Informationen dazu, wie Active IQ Unified Manager Sicherheitskriterien auswertet

Im Allgemeinen werden die Sicherheitskriterien für Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes anhand der Empfehlungen im *NetApp Security Hardening Guide for ONTAP 9* bewertet.

Zu den Sicherheitsüberprüfungen gehören unter anderem:

- ob ein Cluster ein sicheres Authentifizierungsverfahren wie SAML verwendet
- ob die Kommunikation zwischen den Peer-Clustern verschlüsselt ist
- ob für eine Storage VM das Revisionsprotokoll aktiviert ist
- ob für Ihre Volumes Software- oder Hardwareverschlüsselung aktiviert ist

Ausführliche Informationen enthalten die Themen zu Compliance-Kategorien und dem "NetApp Security Hardening Guide für ONTAP 9".

> Upgrade-Ereignisse, die von der Active IQ Plattform gemeldet werden, gelten ebenfalls als Sicherheitsereignisse. Diese Ereignisse kennzeichnen Probleme, deren Behebung ein Upgrade der ONTAP Software, der Node-Firmware oder der Betriebssystemsoftware erfordert (bei Sicherheitshinweisen). Diese Ereignisse werden nicht im Sicherheitsbereich angezeigt, sind aber auf der Bestandsseite für Event Management verfügbar.

Weitere Informationen sind unter "Management von Cluster-Sicherheitszielen" verfügbar.

Cluster Compliance Kategorien in Active IQ Unified Manager

Diese Tabelle beschreibt die Cluster-Sicherheits-Compliance-Parameter, die Unified Manager auswertet, die NetApp Empfehlung und ob der Parameter die Gesamtbewertung beeinflusst, ob der Cluster konform ist oder nicht.

Nicht konforme SVMs auf einem Cluster wirken sich auf den Compliance-Wert des Clusters aus. Daher kann es in manchen Fällen erforderlich sein, ein Sicherheitsproblem mit einer SVM zu beheben, bevor die Clustersicherheit als konform gilt.

Es ist zu beachten, dass nicht jeder der unten aufgeführten Parameter bei allen Installationen angezeigt wird. Wenn Sie beispielsweise keine Cluster-Peering-Beziehungen haben oder AutoSupport in einem Cluster deaktiviert haben, werden auf der UI-Seite die Elemente „Cluster Peering“ oder „AutoSupport HTTPS Transport“ nicht angezeigt.

Parameter	Beschreibung	Empfehlung	Beeinträchtigt die Cluster-Compliance
Globales FIPS	Zeigt an, ob der globale FIPS (Federal Information Processing Standard) 140-2-Compliance-Modus aktiviert oder deaktiviert ist. Wenn FIPS aktiviert ist, sind TLSv1 und SSLv3 deaktiviert, und nur TLSv1.1 und TLSv1.2 sind zulässig.	Aktiviert	Ja
Telnet	Zeigt an, ob der Telnet-Zugriff auf das System aktiviert oder deaktiviert ist. NetApp empfiehlt Secure Shell (SSH) für einen sicheren Fernzugriff.	Deaktiviert	Ja
Unsichere SSH-Einstellungen	Zeigt an, ob SSH unsichere Verschlüsselungsverfahren verwendet, z. B. solche, die mit *cbc beginnen.	Nein	Ja
Anmeldebanner	Zeigt an, ob das Anmeldebanner für Benutzer, die auf das System zugreifen, aktiviert oder deaktiviert ist.	Aktiviert	Ja

Parameter	Beschreibung	Empfehlung	Beeinträchtigt die Cluster-Compliance
Cluster-Peering	Gibt an, ob die Kommunikation zwischen gepeerten Clustern verschlüsselt oder unverschlüsselt ist. Die Verschlüsselung muss sowohl auf dem Quell- als auch auf dem Zielcluster konfiguriert sein, damit dieser Parameter als konform gilt.	Verschlüsselt	Ja
Netzwerkzeitprotokoll	Zeigt an, ob der Cluster einen oder mehrere konfigurierte NTP-Server besitzt. Für Redundanz und optimalen Service empfiehlt NetApp, dem Cluster mindestens drei NTP-Server zuzuordnen.	Konfiguriert	Ja
OCSP	Ab 9.14.1 stellt Active IQ Unified Manager Statusinformationen zum Online Certificate Status Protocol (OCSP) auf Ebene der Storage Virtual Machine (SVM, früher als Vserver bezeichnet) bereit. Dies bedeutet, dass die OCSP-Validierung auf alle zur SVM hergestellten SSL/TLS-Verbindungen angewendet wird und die Integrität und Gültigkeit der in diesen Verbindungen verwendeten Zertifikate sicherstellt.	Aktiviert	Nein
Remote-Revisionsprotokollierung	Gibt an, ob die Protokollweiterleitung (Syslog) verschlüsselt oder nicht verschlüsselt ist.	Verschlüsselt	Ja
AutoSupport HTTPS-Transport	Gibt an, ob HTTPS als Standardtransportprotokoll zum Senden von AutoSupport Nachrichten an den NetApp Support verwendet wird.	Aktiviert	Ja

Parameter	Beschreibung	Empfehlung	Beeinträchtigt die Cluster-Compliance
Standard-Admin-Benutzer	Zeigt an, ob der Standard-Administratorbenutzer (integriert) aktiviert oder deaktiviert ist. NetApp empfiehlt, nicht benötigte integrierte Konten zu sperren (zu deaktivieren).	Deaktiviert	Ja
SAML Benutzer	Zeigt an, ob SAML konfiguriert ist. SAML ermöglicht die Konfiguration der Multi-Faktor-Authentifizierung (MFA) als Anmeldemethode für Single Sign-On.	Nein	Nein
Active Directory Benutzer	Zeigt an, ob Active Directory konfiguriert ist. Active Directory und LDAP sind die bevorzugten Authentifizierungsmechanismen für Benutzer, die auf Cluster zugreifen.	Nein	Nein
LDAP-Benutzer	Gibt an, ob LDAP konfiguriert ist. Active Directory und LDAP sind gegenüber lokalen Benutzern die bevorzugten Authentifizierungsmechanismen für Benutzer, die Cluster verwalten.	Nein	Nein
Zertifikatsbenutzer	Zeigt an, ob ein Benutzerzertifikat für die Anmeldung am Cluster konfiguriert ist.	Nein	Nein
Lokale Benutzer	Zeigt an, ob lokale Benutzer für die Anmeldung am Cluster konfiguriert sind.	Nein	Nein
Remote Shell	Zeigt an, ob RSH aktiviert ist. Aus Sicherheitsgründen sollte RSH deaktiviert sein. Secure Shell (SSH) wird für sicheren Fernzugriff bevorzugt.	Deaktiviert	Ja

Parameter	Beschreibung	Empfehlung	Beeinträchtigt die Cluster-Compliance
MD5 im Einsatz	Zeigt an, ob ONTAP Benutzerkonten die weniger sichere MD5 Hashfunktion verwenden. Die Migration von MD5 gehashten Benutzerkonten zu einer sichereren kryptografischen Hashfunktion wie SHA-512 wird empfohlen.	Nein	Ja
Zertifikatsausstellertyp	Gibt die Art des verwendeten digitalen Zertifikats an.	CA-signiert	Nein

Grundlegendes zu den Konformitätskategorien von Storage VMs in Active IQ Unified Manager

Diese Tabelle beschreibt die Sicherheits-Compliance-Kriterien für Storage Virtual Machine (SVM), die Unified Manager auswertet, die NetApp Empfehlung und ob der Parameter die Gesamtbewertung beeinflusst, ob die SVM konform ist oder nicht.

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM Compliance
Audit-Protokoll	Zeigt an, ob die Audit-Protokollierung aktiviert oder deaktiviert ist.	Aktiviert	Ja
Unsichere SSH-Einstellungen	Zeigt an, ob SSH unsichere Verschlüsselungsverfahren verwendet, zum Beispiel solche, die mit `cbc*` beginnen.	Nein	Ja
Anmeldebanner	Zeigt an, ob das Anmeldebanner für Benutzer, die auf SVMs im System zugreifen, aktiviert oder deaktiviert ist.	Aktiviert	Ja
LDAP Verschlüsselung	Zeigt an, ob die LDAP-Verschlüsselung aktiviert oder deaktiviert ist.	Aktiviert	Nein
NTLM-Authentifizierung	Zeigt an, ob die NTLM-Authentifizierung aktiviert oder deaktiviert ist.	Aktiviert	Nein

Parameter	Beschreibung	Empfehlung	Beeinträchtigt SVM Compliance
LDAP Nutzdatensignierung	Zeigt an, ob die LDAP-Payload-Signierung aktiviert oder deaktiviert ist.	Aktiviert	Nein
CHAP Einstellungen	Zeigt an, ob CHAP aktiviert oder deaktiviert ist.	Aktiviert	Nein
Kerberos V5	Zeigt an, ob die Kerberos V5 Authentifizierung aktiviert oder deaktiviert ist.	Aktiviert	Nein
NIS-Authentifizierung	Zeigt an, ob die Verwendung der NIS-Authentifizierung konfiguriert ist.	Deaktiviert	Nein
FPolicy Status Aktiv	Zeigt an, ob eine FPolicy erstellt wurde oder nicht.	Ja	Nein
SMB-Verschlüsselung aktiviert	Gibt an, ob SMB Signing und Sealing nicht aktiviert ist.	Ja	Nein
SMB Signierung aktiviert	Gibt an, ob die SMB Signierung nicht aktiviert ist.	Ja	Nein

Konformitätskategorien für Volumes in Active IQ Unified Manager

Diese Tabelle beschreibt die Parameter der Volumenverschlüsselung, die Unified Manager auswertet, um festzustellen, ob die Daten auf Ihren Volumes ausreichend vor dem Zugriff durch unbefugte Benutzer geschützt sind.

Die Parameter der Volume-Verschlüsselung haben keinen Einfluss darauf, ob der Cluster oder die Storage VM als konform gilt.

Parameter	Beschreibung
Softwareverschlüsselt	Zeigt die Anzahl der Volumes an, die mit den Software-Verschlüsselungslösungen NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) geschützt sind.
Hardware-verschlüsselt	Zeigt die Anzahl der Volumes an, die mit der Hardwareverschlüsselung NetApp Storage Encryption (NSE) geschützt sind.
Software- und hardwareverschlüsselt	Zeigt die Anzahl der Volumes an, die sowohl durch Software- als auch durch Hardwareverschlüsselung geschützt sind.
Nicht verschlüsselt	Zeigt die Anzahl der nicht verschlüsselten Volumes an.

Informationen zum Compliance-Status von Clustern und SVMs in Active IQ Unified Manager

Clusters und Storage Virtual Machines (SVMs) gelten als nicht konform, wenn eines der Sicherheitskriterien, die anhand der Empfehlungen im *NetApp Security Hardening Guide for ONTAP 9* bewertet werden, nicht erfüllt ist. Zusätzlich gilt ein Cluster als nicht konform, wenn eine SVM als nicht konform gekennzeichnet ist.

Die Statussymbole auf den Sicherheitskarten haben in Bezug auf ihre Compliance die folgenden Bedeutungen:

- - Der Parameter ist wie empfohlen konfiguriert.
- - Der Parameter ist nicht wie empfohlen konfiguriert.
- - Entweder ist die Funktionalität im Cluster nicht aktiviert oder der Parameter ist nicht wie empfohlen konfiguriert, aber dieser Parameter trägt nicht zur Compliance des Objekts bei.

Der Status der Volume-Verschlüsselung hat keinen Einfluss darauf, ob der Cluster oder die SVM als konform gelten.

Sicherheitsstatus für Cluster und Storage VMs in Active IQ Unified Manager anzeigen

Active IQ Unified Manager ermöglicht Ihnen, den Sicherheitsstatus der Storage Objekte in Ihrer Umgebung an verschiedenen Stellen der Benutzeroberfläche anzuzeigen. Sie können Informationen und Berichte anhand definierter Parameter erfassen und analysieren sowie verdächtiges Verhalten oder unautorisierte Systemänderungen auf den überwachten Clustern und Storage VMs erkennen.

Die Sicherheitsempfehlungen finden Sie unter "NetApp Security Hardening Guide für ONTAP 9"

Anzeigen des Sicherheitsstatus auf Objektebene auf der Seite „Sicherheit“

Als Systemadministrator können Sie auf der Seite **Sicherheit** Transparenz über die Sicherheitsstärke Ihrer ONTAP Cluster und Storage VMs auf Datacenter- und Standortebene erhalten. Die unterstützten Objekte sind Cluster, Storage VMs und Volumes. Die folgenden Schritte sind erforderlich:

Schritte

1. Im linken Navigationsbereich auf **Dashboard** klicken.
2. Je nachdem, ob der Sicherheitsstatus für alle überwachten Cluster oder für einen einzelnen Cluster angezeigt werden soll, erfolgt die Auswahl im Dropdown-Menü über **Alle Cluster** oder über einen einzelnen Cluster.
3. Im Bereich **Sicherheit** erfolgt ein Klick auf den Pfeil nach rechts. Die Seite **Sicherheit** wird angezeigt.

Durch Klicken auf die Balkendiagramme, Anzahlangaben und `View Reports` Links gelangen Sie zur Seite „Volumes“, „Clusters“ oder „Storage VMs“, auf der die entsprechenden Details angezeigt oder bei Bedarf Berichte erstellt werden können.

Auf der Seite „Sicherheit“ werden die folgenden Bereiche angezeigt:

- **Cluster Compliance**: der Sicherheitsstatus (Anzahl der Compliance-konformen bzw. nicht Compliance-konformen Cluster) aller Cluster in einem Datacenter
- **Storage VM Compliance**: der Sicherheitsstatus (Anzahl der Storage VMs, die konform oder nicht konform

sind) für alle Storage VMs in Ihrem Datacenter

- **Volume-Verschlüsselung**: der Verschlüsselungsstatus (Anzahl der verschlüsselten bzw. unverschlüsselten Volumes) aller Volumes in Ihrer Umgebung
- **Status des Ransomware-Schutzes auf Volume-Ebene**: der Sicherheitsstatus (Anzahl der Volumes mit aktiviertem oder deaktiviertem Ransomware-Schutz) aller Volumes in Ihrer Umgebung
- **Clusterauthentifizierung und Zertifikate**: die Anzahl der Cluster, die die jeweiligen Authentifizierungsverfahren wie SAML, Active Directory oder Zertifikate und lokale Authentifizierung verwenden. Das Panel zeigt außerdem die Anzahl der Cluster an, deren Zertifikate entweder abgelaufen sind oder in den nächsten 60 Tagen ablaufen.

Die Sicherheitsdetails aller Cluster finden Sie auf der Seite „Clusters“.

Die Detailseite **Clusters / Security** ermöglicht die Anzeige des Sicherheits-Compliance-Status auf Cluster-Level.

Schritte

1. Im linken Navigationsbereich **Storage > Clusters** auswählen.
2. Die Auswahl erfolgt über **Ansicht > Sicherheit > Alle Cluster**.

Standard-Sicherheitsparameter wie Global FIPS, Telnet, unsichere SSH-Einstellungen, Anmeldebanner, Netzwerkzeitprotokoll, AutoSupport HTTPS-Transport und der Status des Ablaufs des Clusterzertifikats werden angezeigt.

Sie können auf die ⋮ Schaltfläche „Weitere Optionen“ klicken und die Sicherheitsdetails auf der Seite **Security** von Unified Manager oder in System Manager anzeigen. Für die Anzeige der Details in System Manager sind gültige Anmeldeinformationen erforderlich.

> ⓘ Wenn ein Cluster über ein abgelaufenes Zertifikat verfügt, können Sie unter **Gültigkeit des Clusterzertifikats** auf `expired` klicken und es in System Manager (9.10.1 und höher) erneuern. Auf `expired` können Sie nicht klicken, wenn die System Manager Instanz älter als 9.10.1 ist.

Die Sicherheitsdetails aller Cluster sind auf der Seite „Storage VMs“ einsehbar.

Die Detailseite **Storage VMs / Security** ermöglicht die Anzeige des Status der Sicherheits-Compliance auf Storage-VM-Ebene.

Schritte

1. Die Auswahl erfolgt im linken Navigationsbereich über **Storage > Storage VMs**.
2. Die Auswahl erfolgt über **Ansicht > Sicherheit > Alle Speicher-VMs**. Eine Liste der Cluster mit den Sicherheitsparametern wird angezeigt.

Ein Standardüberblick über die Sicherheits-Compliance der Storage VMs ergibt sich aus der Überprüfung der Sicherheitsparameter wie Storage VMs, Cluster, Anmeldebanner, Revisionsprotokoll und unsichere SSH-Einstellungen.

Sie können auf die ⋮ Schaltfläche „Weitere Optionen“ klicken und die Sicherheitsdetails auf der Seite **Security** von Unified Manager oder in System Manager anzeigen. Für die Anzeige der Details in System Manager sind gültige Anmeldeinformationen erforderlich.

Details zur Anti-Ransomware-Sicherheit für Volumes und Storage VMs finden Sie unter "Anzeigen des Anti-Ransomware-Status aller Volumes und Storage VMs".

Sicherheitsereignisse, die möglicherweise Software- oder Firmware-Updates in Active IQ Unified Manager erfordern, können angezeigt werden

Es gibt bestimmte Sicherheitsereignisse, die den Wirkungsbereich „Upgrade“ haben. Diese Ereignisse werden von der Active IQ Plattform gemeldet und identifizieren Probleme, deren Behebung ein Upgrade der ONTAP Software, der Node-Firmware oder der Betriebssystemsoftware (bei Sicherheitshinweisen) erfordert.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Bei einigen dieser Probleme können möglicherweise sofortige Korrekturmaßnahmen erforderlich sein, während andere bis zur nächsten planmäßigen Wartung warten können. Alle diese Ereignisse können angezeigt und Benutzern zugewiesen werden, die die Probleme beheben können. Wenn es bestimmte Ereignisse für Sicherheitsupgrades gibt, zu denen Sie nicht benachrichtigt werden möchten, kann diese Liste bei der Identifizierung dieser Ereignisse helfen, damit sie deaktiviert werden können.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.

   Standardmäßig werden auf der Inventarseite „Event Management“ alle aktiven Ereignisse (Neu und Bestätigt) angezeigt.

2. Im Menü „View“ erfolgt die Auswahl von **Upgrade events**.

   Die Seite zeigt alle aktiven Upgrade-Sicherheitsereignisse an.

Anzeige, wie Cluster die Benutzerauthentifizierung auf allen Clustern in Active IQ Unified Manager verwalten

Die Sicherheitsseite zeigt die Arten der Authentifizierung an, die zur Benutzerauthentifizierung auf jedem Cluster verwendet werden, sowie die Anzahl der Benutzer, die mit der jeweiligen Art auf den Cluster zugreifen. Damit lässt sich überprüfen, ob die Benutzerauthentifizierung gemäß den Vorgaben Ihres Unternehmens sicher durchgeführt wird.

Schritte

1. Im linken Navigationsbereich auf **Dashboard** klicken.
2. Oben im Dashboard erfolgt die Auswahl **Alle Cluster** über das Dropdown-Menü.
3. Im Bereich **Sicherheit** führt ein Klick auf den Pfeil nach rechts zur Seite **Sicherheit**.
4. Auf der Karte **Cluster-Authentifizierung** ist die Anzahl der Benutzer zu sehen, die mit dem jeweiligen Authentifizierungstyp auf das System zugreifen.
5. Auf der Karte **Cluster Security** sehen Sie, welche Authentifizierungsmechanismen zur Authentifizierung von Benutzern auf den einzelnen Clustern verwendet werden.

Wenn einige Benutzer mit einer unsicheren Methode oder mit einer Methode, die von NetApp nicht empfohlen wird, auf das System zugreifen, können Sie diese Methode deaktivieren.

Der Verschlüsselungsstatus aller Volumes in Active IQ Unified Manager kann angezeigt werden

Sie können eine Liste aller Volumes und deren aktuellen Verschlüsselungsstatus einsehen, um festzustellen, ob die Daten auf Ihren Volumes ausreichend vor dem Zugriff durch unbefugte Benutzer geschützt sind.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Für ein Volume sind folgende Verschlüsselungsarten möglich:

- Software - Volumes, die mit den Softwareverschlüsselungslösungen NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) geschützt sind.
- Hardware - Volumes, die mit der Hardwareverschlüsselung NetApp Storage Encryption (NSE) geschützt sind.
- Software und Hardware - Volumes, die sowohl durch Software- als auch durch Hardwareverschlüsselung geschützt sind.
- Keine - Volumes, die nicht verschlüsselt sind.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Systemstatus** > **Volume-Verschlüsselung**
3. In der Ansicht **Systemstatus: Volume-Verschlüsselung** können Sie nach dem Feld **Verschlüsselungstyp** sortieren oder mithilfe des Filters Volumes anzeigen, die einen bestimmten Verschlüsselungstyp aufweisen oder die nicht verschlüsselt sind (Verschlüsselungstyp “None”).

Der Anti-Ransomware-Status aller Volumes und Speicher-VMs in Active IQ Unified Manager kann angezeigt werden

Sie können eine Liste aller Volumes und Storage VMs (SVMs) sowie deren aktuellen Anti-Ransomware-Status einsehen, um festzustellen, ob die Daten auf Ihren Volumes und SVMs ausreichend vor Ransomware-Angriffen geschützt sind.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Weitere Informationen zu den verschiedenen Anti-Ransomware-Status finden Sie unter "ONTAP: Anti-Ransomware aktivieren".

Sicherheitsdetails aller Volumes mit Anti-Ransomware-Erkennung

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“: **Systemstatus** > **Sicherheit** > **Anti-Ransomware**
3. In der Ansicht **Sicherheit: Anti-Ransomware** können Sie nach den verschiedenen Feldern sortieren oder den Filter verwenden.

> Anti-Ransomware wird für Offline-Volumes, eingeschränkte Volumes, SnapLock Volumes, FlexGroup Volumes, FlexCache Volumes, ausschließlich SAN-basierte Volumes, Volumes von

gestoppten Storage VMs, Root-Volumes von Storage VMs oder Datensicherungs-Volumes nicht unterstützt.

Anzeige der Sicherheitsdetails aller Storage VMs mit Anti-Ransomware-Erkennung

Schritte

1. Die Auswahl erfolgt im linken Navigationsbereich über **Storage > Storage VMs**.
2. **Ansicht > Sicherheit > Anti-Ransomware** auswählen. Eine Liste der SVMs mit dem Anti-Ransomware-Status wird angezeigt.

Die Anti-Ransomware-Überwachung wird auf Storage VMs, auf denen das NAS-Protokoll nicht aktiviert ist, nicht unterstützt.

Alle aktiven Sicherheitsereignisse in Active IQ Unified Manager anzeigen

Sie können alle aktiven Sicherheitsereignisse einsehen und jedes einzelne einem Benutzer zuweisen, der das Problem beheben kann. Falls Sie bestimmte Sicherheitsereignisse nicht erhalten möchten, hilft Ihnen diese Liste außerdem dabei, die zu deaktivierenden Ereignisse zu identifizieren.

Bevor Sie beginnen

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

Schritte

1. Im linken Navigationsbereich auf **Event Management** klicken.

   Standardmäßig zeigt die Inventarseite „Event Management“ neue und bestätigte Ereignisse an.

2. Im Menü „Ansicht“ ist die Option „Aktive Sicherheitsereignisse“ auszuwählen.

   Die Seite zeigt alle neuen und bestätigten Sicherheitsereignisse an, die in den letzten 7 Tagen generiert wurden.

Hinzufügen von Warnmeldungen für Sicherheitsereignisse in Active IQ Unified Manager

Sie können Benachrichtigungen für einzelne Sicherheitsereignisse genauso konfigurieren wie für alle anderen Ereignisse, die von Unified Manager empfangen werden. Außerdem können Sie, wenn alle Sicherheitsereignisse gleich behandelt werden sollen und eine E-Mail an dieselbe Person gesendet werden soll, eine einzelne Benachrichtigung erstellen, die Sie informiert, sobald Sicherheitsereignisse ausgelöst werden.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Das folgende Beispiel zeigt, wie eine Warnung für das Sicherheitsereignis “Telnet Protocol Enabled” erstellt wird. Dadurch wird eine Warnung gesendet, wenn der Telnet-Zugriff für den administrativen Fernzugriff auf den Cluster konfiguriert ist. Diese Vorgehensweise kann verwendet werden, um Warnungen für alle Sicherheitsereignisse zu erstellen.

Schritte

1. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
2. Auf der Seite **Alarmeinstellungen Hinzufügen** auswählen.
3. Im Dialogfeld **Warnung hinzufügen** auf **Name** klicken und einen Namen sowie eine Beschreibung für die Warnung eingeben.
4. Unter **Ressourcen** erfolgt die Auswahl des Clusters oder der Cluster, für den bzw. die diese Warnung aktiviert werden soll.
5. Nach Auswahl von **Events** können die folgenden Aktionen durchgeführt werden:
   a. In der Liste „Ereignisschweregrad“ wird die Option **Warnung** ausgewählt.
   b. In der Liste „Übereinstimmende Ereignisse“ ist **Telnet Protocol Enabled** auszuwählen.
6. Unter **Aktionen** folgt im Feld **Diese Benutzer benachrichtigen** die Auswahl des Namens des Benutzers, der die Benachrichtigungs-E-Mail erhalten soll.
7. Auf dieser Seite können alle weiteren Optionen für die Benachrichtigungshäufigkeit, das Auslösen von SNMP-Taps und das Ausführen eines Skripts konfiguriert werden.
8. Auf **Speichern** klicken.

Deaktivieren bestimmter Sicherheitsereignisse in Active IQ Unified Manager

Alle Ereignisse sind standardmäßig aktiviert. Sie können bestimmte Ereignisse deaktivieren, um zu verhindern, dass Benachrichtigungen für Ereignisse generiert werden, die in Ihrer Umgebung nicht relevant sind. Sie können deaktivierte Ereignisse wieder aktivieren, wenn Sie wieder Benachrichtigungen dafür erhalten möchten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Wenn Sie Ereignisse deaktivieren, werden die zuvor im System generierten Ereignisse als veraltet markiert, und die für diese Ereignisse konfigurierten Warnmeldungen werden nicht ausgelöst. Wenn Sie deaktivierte Ereignisse wieder aktivieren, werden die Benachrichtigungen für diese Ereignisse ab dem nächsten Überwachungszyklus generiert.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Ereigniseinrichtung**.
2. Auf der Seite **Event** Setup können Ereignisse deaktiviert oder aktiviert werden, indem eine der folgenden Optionen ausgewählt wird:

Wenn Sie möchten…	Fahren Sie dann wie folgt fort…
Ereignisse deaktivieren	a. Klicken Sie auf **Deaktivieren**. b. Im Dialogfeld „Ereignisse deaktivieren“ wird der Schweregrad **Warning** ausgewählt. Dies ist die Kategorie für alle Sicherheitsereignisse. c. In der Spalte „Übereinstimmende Ereignisse“ lassen sich die Sicherheitsereignisse auswählen, die deaktiviert werden sollen; anschließend lassen sich diese Ereignisse mit dem Pfeil nach rechts in die Spalte „Ereignisse deaktivieren“ verschieben. d. Anschließend erfolgt die Auswahl von **Save and Close**. e. Stellen Sie sicher, dass die deaktivierten Ereignisse in der Listenansicht der Seite „Ereigniseinrichtung“ angezeigt werden.
Ereignisse aktivieren	a. In der Liste der deaktivierten Ereignisse erfolgt die Auswahl des Kästchens für das Ereignis oder die Ereignisse, die wieder aktiviert werden sollen. b. Klicken Sie auf **Enable**.

Sicherheitsereignisse in Active IQ Unified Manager anzeigen

Sicherheitsereignisse liefern Ihnen Informationen zum Sicherheitsstatus von ONTAP Clustern, Storage Virtual Machines (SVMs) und Volumes basierend auf den im *NetApp Security Hardening Guide for ONTAP 9* definierten Parametern. Diese Ereignisse benachrichtigen Sie über potenzielle Probleme, sodass Sie deren Schweregrad bewerten und das Problem gegebenenfalls beheben können.

Sicherheitsereignisse sind nach Quelltyp gruppiert und enthalten den Ereignis- und Trap-Namen, das Auswirkungslevel und den Schweregrad. Diese Ereignisse werden in den Ereigniskategorien für Cluster und Storage VM angezeigt.

Verwaltung von Backup- und Wiederherstellungsvorgängen

Verwalten von Sicherungs- und Wiederherstellungsvorgängen in Active IQ Unified Manager

Sie können Backups von Active IQ Unified Manager erstellen und die Wiederherstellungsfunktion verwenden, um das Backup im Falle eines Systemausfalls oder Datenverlusts auf demselben (lokalen) System oder auf einem neuen (Remote-)System wiederherzustellen.

Es gibt drei Sicherungs- und Wiederherstellungsmethoden, abhängig vom Betriebssystem, auf dem Unified Manager installiert ist, und von der Anzahl der verwalteten Cluster und Knoten:

Betriebssystem	Größe der Bereitstellung	Empfohlene Backup-Methode
VMware vSphere	Beliebig	VMware Snapshot der virtuellen Unified Manager Appliance
Red Hat Enterprise Linux	Klein	Unified Manager MySQL-Datenbankdump
	Groß	NetApp Snapshot der Unified Manager Datenbank
Microsoft Windows	Klein	Unified Manager MySQL-Datenbankdump
	Groß	NetApp Momentaufnahme der Unified Manager Datenbank mit iSCSI-Protokoll

Eine Beschreibung dieser verschiedenen Methoden folgt in den nächsten Abschnitten.

Sicherung und Wiederherstellung für Active IQ Unified Manager auf einer virtuellen Appliance

Das Backup- und Wiederherstellungsmodell für Unified Manager bei der Installation auf einer virtuellen Appliance ist das Erfassen und Wiederherstellen eines Images der vollständigen virtuellen Applikation.

Die folgenden Schritte ermöglichen Ihnen die Erstellung einer Sicherung der virtuellen Appliance:

1. Erforderlich sind das Ausschalten der VM und das Erstellen eines VMware Snapshot der virtuellen Unified Manager Appliance.
2. Sie können auf dem Datenspeicher eine NetApp Snapshot Kopie erstellen, um den VMware Snapshot zu erfassen.

   Wenn der Datenspeicher nicht auf einem System gehostet wird, auf dem ONTAP software ausgeführt wird, erfolgt das Erstellen einer Sicherung des VMware-Snapshots gemäß den Richtlinien des Storage-Herstellers.

3. Replizieren der NetApp Snapshot-Kopie oder eines gleichwertigen Snapshots in einen alternativen Storage.
4. Den VMware Snapshot löschen.

Mithilfe dieser Aufgaben lässt sich ein Backup-Zeitplan implementieren, damit die virtuelle Appliance Unified Manager geschützt ist, falls Probleme auftreten.

Um die VM wiederherzustellen, können Sie den von Ihnen erstellten VMware Snapshot verwenden, um die VM in den zeitpunktgenauen Zustand zum Zeitpunkt der Sicherung zurückzusetzen.

Sicherung und Wiederherstellung mithilfe eines MySQL Datenbank-Dumps

Sicherung und Wiederherstellung mithilfe eines MySQL Datenbank-Dumps in Active IQ Unified Manager

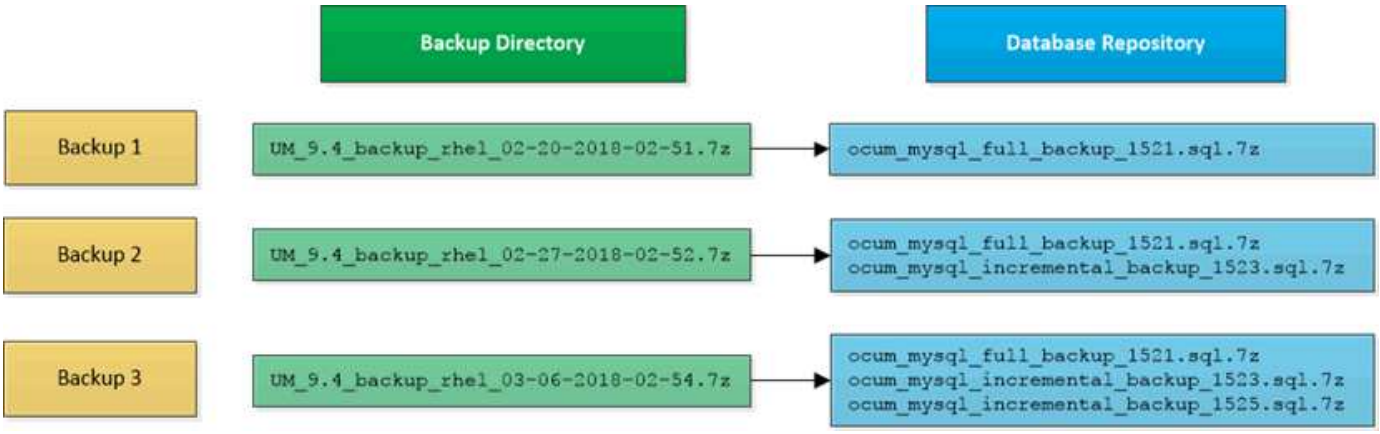
Ein MySQL Datenbank-Dump-Backup ist eine Kopie der Active IQ Unified Manager Datenbank und der Konfigurationsdateien, die Sie im Falle eines Systemausfalls oder Datenverlusts verwenden können. Sie können ein Backup so planen, dass es an einem

lokalen oder an einem Remote-Ziel gespeichert wird. Es wird dringend empfohlen, einen Remote-Speicherort zu definieren, der sich außerhalb des Active IQ Unified Manager Hostsystems befindet.

Der MySQL Datenbank-Dump ist der Standardmechanismus für Backups, wenn Unified Manager auf einem Linux- oder Windows-Server installiert ist. Wenn Unified Manager jedoch eine große Anzahl von Clustern und Nodes managt oder Ihre MySQL Backups viele Stunden für den Abschluss benötigen, können Sie mit Snapshot Kopien sichern. Diese Funktion ist unter Red Hat Enterprise Linux und Windows verfügbar.

Ein Datenbank-Dump-Backup besteht aus einer einzelnen Datei im Backup-Verzeichnis und einer oder mehreren Dateien im Datenbank-Repository-Verzeichnis. Die Datei im Backup-Verzeichnis ist sehr klein, da sie lediglich einen Verweis auf die Dateien im Datenbank-Repository-Verzeichnis enthält, die zum Neuerstellen des Backups erforderlich sind.

Beim ersten Erstellen einer Datenbanksicherung wird eine einzelne Datei im Sicherungsverzeichnis erstellt, und im Verzeichnis des Datenbank-Repositorys wird eine vollständige Sicherungsdatei erstellt. Beim nächsten Erstellen einer Sicherung wird eine einzelne Datei im Sicherungsverzeichnis erstellt, und im Verzeichnis des Datenbank-Repositorys wird eine inkrementelle Sicherungsdatei erstellt, die die Unterschiede zur vollständigen Sicherungsdatei enthält. Dieser Vorgang wird beim Erstellen weiterer Sicherungen bis zur maximalen Aufbewahrungseinstellung fortgesetzt, wie in der folgenden Abbildung dargestellt.



In diesen beiden Verzeichnissen dürfen keine Sicherungsdateien umbenannt oder entfernt werden, andernfalls schlägt jeder nachfolgende Wiederherstellungsvorgang fehl.

Wenn Sie Ihre Sicherungsdateien auf dem lokalen System speichern, sollten Sie einen Prozess starten, der die Sicherungsdateien an einen entfernten Speicherort kopiert, damit sie im Falle eines Systemproblems, das eine vollständige Wiederherstellung erfordert, verfügbar sind.

Vor Beginn eines Sicherungsvorgangs führt Active IQ Unified Manager eine Integritätsprüfung durch, um sicherzustellen, dass alle erforderlichen Sicherungsdateien und Sicherungsverzeichnisse vorhanden und beschreibbar sind. Außerdem prüft Active IQ Unified Manager, ob auf dem System ausreichend Speicherplatz zum Erstellen der Sicherungsdatei verfügbar ist.

Konfiguration der Einstellungen für die Datenbank-Dumpsicherung in Active IQ Unified Manager

Sie können die Einstellungen für das Datenbank-Dump-Backup in Unified Manager konfigurieren, um den Datenbank-Backup-Pfad, die Anzahl der Aufbewahrungen und den Backup-Zeitplan festzulegen. Sie können täglich oder wöchentlich geplante Backups

aktivieren. Standardmäßig sind geplante Backups deaktiviert, es sollte jedoch ein Backup-Zeitplan festgelegt werden.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Sie müssen über mindestens 150 GB freien Speicherplatz an dem von Ihnen als Sicherungspfad definierten Ort verfügen.

  Es wird empfohlen, einen Remote-Standort zu verwenden, der sich außerhalb des Unified Manager Host-Systems befindet.

- Wenn Unified Manager auf einem Linux-System installiert ist und MySQL Backup verwendet wird, sind für das Backup-Verzeichnis die folgenden Berechtigungen und Besitzverhältnisse erforderlich.

  Berechtigungen: 0750, Eigentümer: jboss:maintenance

- Wenn Unified Manager auf einem Windows-System installiert ist und MySQL-Backup verwendet wird, muss sichergestellt werden, dass nur der Administrator Zugriff auf das Backup-Verzeichnis hat.

Die erste Datensicherung benötigt mehr Zeit als nachfolgende, da es sich um eine vollständige Sicherung handelt. Eine vollständige Sicherung kann über 1 GB groß sein und drei bis vier Stunden dauern. Nachfolgende Sicherungen sind inkrementell und benötigen weniger Zeit.

- Wenn Sie feststellen, dass die Anzahl der inkrementellen Sicherungsdateien für den den Sicherungen zugewiesenen Speicherplatz zu groß ist, können Sie regelmäßig eine vollständige Sicherung erstellen, um die alte Sicherung und ihre inkrementellen Dateien zu ersetzen. Alternativ können Sie eine Sicherung mithilfe von Snapshot-Kopien erstellen.
- Ein Backup, das in den ersten 15 Tagen nach dem Hinzufügen eines neuen Clusters erstellt wurde, ist möglicherweise nicht genau genug, um die historischen Performance-Daten zu erhalten.

Schritte

1. Im linken Navigationsbereich können Sie **General** > **Database Backup** auswählen.
2. Auf der Seite **Datenbanksicherung** können die **Sicherungseinstellungen** ausgewählt werden.
3. Die entsprechenden Werte für einen Sicherungspfad, die Anzahl der aufzubewahrenden Backups und den Zeitplan werden konfiguriert.

   Der Standardwert für die Anzahl der Aufbewahrungen ist 10; Sie können 0 verwenden, um eine unbegrenzte Anzahl von Backups zu erstellen.

4. Sie wählen die Schaltfläche **Scheduled Daily** oder **Scheduled Weekly** aus und geben anschließend die Details des Zeitplans an.
5. Auf **Anwenden** klicken.

Die Sicherungsdateien des Datenbank-Dumps werden gemäß dem Zeitplan erstellt. Auf der Seite „Datenbanksicherung“ können Sie die verfügbaren Sicherungsdateien einsehen.

Informationen zur Wiederherstellung der Datenbank in Active IQ Unified Manager

Die Wiederherstellung einer MySQL-Datenbank ist der Vorgang, bei dem eine vorhandene Unified Manager Sicherungsdatei auf demselben oder auf einem anderen

Unified Manager Server wiederhergestellt wird. Sie führen den Wiederherstellungsvorgang über die Unified Manager Wartungs-Managementplattform aus.

Wenn Sie eine Wiederherstellung auf demselben (lokalen) System durchführen und alle Sicherungsdateien lokal gespeichert sind, können Sie die Wiederherstellungsoption mit dem Standardspeicherort ausführen. Wenn Sie eine Wiederherstellung auf einem anderen Unified Manager System (einem Remote-System) durchführen, müssen Sie die Sicherungsdatei oder die Sicherungsdateien aus dem sekundären Storage auf die lokale Festplatte kopieren, bevor Sie die Wiederherstellungsoption ausführen.

Während des Wiederherstellungsprozesses werden Sie von Unified Manager abgemeldet. Sie können sich nach Abschluss des Wiederherstellungsprozesses wieder im System anmelden.

Wenn Sie das Sicherungsabbild auf einem neuen Server wiederherstellen, müssen Sie nach Abschluss der Wiederherstellung ein neues HTTPS-Sicherheitszertifikat generieren und den Unified Manager Server neu starten. Gegebenenfalls müssen Sie auch die SAML-Authentifizierungseinstellungen neu konfigurieren, wenn Sie das Sicherungsabbild auf einem neuen Server wiederherstellen.

> Alte Sicherungsdateien können nach einem Upgrade von Unified Manager auf eine neuere Softwareversion nicht mehr zur Wiederherstellung eines Images verwendet werden. Um Speicherplatz zu sparen, werden beim Upgrade von Unified Manager alle alten Sicherungsdateien außer der neuesten automatisch gelöscht.

Verwandte Informationen

"Generieren eines HTTPS-Sicherheitszertifikats"

"Aktivieren der SAML-Authentifizierung"

"Authentifizierung mit Active Directory oder OpenLDAP"

Wiederherstellung einer MySQL Datenbank Sicherung auf einem Linux-System in Active IQ Unified Manager

Bei Datenverlust oder Datenbeschädigung können Sie Unified Manager mit minimalem Datenverlust in den vorherigen stabilen Zustand zurückversetzen. Sie können die Unified Manager Datenbank mithilfe der Unified Manager Managementplattform auf einem lokalen oder entfernten Red Hat Enterprise Linux-System wiederherstellen.

Bevor Sie beginnen

- Sie benötigen die Anmeldedaten des Root-Benutzers für den Linux-Host, auf dem Unified Manager installiert ist.
- Sie müssen über eine Benutzerkennung und ein Passwort verfügen, die für die Anmeldung an der Managementplattform für die Wartung des Unified Manager Servers autorisiert sind.
- Sie müssen die Sicherungsdatei des Unified Manager und den Inhalt des Datenbank-Repository-Verzeichnisses auf das System kopiert haben, auf dem Sie den Wiederherstellungsvorgang durchführen werden.

  Es wird empfohlen, die Sicherungsdatei in das Standardverzeichnis `/data/ocum`-backup zu kopieren. Die Datenbank-Repository-Dateien müssen in das Unterverzeichnis `/database-dumps-repo` unter dem Verzeichnis `/ocum-backup` kopiert werden.

- Die Sicherungsdateien müssen vom `.7z` Typ sein.

Die Wiederherstellungsfunktion ist plattform- und versionsspezifisch. Eine Unified Manager Sicherung kann nur auf derselben Version von Unified Manager wiederhergestellt werden. Sie können eine Linux-Sicherungsdatei oder eine Sicherungsdatei einer virtuellen Appliance auf einem Red Hat Enterprise Linux-System wiederherstellen.

Enthält der Name des Sicherungsordners ein Leerzeichen, muss der absolute oder relative Pfad in doppelte Anführungszeichen gesetzt werden.

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, sollte nach der Installation von Unified Manager nach Abschluss der Installation weder die Benutzeroberfläche gestartet noch Cluster, Benutzer oder Authentifizierungseinstellungen konfiguriert werden. Die Sicherungsdatei ergänzt diese Informationen während des Wiederherstellungsprozesses.
2. Die Verbindung mit der IP-Adresse oder dem vollqualifizierten Domainnamen des Unified Manager Systems erfolgt mithilfe von Secure Shell.
3. Die Anmeldung am System erfolgt mit dem Benutzernamen und Passwort des Wartungsbenutzers (umadmin).
4. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.
5. Im **Main Menu** der Wartungskonsole erfolgt die Eingabe der Nummer für die Option **Backup Restore**.
6. Erforderlich ist die Eingabe der Nummer für **Restore MySQL Backup**.
7. Bei entsprechender Aufforderung erfolgt die Eingabe des absoluten Pfads der Sicherungsdatei.

   ```
   Bundle to restore from: /data/ocum-
   backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
   ```

   Nach Abschluss des Wiederherstellungsvorgangs können Sie sich bei Unified Manager anmelden.

Falls der OnCommand Workflow Automation Server nach dem Wiederherstellen der Sicherung nicht funktioniert, sind die folgenden Schritte erforderlich:

1. Auf dem Workflow Automation Server muss die IP-Adresse des Unified Manager Servers auf den neuesten Rechner umgestellt werden.
2. Wenn die Datenerfassung in Schritt 1 fehlschlägt, muss auf dem Unified Manager Server das Datenbankpasswort zurückgesetzt werden.

Wiederherstellung einer MySQL Datenbank Sicherung unter Windows in Active IQ Unified Manager

Im Falle eines Datenverlusts oder einer Datenbeschädigung können Sie die Wiederherstellungsfunktion verwenden, um Unified Manager mit minimalem Datenverlust in den vorherigen stabilen Zustand wiederherzustellen. Sie können die Unified Manager MySQL-Datenbank mithilfe der Unified Manager Managementplattform auf einem lokalen Windows-System oder einem entfernten Windows-System wiederherstellen.

Bevor Sie beginnen

- Sie benötigen Windows-Administratorrechte.

- Sie müssen die Sicherungsdatei des Unified Manager und den Inhalt des Datenbank-Repository-Verzeichnisses auf das System kopiert haben, auf dem Sie den Wiederherstellungsvorgang durchführen werden.

  Es wird empfohlen, die Sicherungsdatei in das Standardverzeichnis `\ProgramData\NetApp\OnCommandAppData\ocum\backup` zu kopieren. Die Dateien des Datenbank-Repositorys müssen in das `\database_dumps_repo` Unterverzeichnis des `\backup` Verzeichnisses kopiert werden.

- Die Sicherungsdateien müssen vom `.7z` Typ sein.

Die Wiederherstellungsfunktion ist plattform- und versionsspezifisch. Sie können eine Unified Manager MySQL-Sicherung nur auf derselben Unified Manager Version wiederherstellen, und eine Windows-Sicherung lässt sich nur auf einer Windows-Plattform wiederherstellen.



Wenn die Ordnernamen ein Leerzeichen enthalten, ist der absolute oder relative Pfad der Sicherungsdatei in doppelten Anführungszeichen anzugeben.

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, sollte nach der Installation von Unified Manager nach Abschluss der Installation weder die Benutzeroberfläche gestartet noch Cluster, Benutzer oder Authentifizierungseinstellungen konfiguriert werden. Die Sicherungsdatei ergänzt diese Informationen während des Wiederherstellungsprozesses.
2. Für die Anmeldung am Unified Manager System werden Administratoranmeldedaten verwendet.
3. PowerShell oder die Eingabeaufforderung wird als Windows-Administrator gestartet.
4. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.
5. Im **Main Menu** der Wartungskonsole erfolgt die Eingabe der Nummer für die Option **Backup Restore**.
6. Erforderlich ist die Eingabe der Nummer für **Restore MySQL Backup**.
7. Bei entsprechender Aufforderung erfolgt die Eingabe des absoluten Pfads der Sicherungsdatei.

   ```
   Bundle to restore from:
   \ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac
   kup_windows_02-20-2020-02-51.7z
   ```

   Nach Abschluss des Wiederherstellungsvorgangs können Sie sich bei Unified Manager anmelden.

Falls der OnCommand Workflow Automation Server nach dem Wiederherstellen der Sicherung nicht funktioniert, sind die folgenden Schritte erforderlich:

1. Auf dem Workflow Automation Server muss die IP-Adresse des Unified Manager Servers auf den neuesten Rechner umgestellt werden.
2. Wenn die Datenerfassung in Schritt 1 fehlschlägt, muss auf dem Unified Manager Server das Datenbankpasswort zurückgesetzt werden.

Sicherung und Wiederherstellung mithilfe von NetApp Snapshots

Sicherung und Wiederherstellung mithilfe von NetApp Snapshots in Active IQ Unified Manager

Eine NetApp Snapshot Kopie erstellt ein zeitpunktgenaues Image der Unified Manager Datenbank und der Konfigurationsdateien, das im Falle eines Systemausfalls oder Datenverlusts zur Wiederherstellung verwendet werden kann. Die Snapshot Kopie wird regelmäßig in ein Volume auf einem Ihrer ONTAP Cluster geschrieben, damit stets eine aktuelle Kopie verfügbar ist.

Diese Funktionalität ist für Active IQ Unified Manager, der auf einer virtuellen Appliance installiert ist, nicht verfügbar.

Konfiguration der Sicherung unter Linux in Active IQ Unified Manager

Wenn Ihr Active IQ Unified Manager auf einem Linux-Rechner installiert ist, können Sie Ihr Backup und Ihre Wiederherstellung mithilfe von NetApp Snapshots konfigurieren.

Snapshot-Kopien benötigen nur sehr wenig Zeit, in der Regel nur wenige Minuten, und die Unified Manager Datenbank ist nur für einen sehr kurzen Zeitraum gesperrt, sodass es nur zu sehr geringen Beeinträchtigungen Ihrer Installation kommt. Das Image benötigt nur minimalen Storage-Platz und verursacht einen vernachlässigbaren Performance-Overhead, da nur Änderungen an Dateien seit der letzten Snapshot-Kopie aufgezeichnet werden. Da der Snapshot auf einem ONTAP Cluster erstellt wird, können bei Bedarf andere NetApp Funktionen wie SnapMirror genutzt werden, um einen sekundären Schutz zu erstellen.

Vor Beginn eines Sicherungsvorgangs führt Unified Manager eine Integritätsprüfung durch, um sicherzustellen, dass das Zielsystem verfügbar ist.

- Eine Snapshot-Kopie kann nur in derselben Version von Active IQ Unified Manager wiederhergestellt werden.

  Wurde beispielsweise ein Backup auf Unified Manager 9.18 erstellt, lässt es sich nur auf Unified Manager 9.18 Systemen wiederherstellen.

- Jede Änderung an der Snapshot-Konfiguration kann dazu führen, dass der Snapshot ungültig wird.

Konfiguration des Speicherorts für Snapshot Kopien in Active IQ Unified Manager

Sie können mit ONTAP System Manager oder der ONTAP CLI das Volume konfigurieren, in dem Snapshot-Kopien auf einem Ihrer ONTAP Cluster gespeichert werden.

Bevor Sie beginnen

Der Cluster, die Storage VM und das Volume müssen die folgenden Anforderungen erfüllen:

- Clusteranforderungen:
  - ONTAP 9.3 oder höher muss installiert sein
  - Es sollte sich in geografischer Nähe zum Unified Manager Server befinden
  - Es kann von Unified Manager überwacht werden, ist aber nicht erforderlich
- Anforderungen an die Storage VM:
  - Der Namensschalter und die Namenszuordnung müssen so eingestellt sein, dass “files” verwendet wird

- Lokale Benutzer, die den Client-seitigen Benutzern entsprechen
- Stellen Sie sicher, dass „Alle Lese-/Schreibzugriffe“ ausgewählt ist
- Der Superuser-Zugriff sollte in der Exportrichtlinie auf „`any`“ gesetzt sein.
- NFS für NetApp Snapshot für Linux
- NFSv4 muss auf dem NFS-Server aktiviert sein, und die NFSv4-ID-Domäne muss auf dem Client und der Storage VM angegeben sein
- Das Volume sollte mindestens doppelt so groß sein wie das Verzeichnis Unified Manager/opt/netapp/data

  Die aktuelle Größe lässt sich mit dem Befehl du -sh /opt/netapp/data/ überprüfen.

- Volume-Anforderungen:
  - Das Volume sollte mindestens doppelt so groß sein wie das Verzeichnis /opt/netapp/data des Unified Manager
  - Der Sicherheitsstil muss auf UNIX eingestellt sein
  - Die lokale Snapshot-Richtlinie muss deaktiviert sein
  - Die automatische Größenanpassung des Volume sollte aktiviert sein.
  - Das Performance Service Level sollte auf eine Richtlinie mit hohen IOPS und niedriger Latenz festgelegt werden, wie z. B. “Extreme”

Ausführliche Schritte zum Erstellen des NFS-Volumes finden Sie unter "Konfiguration von NFSv4 in ONTAP 9" und im "ONTAP 9 NFS Express-Leitfaden für die Konfiguration".

Der Zielspeicherort für Snapshot-Kopien in Active IQ Unified Manager ist anzugeben

Sie sollten den Zielspeicherort für Active IQ Unified Manager Snapshot Kopien auf einem Volume konfigurieren, das Sie bereits in einem Ihrer ONTAP Cluster eingerichtet haben. Sie sollten zum Definieren des Speicherorts die Managementplattform verwenden.

- Sie benötigen die Anmeldedaten des Root-Benutzers für den Linux-Host, auf dem Active IQ Unified Manager installiert ist.
- Sie müssen über eine Benutzerkennung und ein Passwort verfügen, die für die Anmeldung an der Managementplattform für die Wartung des Unified Manager Servers autorisiert sind.
- Sie benötigen die Cluster Management IP-Adresse, den Namen der Storage VM, den Namen des Volumes sowie den Benutzernamen und das Kennwort des Storage-Systems.
- Voraussetzung ist, dass Sie das Volume auf dem Active IQ Unified Manager Host eingebunden haben und den Mount-Pfad kennen.

Schritte

1. Secure Shell dient zum Herstellen einer Verbindung mit der IP-Adresse oder dem FQDN des Active IQ Unified Manager Systems.
2. Die Anmeldung am System erfolgt mit dem Benutzernamen und Passwort des Wartungsbenutzers (umadmin).
3. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.
4. Im **Main Menu** der Wartungskonsole erfolgt die Eingabe der Nummer für die Option **Backup Restore**.
5. Die Nummer für **Konfigurieren von NetApp Snapshot Backup** eingeben.

6. Sie geben die Nummer ein, um NFS zu konfigurieren.
7. Nachdem die erforderlichen Informationen geprüft wurden, kann die Nummer für **Details zur Backup-Konfiguration eingeben** eingegeben werden.
8. Zur Identifizierung des Volumes, auf dem der Snapshot gespeichert werden soll, werden die IP-Adresse der Cluster-Management-Schnittstelle, der Name der Storage VM, der Name des Volumes, der LUN-Name, der Storage-System-Benutzername und das Kennwort sowie der Mount-Pfad angegeben.
9. Diese Angaben überprüfen und `y` eingeben.

   Das System führt folgende Aufgaben aus:

   - Stellt die Verbindung zum Cluster her
   - Beendet alle Services
   - Erstellt ein neues Verzeichnis im Volume und kopiert die Konfigurationsdateien der Active IQ Unified Manager Datenbank
   - Dateien aus Active IQ Unified Manager löschen und einen symbolischen Link zum neuen Datenbankverzeichnis erstellen
   - Neustart aller Services
10. Sofern dies noch nicht erfolgt ist, können Sie nach dem Verlassen der Managementplattform und dem Starten der Active IQ Unified Manager Oberfläche einen Zeitplan für die Snapshot-Kopie erstellen.

Konfigurieren der Datensicherung unter Windows in Active IQ Unified Manager

Active IQ Unified Manager unterstützt Backup und Wiederherstellung mithilfe von NetApp Snapshots auf Windows-Betriebssystemen mithilfe von LUNs unter Verwendung des iSCSI-Protokolls.

Snapshot-basierte Backups können erstellt werden, während alle Unified Manager Services ausgeführt werden. Als Teil des Snapshot wird ein konsistenter Zustand der Datenbank erfasst, da das Backup eine globale Lesesperre für die gesamte Datenbank setzt, die gleichzeitige Schreibvorgänge verhindert. Damit Ihr auf Windows OS installiertes Unified Manager System Backups und Wiederherstellungen mithilfe von NetApp Snapshots durchführen kann, sollte die Unified Manager Backup-Konfiguration zunächst über die Managementplattform auf snapshotbasiert konfiguriert werden.

Bevor Sie Unified Manager für die Erstellung von Snapshot-Kopien konfigurieren, sollten Sie die folgenden Konfigurationsaufgaben durchführen.

- Konfiguration des ONTAP Clusters
- Konfiguration des Windows Hostrechners

Konfigurieren eines Sicherungsspeicherorts für Active IQ Unified Manager unter Windows

Nach dem Sichern von Unified Manager unter Windows sollte das Volume für die Speicherung von Snapshot Kopien konfiguriert werden.

Bevor Sie beginnen

Der Cluster, die Storage VM und das Volume müssen die folgenden Anforderungen erfüllen:

- Clusteranforderungen:
  - ONTAP 9.3 oder höher muss installiert sein

- Es sollte sich in geografischer Nähe zum Unified Manager Server befinden
- Es wird durch Unified Manager überwacht.

- Anforderungen an die Storage VM:
  - iSCSI-Konnektivität auf ONTAP Cluster
  - Das iSCSI-Protokoll muss für die konfigurierte Maschine aktiviert sein.
  - Für die Backup-Konfiguration sind ein dediziertes Volume und eine dedizierte LUN erforderlich. Das ausgewählte Volume sollte nur eine einzige LUN und sonst nichts enthalten.
  - Die Größe der LUN sollte mindestens doppelt so groß sein wie die Datenmenge, die voraussichtlich in Active IQ Unified Manager 9.9 verarbeitet wird.

    Dies setzt auch für das Volume dieselbe Größenanforderung voraus.

  - Stellen Sie sicher, dass „Alle Lese-/Schreibzugriffe“ ausgewählt ist
  - Der Superuser-Zugriff sollte in der Exportrichtlinie auf „`any`“ gesetzt sein.
- Volume- und LUN-Anforderungen:
  - Das Volume sollte mindestens doppelt so groß sein wie das Unified Manager MySQL-Datenverzeichnis.
  - Der Sicherheitsstil muss auf Windows eingestellt sein
  - Die lokale Snapshot-Richtlinie muss deaktiviert sein
  - Die automatische Größenanpassung des Volume sollte aktiviert sein.
  - Das Performance Service Level sollte auf eine Richtlinie mit hohen IOPS und niedriger Latenz festgelegt werden, wie z. B. “Extreme”

Konfigurieren eines ONTAP Clusters für Sicherung und Wiederherstellung in Active IQ Unified Manager

Bevor Sie Active IQ Unified Manager mithilfe einer Snapshot-Kopie auf Windows-Systemen sichern und wiederherstellen können, müssen Sie auf ONTAP Clustern einige Vorkonfigurationsschritte durchführen.

Sie können den ONTAP cluster entweder über die Befehlszeile oder die System Manager Benutzeroberfläche konfigurieren. Die Konfiguration des ONTAP cluster umfasst die Einrichtung von Data LIFs, sodass sie der Storage VM als iSCSI LIFs zugewiesen werden können. Der nächste Schritt ist die Konfiguration einer iSCSI-fähigen Storage VM über die System Manager Benutzeroberfläche. Für diese Storage VM muss eine statische Netzwerkroute konfiguriert werden, um zu steuern, wie LIFs das Netzwerk für ausgehenden Datenverkehr verwenden.



Es sollte ein dediziertes Volume und eine LUN für die Backup-Konfiguration vorhanden sein. Das ausgewählte Volume sollte nur eine LUN enthalten. Die Größe der LUN sollte mindestens doppelt so groß sein wie die Datenmenge, die von Active IQ Unified Manager voraussichtlich verarbeitet werden soll.

Sie müssen folgende Konfiguration vornehmen:

Schritte

1. Die Konfiguration erfolgt mit einer iSCSI-fähigen Storage VM oder mit einer vorhandenen Storage VM mit derselben Konfiguration.
2. Konfiguration einer Netzwerkroute für die konfigurierte Storage VM.

3. Für diese einzelne LUN ist ein Volume mit ausreichender Kapazität zu konfigurieren, das ausschließlich dieser LUN zugeordnet ist.

> Wenn die LUN in System Manager erstellt wird, kann beim Aufheben der Zuordnung der LUN die Initiatorgruppe gelöscht werden, und die Wiederherstellung kann fehlschlagen. Zur Vermeidung dieses Szenarios ist darauf zu achten, dass eine LUN bei der Erstellung explizit erstellt wird und beim Aufheben der Zuordnung nicht gelöscht wird.

4. Konfiguration einer Initiatorgruppe in der Storage VM.
5. Einen Portsatz konfigurieren.
6. Integration der Initiatorgruppe in das Portset.
7. Zuordnung der LUN zur Initiatorgruppe.

Konfiguration eines Windows-Hostcomputers in Active IQ Unified Manager

Sie müssen Ihren Windows-Hostrechner konfigurieren, bevor Sie NetApp Snapshot zum Sichern und Wiederherstellen von Active IQ Unified Manager verwenden können. Zum Starten des Microsoft iSCSI-Initiators auf einem Windows-Hostrechner geben Sie „`iscsi`“ in die Suchleiste ein und klicken auf **iSCSI Initiator**.

Bevor Sie beginnen

Es empfiehlt sich, alle vorherigen Konfigurationen auf dem Host-Rechner zu löschen.

Wenn versucht wird, den iSCSI-Initiator auf einer Neuinstallation von Windows zu starten, wird eine Bestätigung angefordert, und nach der Bestätigung wird das Dialogfeld „iSCSI-Eigenschaften“ angezeigt. Bei einer bestehenden Windows-Installation wird das Dialogfeld „iSCSI-Eigenschaften“ mit einem Ziel angezeigt, das entweder inaktiv ist oder versucht, eine Verbindung herzustellen. Daher muss sichergestellt werden, dass alle vorherigen Konfigurationen auf dem Windows-Host entfernt werden.

Schritte

1. Auf dem Host-Rechner müssen alle vorherigen Konfigurationen entfernt werden.
2. Ermittlung des Zielportals.
3. Verbindung zum Zielportal herstellen.
4. Die Verbindung zum Zielportal erfolgt über Multipath.
5. Die Ermittlung beider LIFs ist möglich.
6. Die im Windows-Rechner als Gerät konfigurierte LUN wird ermittelt.
7. In Windows lässt sich die erkannte LUN als neues Volume-Laufwerk konfigurieren.

Geben Sie den Zielspeicherort für Snapshot Kopien unter Windows in Active IQ Unified Manager an

Sie sollten den Zielspeicherort für Active IQ Unified Manager Snapshot Kopien auf einem Volume konfigurieren, das Sie bereits in einem Ihrer ONTAP Cluster eingerichtet haben. Sie sollten zum Definieren des Speicherorts die Managementplattform verwenden.

- Sie benötigen Administratorrechte für den Windows-Host, auf dem Active IQ Unified Manager installiert ist.
- Sie müssen über eine Benutzerkennung und ein Passwort verfügen, die für die Anmeldung an der Managementplattform für die Wartung des Unified Manager Servers autorisiert sind.
- Sie benötigen die Cluster-Management-IP-Adresse, den Namen der Storage-VM, den Namen des

Volumes, den LUN-Namen sowie den Storage-System-Benutzernamen und das Kennwort.

- Sie müssen das Volume als Netzlaufwerk auf dem Active IQ Unified Manager Host gemountet haben, und das gemountete Laufwerk muss verfügbar sein.

Schritte

1. Die Verbindung mit der IP-Adresse oder dem vollqualifizierten Domain-Namen des Active IQ Unified Manager Systems erfolgt mithilfe von Power Shell.
2. Die Anmeldung am System erfolgt mit dem Benutzernamen und Passwort des Wartungsbenutzers (umadmin).
3. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.
4. Im **Main Menu** der Wartungskonsole erfolgt die Eingabe der Nummer für die Option **Backup Restore**.
5. Die Nummer für **Konfigurieren von NetApp Snapshot Backup** eingeben.
6. Die Nummer für die Konfiguration von iSCSI eingeben.
7. Nachdem die erforderlichen Informationen geprüft wurden, kann die Nummer für **Details zur Backup-Konfiguration eingeben** eingegeben werden.
8. Zur Identifizierung des Volumes, in das der Snapshot geschrieben wird, sind die IP-Adresse der Cluster Management-Schnittstelle, der Name der Storage VM, der Name des Volumes, der LUN-Name, der Benutzername und das Kennwort des Storage-Systems sowie das Mount-Laufwerk anzugeben.
9. Diese Angaben überprüfen und `y` eingeben.

   Das System führt folgende Aufgaben aus:

   - Storage VM wurde validiert
   - Volume ist validiert
   - Das Laufwerk wird eingebunden und der Status validiert.
   - Vorhandensein und Status der LUN
   - Vorhandensein eines Netzwerklaufwerks
   - Es wird geprüft, ob auf dem gemounteten Volume der empfohlene Speicherplatz vorhanden ist (mehr als das Doppelte des mysql-Datenverzeichnisses).
   - LUN-Pfad, der der dedizierten LUN im Volume entspricht
   - Name der Initiatorgruppe
   - GUID des Volumes, auf dem das Netzlaufwerk eingebunden ist
   - iSCSI-Initiator zur Kommunikation mit ONTAP
10. Nach dem Verlassen der Managementplattform lässt sich in der Benutzeroberfläche von Active IQ Unified Manager ein Zeitplan für Snapshot-Kopien erstellen.

Konfiguration einer Snapshot-Sicherung über die Wartungskonsole in Active IQ Unified Manager

Für die Erstellung eines Backups von Active IQ Unified Manager mithilfe einer Snapshot-Kopie sind einige Konfigurationsschritte in der Managementplattform erforderlich.

Bevor Sie beginnen

Für Ihr System benötigen Sie folgende Details:

- Cluster IP-Adresse
- Name der Storage VM
- Volumenname
- LUN-Name
- Mount-Pfad
- Anmeldeinformationen für das Storage-System

Schritte

1. Sie können auf die Managementplattform von Unified Manager zugreifen.
2. Die Auswahl von **Backup Restore** erfolgt durch Eingabe von 4.
3. Die Auswahl von **Backup und Wiederherstellung mit NetApp Snapshot** erfolgt durch Eingabe von 2.

   Wenn Sie die Backup-Konfiguration ändern möchten, können Sie durch Eingabe von 3 **Update NetApp Snapshot Backup Configuration** auswählen. Sie können nur das Passwort aktualisieren.

4. Im Menü dient die Eingabe von 1 zur Auswahl von **NetApp Snapshot Backup konfigurieren**.
5. Für die Angabe der erforderlichen Informationen 1 eingeben.
6. Erforderlich sind der Benutzername und das Passwort für die Managementplattform sowie anschließend die Bestätigung, dass die LUN auf dem Host eingebunden ist.

   Der Prozess überprüft anschließend, ob das von Ihnen angegebene Datenverzeichnis, der LUN-Pfad, die Storage VM, die Volumes, die verfügbare Speicherkapazität, das Laufwerk usw. korrekt sind. Folgende Vorgänge laufen im Hintergrund ab:

   - Services sind gestoppt
   - Das Datenbankverzeichnis wird auf eingebundenen Storage verschoben
   - Das Datenbankverzeichnis wird gelöscht und symbolische Verknüpfungen werden erstellt
   - Nach Abschluss der Konfiguration in der Active IQ Unified Manager Benutzeroberfläche werden die Dienste neu gestartet. Der Backup-Typ wird in NetApp Snapshot geändert und in der Benutzeroberfläche als Datenbank-Backup (Snapshot-basiert) angezeigt.

Vor Beginn eines Backup-Vorgangs sollte geprüft werden, ob es Änderungen an der Snapshot-Konfiguration gibt, da diese dazu führen könnten, dass der Snapshot ungültig wird. Angenommen, die Backup-Konfiguration wurde für Laufwerk G eingerichtet und ein Snapshot wurde erstellt. Später wurde die Backup-Konfiguration für Laufwerk E geändert, und die Daten werden gemäß der neuen Konfiguration auf Laufwerk E gespeichert. Wenn dann versucht wird, den Snapshot wiederherzustellen, der erstellt wurde, als Laufwerk G verwendet wurde, schlägt dies mit der Fehlermeldung fehl, dass Laufwerk G nicht vorhanden ist.

In Active IQ Unified Manager lässt sich ein Sicherungszeitplan für Linux und Windows festlegen

Über die Unified Manager Benutzeroberfläche können Sie den Zeitplan konfigurieren, nach dem Unified Manager Snapshot Kopien erstellt werden.

Bevor Sie beginnen

- Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
- Die Einstellungen für die Erstellung von Snapshot-Kopien über die Managementplattform müssen

konfiguriert worden sein, damit das Ziel identifiziert werden kann, an dem die Snapshots erstellt werden.

Snapshot Kopien werden in nur wenigen Minuten erstellt, und die Unified Manager Datenbank wird nur für wenige Sekunden gesperrt.

> Ein Backup, das in den ersten 15 Tagen nach dem Hinzufügen eines neuen Clusters erstellt wurde, ist möglicherweise nicht genau genug, um die historischen Performance-Daten zu erhalten.

Schritte

1. Im linken Navigationsbereich können Sie **General** > **Database Backup** auswählen.
2. Auf der Seite **Datenbanksicherung** können die **Sicherungseinstellungen** ausgewählt werden.
3. Im Feld **Aufbewahrungsanzahl** wird die maximale Anzahl der Snapshot Kopien festgelegt, die beibehalten werden soll.

   Der Standardwert für die Aufbewahrungsanzahl ist 10. Die maximale Anzahl an Snapshot Kopien hängt von der ONTAP Softwareversion im Cluster ab. Sie können dieses Feld leer lassen, um unabhängig von der ONTAP Version den Maximalwert zu implementieren.

4. Sie wählen die Schaltfläche **Scheduled Daily** oder **Scheduled Weekly** aus und geben anschließend die Details des Zeitplans an.
5. Auf **Anwenden** klicken.

Snapshot-Kopien werden gemäß dem Zeitplan erstellt. Die verfügbaren Backup-Dateien sind auf der Seite „Datenbank-Backup“ zu sehen.

Aufgrund der Wichtigkeit dieses Volumes und der Snapshots empfiehlt es sich, eine oder zwei Warnmeldungen für dieses Volume zu erstellen, damit Sie benachrichtigt werden, wenn eines der folgenden Ereignisse eintritt:

- Der Speicherplatz des Volumes ist zu 90 % belegt. Für das Einrichten der Benachrichtigung dient das Ereignis **Volume Space Full**.

  Sie können die Kapazität des Volumes mithilfe von ONTAP System Manager oder der ONTAP CLI erhöhen, damit der Unified Manager Datenbank nicht der Speicherplatz ausgeht.

- Die Anzahl der Snapshots nähert sich der maximalen Anzahl. Die Warnung lässt sich mit dem Ereignis **Too Many Snapshot Copies** einrichten.

  Sie können ältere Snapshots mit ONTAP System Manager oder der ONTAP CLI löschen, sodass immer Platz für neue Snapshot Kopien vorhanden ist.

Sie konfigurieren Warnmeldungen auf der Seite „Alert Setup“.

Active IQ Unified Manager mithilfe von Snapshot Kopien wiederherstellen

Bei Datenverlust oder Datenbeschädigung können Sie Unified Manager mit minimalem Datenverlust in den vorherigen stabilen Zustand zurückversetzen. Sie können die Unified Manager Snapshot-Datenbank über die Unified Manager Managementplattform auf einem lokalen oder entfernten Betriebssystem wiederherstellen.

Bevor Sie beginnen

- Sie benötigen die Anmeldedaten des Root-Benutzers für den Linux-Host und Administratorrechte für den Windows-Hostrechner, auf dem Unified Manager installiert ist.
- Sie müssen über eine Benutzerkennung und ein Passwort verfügen, die für die Anmeldung an der Managementplattform für die Wartung des Unified Manager Servers autorisiert sind.

Die Wiederherstellungsfunktion ist plattform- und versionsspezifisch. Eine Unified Manager Sicherung kann nur auf derselben Version von Unified Manager wiederhergestellt werden.

Schritte

1. Die Verbindung erfolgt über die IP-Adresse oder die vollqualifizierte Domain des Unified Manager Systems.
   - Linux: Secure Shell
   - Windows: PowerShell
2. Zur Anmeldung am System dienen die Anmeldedaten des Root-Benutzers.
3. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.
4. Im **Hauptmenü** der Wartungs-Managementplattform wird für die Option **Sicherung wiederherstellen** die Nummer 4 eingegeben.
5. Die Auswahl von **Sichern und Wiederherstellen mit NetApp Snapshot** erfolgt mit 2.

   Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, sollte nach Abschluss der Installation von Unified Manager die Benutzeroberfläche nicht gestartet und es sollten keine Cluster, Benutzer oder Authentifizierungseinstellungen konfiguriert werden. Für die Auswahl von **Configure NetApp Snapshot Backup** ist 1 einzugeben, und die Einstellungen für Snapshot Kopien sind wie auf dem ursprünglichen System zu konfigurieren.

6. 3 dient zur Auswahl von **Wiederherstellung mithilfe von NetApp Snapshot**.
7. Die Snapshot-Kopie, aus der Unified Manager wiederhergestellt werden soll, wird ausgewählt. Anschließend wird **Enter** gedrückt.
8. Nach Abschluss des Wiederherstellungsprozesses können Sie sich an der Unified Manager Benutzeroberfläche anmelden.

Falls der Workflow Automation Server nach dem Wiederherstellen der Sicherung nicht funktioniert, sind folgende Schritte erforderlich:

1. Auf dem Workflow Automation Server muss die IP-Adresse des Unified Manager Servers auf den neuesten Rechner umgestellt werden.
2. Wenn die Datenerfassung in Schritt 1 fehlschlägt, muss auf dem Unified Manager Server das Datenbankpasswort zurückgesetzt werden.

Der Sicherungstyp in Active IQ Unified Manager kann geändert werden

Wenn Sie den Sicherungstyp für Ihr Active IQ Unified Manager System ändern möchten, können Sie dazu die Optionen der Wartungskonsole verwenden. Mit der Option **Unconfigure NetApp Snapshot Backup** können Sie zur MySQL-basierten Sicherung zurückkehren.

Bevor Sie beginnen

Sie müssen über eine Benutzerkennung und ein Passwort verfügen, die für die Anmeldung an der Managementplattform für die Wartung des Unified Manager Servers autorisiert sind.

Schritte

1. Auf die Wartungskonsole zugreifen.
2. Im **Hauptmenü** steht die Option 4 für Sicherung und Wiederherstellung zur Verfügung.
3. Im **Backup and Restore Menu** erfolgt die Auswahl von Option 2.
4. 4 für **Unconfigure NetApp Snapshot Backup** auswählen.

   Angezeigt werden die durchgeführten Aktionen: die Services anhalten, den symbolischen Link aufheben, die Daten vom Storage in ein Verzeichnis verschieben und anschließend die Services wieder starten.

   Nach der Änderung der Sicherungsmethode ändert sich der Sicherungsmechanismus von Snapshot Kopie zur standardmäßigen MySQL-Sicherung. Diese Änderung wird im Abschnitt „Datenbanksicherung“ der allgemeinen Einstellungen angezeigt.

Grundlegendes zum On-Demand-Backup für Active IQ Unified Manager

Mit der Benutzeroberfläche von Active IQ Unified Manager können Sie bei Bedarf ein On-Demand-Backup erstellen. Mit dem On-Demand-Backup können Sie mithilfe der vorhandenen Backup-Methode sofort ein Backup erstellen. Das On-Demand-Backup unterscheidet nicht zwischen MySQL- oder NetApp Snapshot-basierten Backups.

Sie können eine bedarfsgesteuerte Datensicherung über die Schaltfläche **Backup Now** auf der Seite „Database Backup“ durchführen. Die bedarfsgesteuerte Datensicherung ist unabhängig von den Zeitplänen, die Sie für Active IQ Unified Manager konfiguriert haben.

Migration einer Active IQ Unified Manager virtuellen Appliance auf ein Linux System

Sie können ein Dump-Backup der Unified Manager MySQL-Datenbank von einer virtuellen Appliance auf ein Red Hat Enterprise Linux-System wiederherstellen, wenn Sie das Host-Betriebssystem ändern möchten, auf dem Unified Manager ausgeführt wird.

Bevor Sie beginnen

- Auf der virtuellen Appliance:
  - Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.
  - Für den Wiederherstellungsvorgang müssen Sie den Namen des Unified Manager Wartungsbenutzers kennen.
- Auf dem Linux-System:
  - Unified Manager muss auf einem Linux-Server gemäß den Anweisungen in "Installation von Unified Manager auf Linux-Systemen" installiert worden sein.
  - Die Version von Unified Manager auf diesem Server muss mit der Version auf der virtuellen Appliance identisch sein, von der aus Sie die Sicherungsdatei verwenden.
  - Nach der Installation sollten Sie auf dem Linux-System weder die UI starten noch Cluster, Benutzer oder Authentifizierungseinstellungen konfigurieren. Die Sicherungsdatei stellt diese Informationen während des Wiederherstellungsprozesses bereit.
  - Sie benötigen die Anmeldedaten des Root-Benutzers für den Linux-Host.

Diese Schritte beschreiben, wie eine Sicherungsdatei auf der virtuellen Appliance erstellt, die Sicherungsdateien nach Red Hat Enterprise Linux kopiert und anschließend die Datenbanksicherung auf dem neuen System wiederhergestellt wird.

Schritte

1. Auf der virtuellen Appliance erfolgt die Auswahl von **Management** > **Database Backup**.
2. Auf der Seite **Datenbanksicherung** können die **Sicherungseinstellungen** ausgewählt werden.
3. Der Backup-Pfad muss auf /jail/support geändert werden.
4. Im Abschnitt „Zeitplan“ wird **Täglich geplant** ausgewählt, und es wird eine Uhrzeit eingegeben, die einige Minuten nach der aktuellen Uhrzeit liegt, damit die Sicherung in Kürze erstellt wird.
5. Auf **Anwenden** klicken.
6. Es dauert einige Stunden, bis die Datensicherung erstellt ist.

   Eine vollständige Datensicherung kann über 1 GB groß sein und drei bis vier Stunden dauern.

7. Anmeldung als Root-Benutzer am Linux-Host, auf dem Unified Manager installiert ist, und Kopieren der Sicherungsdateien aus /support auf die virtuelle Appliance mithilfe von SCP.`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

   ```
   root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
   ```

   Voraussetzung ist, dass Sie die .7z-Sicherungsdatei und alle .7z-Repository-Dateien in das Unterverzeichnis /database-dumps-repo kopiert haben.

8. An der Eingabeaufforderung erfolgt die Wiederherstellung des Backups: `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. Nach Abschluss des Wiederherstellungsvorgangs erfolgt die Anmeldung bei der Web-UI von Unified Manager.

Sie sollten die folgenden Aufgaben ausführen:

- Die Generierung eines neuen HTTPS-Sicherheitszertifikats und der Neustart des Unified Manager Server sind erforderlich.
- Der Sicherungspfad wird auf die Standardeinstellung Ihres Linux-Systems (/data/ocum-backup) oder auf einen neuen Pfad Ihrer Wahl geändert, da auf dem Linux-System kein Pfad /jail/support vorhanden ist.
- Wenn WFA verwendet wird, ist eine Neukonfiguration beider Seiten Ihrer Workflow Automation Verbindung erforderlich.
- Bei Verwendung von SAML ist eine Neukonfiguration der Einstellungen für die SAML-Authentifizierung erforderlich.

Nachdem Sie sich vergewissert haben, dass auf Ihrem Linux-System alles wie erwartet funktioniert, können Sie die virtuelle Appliance Unified Manager herunterfahren und entfernen.

Skripte managen

Skripte in Active IQ Unified Manager verwalten

Sie können Skripte verwenden, um mehrere Storage Objekte in Unified Manager automatisch zu ändern oder zu aktualisieren. Das Skript ist mit einer Warnung verknüpft. Wenn ein Ereignis eine Warnung auslöst, führt Unified Manager das Skript aus. Sie

können benutzerdefinierte Skripte hochladen und ihre Ausführung beim Erstellen einer Warnung testen.

Das Hochladen und Ausführen von Skripten in Unified Manager ist standardmäßig aktiviert. Falls Ihr Unternehmen diese Funktion aus Sicherheitsgründen nicht zulassen möchte, können Sie sie unter **Speicherverwaltung** > **Funktionseinstellungen** deaktivieren.

Informationen zur Funktionsweise von Skripten mit Warnmeldungen in Active IQ Unified Manager

Sie können Ihrem Skript eine Warnung zuordnen, sodass das Skript ausgeführt wird, wenn in Unified Manager für ein Ereignis eine Warnung ausgelöst wird. Mithilfe der Skripte lassen sich Probleme mit Storage Objekten beheben oder die Storage Objekte identifizieren, die die Ereignisse generieren.

Wenn in Unified Manager eine Warnung für ein Ereignis generiert wird, wird eine Benachrichtigungs-E-Mail an die angegebenen Empfänger gesendet. Wenn Sie einer Warnung ein Skript zugeordnet haben, wird das Skript ausgeführt. Die Details der an das Skript übergebenen Argumente sind in der Benachrichtigungs-E-Mail enthalten.

> Wenn Sie ein benutzerdefiniertes Skript erstellt und es einer Warnung für einen bestimmten Ereignistyp zugeordnet haben, richten sich die Maßnahmen für diesen Ereignistyp nach Ihrem benutzerdefinierten Skript, und die **Fix it**-Aktionen sind standardmäßig auf der Seite „Management Actions“ oder im Unified Manager Dashboard nicht verfügbar.

Das Skript verwendet für die Ausführung die folgenden Argumente:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Sie können die Argumente in Ihren Skripten verwenden sowie zugehörige Ereignisinformationen erfassen oder Storage Objekte ändern.

Beispiel für das Abrufen von Argumenten aus Skripten

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

Wenn eine Warnmeldung generiert wird, führt das System dieses Skript aus, und die folgende Ausgabe wird angezeigt:

```
-eventID : 290
-eventSourceID : 4138
```

Skripte in Active IQ Unified Manager hinzufügen

Sie können in Unified Manager Skripte hinzufügen und diese mit Warnmeldungen verknüpfen. Diese Skripte werden automatisch ausgeführt, wenn eine Warnmeldung generiert wird, und ermöglichen es Ihnen, Informationen zu den Storage Objekten abzurufen, für die das Ereignis generiert wird.

Bevor Sie beginnen

- Sie müssen die Skripte, die Sie dem Unified Manager Server hinzufügen möchten, erstellt und gespeichert haben.
- Die unterstützten Dateiformate für Skripte sind Perl, Shell, PowerShell, Python und `.bat`Dateien.

Plattform, auf der Unified Manager installiert ist	Unterstützte Sprachen
VMware	Perl- und Shell-Skripte
Linux	Perl, Python und Shell Skripte
Windows	PowerShell, Perl-, Python- und .bat-Skripte

  - Für Perl Skripte muss Perl auf dem Unified Manager Server installiert sein. Bei VMware Installationen ist Perl 5 standardmäßig installiert, und die Skripte unterstützen nur die von Perl 5 unterstützten Funktionen. Wenn Perl nach Unified Manager installiert wurde, muss der Unified Manager Server neu gestartet werden.
  - Für PowerShell-Skripte muss auf dem Windows-Server die entsprechende PowerShell-Ausführungsrichtlinie festgelegt werden, damit die Skripte ausgeführt werden können.

> Wenn Ihr Skript Protokolldateien erstellt, um den Fortschritt des Alarmskripts zu verfolgen, müssen Sie sicherstellen, dass sich die Protokolldateien nicht irgendwo im Unified Manager Installationsordner befinden.

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können benutzerdefinierte Skripte hochladen und Ereignisdetails zur Warnung erfassen.

> Wenn diese Funktion in der Benutzeroberfläche nicht verfügbar ist, wurde die Funktionalität von Ihrem Administrator deaktiviert. Bei Bedarf kann diese Funktionalität unter **Storage Management** > **Feature Settings** aktiviert werden.

Schritte

1. Im linken Navigationsbereich wird **Storage Management** > **Scripts** ausgewählt.
2. Auf der Seite **Skripte** erfolgt die Auswahl von **Hinzufügen**.
3. Im Dialogfeld **Skript hinzufügen** wird mit **Durchsuchen** die Skriptdatei ausgewählt.
4. Geben Sie für das ausgewählte Skript eine Beschreibung ein.
5. Klicken Sie auf **Add**.

Skripte in Active IQ Unified Manager löschen

Sie können ein Skript aus dem Unified Manager löschen, wenn das Skript nicht mehr benötigt wird oder ungültig ist.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Das Skript darf nicht mit einer Warnmeldung verknüpft sein.

Schritte

1. Im linken Navigationsbereich wird **Storage Management** > **Scripts** ausgewählt.
2. Auf der Seite **Skripte** wählen Sie das Skript aus, das Sie löschen möchten, und klicken dann auf **Löschen**.
3. Die Bestätigung der Löschung erfolgt im Dialogfeld **Warning** durch Klicken auf **Yes**.

Ausführung des Testskripts in Active IQ Unified Manager

Sie können überprüfen, ob Ihr Skript korrekt ausgeführt wird, wenn eine Warnung für ein Storage-Objekt generiert wird.

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen ein Skript im unterstützten Dateiformat in Unified Manager hochgeladen haben.

Schritte

1. Im linken Navigationsbereich wird **Storage Management** > **Scripts** ausgewählt.
2. Auf der Seite „Skripte“ erfolgt das Hinzufügen Ihres Testskripts.
3. Im linken Navigationsbereich auf **Storage Management** > **Alert Setup** klicken.
4. Auf der Seite **Alert Setup** können Sie eine der folgenden Aktionen auswählen:

Zu…	Folgendes ist zu tun…
Hinzufügen einer Benachrichtigung	a. Klicken Sie auf **Add**. b. Im Abschnitt „Aktionen“ können Sie die Warnung Ihrem Testskript zuordnen.
Eine Warnmeldung bearbeiten	a. Eine Benachrichtigung auswählen und dann auf **Bearbeiten** klicken. b. Im Abschnitt „Aktionen“ können Sie die Warnung Ihrem Testskript zuordnen.

5. Auf **Speichern** klicken.
6. Auf der Seite **Alert Setup** den hinzugefügten oder geänderten Alarm auswählen und anschließend auf **Test** klicken.

   Das Skript wird mit dem Argument “-test” ausgeführt, und ein Benachrichtigungsalarm wird an die E-Mail-Adressen gesendet, die beim Erstellen des Alarms angegeben wurden.

Gruppen verwalten und überwachen

Gruppen verstehen

Informationen zu Gruppen in Active IQ Unified Manager

Eine Gruppe ist eine dynamische Sammlung heterogener Storage Objekte (Cluster, SVMs oder Volumes). Sie können in Unified Manager Gruppen erstellen, um eine Reihe von Storage Objekten einfach zu managen. Die Mitglieder einer Gruppe können sich ändern, je nachdem, welche Storage Objekte Unified Manager zu einem bestimmten Zeitpunkt überwacht.

- Jede Gruppe hat einen eindeutigen Namen.
- Sie müssen für jede Gruppe mindestens eine Gruppenregel konfigurieren.
- Sie können eine Gruppe mit mehr als einer Gruppenregel verknüpfen.
- Jede Gruppe kann mehrere Arten von Storage-Objekten wie z. B. Cluster, SVMs oder Volumes enthalten.
- Storage-Objekte werden einer Gruppe dynamisch hinzugefügt, je nachdem, wann eine Gruppenregel erstellt wird oder wann Unified Manager einen Überwachungszyklus abschließt.
- Sie können gleichzeitig Aktionen auf alle Storage Objekte in einer Gruppe anwenden, beispielsweise das Festlegen von Schwellenwerten für Volumes.

Grundlegendes zur Funktionsweise von Gruppenregeln für Gruppen in Active IQ Unified Manager

Eine Gruppenregel ist ein Kriterium, das Sie definieren, damit Storage-Objekte (Volumes, Cluster oder SVMs) in eine bestimmte Gruppe aufgenommen werden können. Zum Definieren einer Gruppenregel für eine Gruppe können Sie Bedingungsgruppen oder Bedingungen verwenden.

- Für eine Gruppe ist die Zuordnung einer Gruppenregel erforderlich.
- Einer Gruppenregel muss ein Objekttyp zugeordnet werden; pro Gruppenregel ist nur ein Objekttyp möglich.
- Nach jedem Überwachungszyklus sowie beim Erstellen, Bearbeiten oder Löschen einer Regel werden Storage-Objekte der Gruppe hinzugefügt oder aus ihr entfernt.
- Eine Gruppenregel kann eine oder mehrere Bedingungsgruppen haben, und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben.
- Speicherobjekte können basierend auf von Ihnen erstellten Gruppenregeln mehreren Gruppen angehören.

Bedingungen

Sie können mehrere Bedingungsgruppen erstellen, und jede Bedingungsgruppe kann eine oder mehrere Bedingungen enthalten. Sie können alle definierten Bedingungsgruppen in einer Gruppenregel anwenden, um festzulegen, welche Storage-Objekte in die Gruppe aufgenommen werden.

Bedingungen innerhalb einer Bedingungsgruppe werden mit einem logischen UND ausgeführt. Alle Bedingungen in einer Bedingungsgruppe müssen erfüllt sein. Wenn Sie eine Gruppenregel erstellen oder ändern, wird eine Bedingung erstellt, die nur die Storage-Objekte anwendet, auswählt und gruppiert, die alle Bedingungen in der Bedingungsgruppe erfüllen. Sie können mehrere Bedingungen innerhalb einer Bedingungsgruppe verwenden, wenn Sie den Umfang der Storage-Objekte eingrenzen möchten, die in eine Gruppe aufgenommen werden.

Sie können Bedingungen mit Storage-Objekten erstellen, indem Sie die folgenden Operanden und Operatoren

verwenden und den erforderlichen Wert angeben.

Storage-Objekttyp	Anwendbare Operanden
Volumen	• Objektname • Name des besitzenden Clusters • Name der zugehörigen SVM • Anmerkungen
SVM	• Objektname • Name des besitzenden Clusters • Anmerkungen
Cluster	• Objektname • Anmerkungen

Wenn Sie Annotation als Operand für ein Storage-Objekt auswählen, ist der Operator „`Is`“ verfügbar. Für alle anderen Operanden können Sie entweder „`Is`“ oder „`Contains`“ als Operator auswählen.

- Operand

  Die Liste der Operanden im Unified Manager ändert sich je nach ausgewähltem Objekttyp. Die Liste umfasst den Objektnamen, den Namen des zugehörigen Clusters, den Namen der zugehörigen SVM und die im Unified Manager definierten Annotationen.

- Operator

  Die Liste der Operatoren ändert sich abhängig vom für eine Bedingung ausgewählten Operanden. Die in Unified Manager unterstützten Operatoren sind „`Is`“ und „`Contains`“.

  Wenn Sie den Operator “Is” auswählen, prüft das System die Bedingung auf eine exakte Übereinstimmung des Operandenwerts mit dem für den ausgewählten Operanden angegebenen Wert.

  Wenn Sie den Operator „`Contains`“ auswählen, wird die Bedingung daraufhin geprüft, ob eines der folgenden Kriterien erfüllt ist:

  - Der Operandenwert stimmt exakt mit dem für den ausgewählten Operanden angegebenen Wert überein
  - Der Operandenwert enthält den für den ausgewählten Operanden angegebenen Wert

- Wert

  Das Wertfeld ändert sich je nach ausgewähltem Operanden.

Beispiel einer Gruppenregel mit Bedingungen

Eine Bedingungsgruppe für ein Volume mit den folgenden zwei Bedingungen:

- Der Name enthält “vol”
- Der SVM-Name lautet “data_svm”

Diese Bedingungsgruppe wählt alle Volumes aus, die “vol” in ihrem Namen enthalten und auf SVMs mit dem Namen “data_svm” gehostet sind.

Bedingungsgruppen

Bedingungsgruppen werden mit logischem ODER verknüpft und anschließend auf Storage-Objekte angewendet. Storage-Objekte müssen mindestens eine der Bedingungsgruppen erfüllen, um in eine Gruppe aufgenommen zu werden. Die Storage-Objekte aller Bedingungsgruppen werden kombiniert. Sie können Bedingungsgruppen verwenden, um den Umfang der Storage-Objekte zu erweitern, die in eine Gruppe aufgenommen werden.

Beispiel einer Gruppenregel mit Bedingungsgruppen

Für ein Volumen werden zwei Bedingungsgruppen berücksichtigt, wobei jede Gruppe die folgenden zwei Bedingungen enthält:

- Bedingungsgruppe 1
  - Der Name enthält “vol”
  - Der SVM-Name ist “data_svm” Bedingungsgruppe 1 wählt alle Volumes aus, die “vol” in ihrem Namen enthalten und auf SVMs mit dem Namen “data_svm” gehostet sind.
- Bedingungsgruppe 2
  - Der Name enthält “vol”
  - Der Annotationswert von data-priority ist “critical” Bedingungsgruppe 2 wählt alle Volumes aus, die “vol” in ihrem Namen enthalten und mit dem Annotationswert data-priority als “critical” annotiert sind.

Wenn eine Gruppenregel, die diese beiden Bedingungsgruppen enthält, auf Storage Objekte angewendet wird, werden die folgenden Storage Objekte einer ausgewählten Gruppe hinzugefügt:

- Alle Volumes, die “vol” in ihrem Namen enthalten und auf der SVM mit dem Namen “data_svm” gehostet sind.
- Alle Volumes, deren Namen “vol” enthalten und die mit dem Anmerkungswert für die Datenpriorität “critical” gekennzeichnet sind.

Informationen zur Funktionsweise von Gruppenaktionen auf Speicherobjekten in Active IQ Unified Manager

Eine Gruppenaktion ist ein Vorgang, der auf alle Storage-Objekte in einer Gruppe angewendet wird. Beispielsweise lässt sich die Gruppenaktion „Volume-Schwellenwert“ so konfigurieren, dass die Schwellenwerte aller Volumes in einer Gruppe gleichzeitig geändert werden.

Gruppen unterstützen eindeutige Gruppenaktionstypen. Eine Gruppe kann nur über einen Gruppenaktionstyp für den Systemstatusschwellenwert von Volumes verfügen. Für dieselbe Gruppe kann jedoch, sofern verfügbar, ein anderer Gruppenaktionstyp konfiguriert werden. Der Rang einer Gruppenaktion bestimmt die Reihenfolge, in der die Aktion auf Storage-Objekte angewendet wird. Die Detailseite eines Storage-Objekts enthält Informationen darüber, welche Gruppenaktion auf das Storage-Objekt angewendet wird.

Beispiel für eindeutige Gruppenaktionen

Angenommen, ein Volume A gehört zu den Gruppen G1 und G2, und für diese Gruppen sind die folgenden Aktionen der Systemstatus-Schwellenwertgruppe für Volumes konfiguriert:

- `Change_capacity_threshold` Gruppenaktion mit Rang 1 zur Konfiguration der Kapazität des Volume
- `Change_snapshot_copies` Gruppenaktion mit Rang 2 zur Konfiguration der Snapshot-Kopien des Volumes

Die `Change_capacity_threshold`Gruppenaktion hat stets Vorrang vor der `Change_snapshot_copies`anderen Gruppenaktion und wird auf Volume A angewendet. Wenn Unified Manager einen Überwachungszyklus abschließt, werden die mit den Systemstatus-Schwellenwerten zusammenhängenden Ereignisse von Volume A gemäß der `Change_capacity_threshold`Gruppenaktion neu ausgewertet. Für die Gruppen G1 und G2 kann keine weitere Gruppenaktion vom Typ „Volume-Schwellenwert“ konfiguriert werden.

Hinzufügen von Gruppen in Active IQ Unified Manager

Sie können Gruppen erstellen, um Cluster, Volumes und Storage Virtual Machines (SVMs) zur einfacheren Verwaltung zu kombinieren.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können Gruppenregeln definieren, um Mitglieder zur Gruppe hinzuzufügen oder aus ihr zu entfernen sowie Gruppenaktionen für die Gruppe zu ändern.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Im Tab **Gruppen** wählen Sie **Hinzufügen** aus.
3. Im Dialogfeld **Gruppe hinzufügen** werden ein Name und eine Beschreibung für die Gruppe eingegeben.
4. Klicken Sie auf **Add**.

Gruppen in Active IQ Unified Manager bearbeiten

Sie können den Namen und die Beschreibung einer Gruppe bearbeiten, die Sie im Unified Manager erstellt haben.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Wenn Sie eine Gruppe bearbeiten, um den Namen zu aktualisieren, müssen Sie einen eindeutigen Namen angeben; Sie können keinen bereits vorhandenen Gruppennamen verwenden.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Im Reiter **Gruppen** können Sie die Gruppe auswählen, die Sie bearbeiten möchten, und anschließend auf **Bearbeiten** klicken.
3. Im Dialogfeld **Gruppe bearbeiten** können Sie den Namen, die Beschreibung oder beides für die Gruppe ändern.
4. Auf **Speichern** klicken.

Gruppen in Active IQ Unified Manager löschen

Sie können eine Gruppe aus Unified Manager löschen, wenn die Gruppe nicht mehr erforderlich ist.

Bevor Sie beginnen

- Keines der Storage-Objekte (Cluster, SVMs oder Volumes) darf einer Gruppenregel zugeordnet sein, die

mit der Gruppe verknüpft ist, die Sie löschen möchten.

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Im Reiter **Gruppen** erfolgt die Auswahl der Gruppe, die gelöscht werden soll; anschließend erfolgt ein Klick auf **Löschen**.
3. Die Bestätigung der Löschung erfolgt im Dialogfeld **Warning** durch Klicken auf **Yes**.

   Das Löschen einer Gruppe löscht nicht die mit der Gruppe verknüpften Gruppenaktionen. Diese Gruppenaktionen werden jedoch nach dem Löschen der Gruppe nicht mehr zugeordnet.

Hinzufügen von Gruppenregeln in Active IQ Unified Manager

Sie können Gruppenregeln für eine Gruppe erstellen, um Storage Objekte wie Volumes, Cluster oder Storage Virtual Machines (SVMs) dynamisch zur Gruppe hinzuzufügen. Für die Erstellung einer Gruppenregel muss mindestens eine Bedingungsgruppe mit mindestens einer Bedingung konfiguriert sein.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Aktuell überwachte Storage-Objekte werden hinzugefügt, sobald die Gruppenregel erstellt wird. Neue Objekte werden erst nach Abschluss des Überwachungszyklus hinzugefügt.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Im Reiter **Gruppenregeln** kann **Hinzufügen** ausgewählt werden.
3. Im Dialogfeld **Gruppenregel hinzufügen** ist ein Name für die Gruppenregel anzugeben.
4. Im Feld **Zielobjekttyp** ist der Typ des Storage Objekts auszuwählen, das gruppiert werden soll.
5. Im Feld **Gruppe** ist die gewünschte Gruppe auszuwählen, für die Gruppenregeln erstellt werden sollen.
6. Im Abschnitt **Bedingungen** sind die folgenden Schritte zum Erstellen einer Bedingung, einer Bedingungsgruppe oder beider Elemente auszuführen:

Zum Erstellen….	Folgendes ist zu tun…
Eine Bedingung	a. Es ist ein Operand aus der Liste der Operanden auszuwählen. b. Als Operator stehen entweder **Enthält** oder **Ist** zur Auswahl. c. Es ist ein Wert einzugeben oder ein Wert aus der verfügbaren Liste auszuwählen.

Zum Erstellen….	Folgendes ist zu tun…
Eine Bedingungsgruppe	a. **Bedingungsgruppe hinzufügen** auswählen b. Es ist ein Operand aus der Liste der Operanden auszuwählen. c. Als Operator stehen entweder **Enthält** oder **Ist** zur Auswahl. d. Es ist ein Wert einzugeben oder ein Wert aus der verfügbaren Liste auszuwählen. e. Mit **Bedingung hinzufügen** lassen sich bei Bedarf weitere Bedingungen erstellen; die Schritte a bis d sind für jede Bedingung zu wiederholen.

7. Klicken Sie auf **Add**.

Beispiel zum Erstellen einer Gruppenregel

Im Dialogfeld „Gruppenregel hinzufügen“ sind zum Erstellen einer Gruppenregel die folgenden Schritte erforderlich, einschließlich der Konfiguration einer Bedingung und des Hinzufügens einer Bedingungsgruppe:

Schritte

1. Einen Namen für die Gruppenregel angeben.
2. Der Objekttyp ist als Storage Virtual Machine (SVM) auszuwählen.
3. Eine Gruppe aus der Liste der Gruppen auswählen.
4. Im Abschnitt „Bedingungen“ ist **Object Name** als Operand auszuwählen.
5. Als Operator ist **Enthält** festzulegen.
6. Die Eingabe des Werts erfolgt als `svm_data`.
7. Auf **Bedingungsgruppe hinzufügen** klicken.
8. Als Operand wird **Object Name** ausgewählt.
9. Als Operator ist **Enthält** festzulegen.
10. Die Eingabe des Werts erfolgt als `vol`.
11. Anschließend erfolgt die Auswahl von **Bedingung hinzufügen**.
12. Anschließend werden die Schritte 8 bis 10 erneut ausgeführt; dabei wird in Schritt 8 **data-priority** als Operand, in Schritt 9 **Is** als Operator und in Schritt 10 **critical** als Wert ausgewählt.
13. Mit **Hinzufügen** erstellen Sie die Bedingung für die Gruppenregel.

Bearbeiten von Gruppenregeln in Active IQ Unified Manager

Sie können Gruppenregeln bearbeiten, um die Bedingungsgruppen und die Bedingungen innerhalb einer Bedingungsgruppe zu ändern und so Storage Objekte zu einer bestimmten Gruppe hinzuzufügen oder daraus zu entfernen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Auf der Registerkarte **Gruppenregeln** ist die Gruppenregel auszuwählen, die bearbeitet werden soll, und anschließend auf **Bearbeiten** zu klicken.
3. Im Dialogfeld **Gruppenregel bearbeiten** können Sie den Gruppenregelnamen, den zugehörigen Gruppennamen, die Bedingungsgruppen und die Bedingungen nach Bedarf ändern.

   Der Zielobjekttyp für eine Gruppenregel kann nicht geändert werden.

4. Auf **Speichern** klicken.

Gruppenregeln in Active IQ Unified Manager löschen

Eine Gruppenregel kann aus Active IQ Unified Manager gelöscht werden, wenn sie nicht mehr benötigt wird.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Wenn eine Gruppenregel gelöscht wird, werden die zugehörigen Speicherobjekte aus der Gruppe entfernt.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Im Reiter **Gruppenregeln** erfolgt die Auswahl der zu löschenden Gruppenregel; anschließend wird auf **Löschen** geklickt.
3. Die Bestätigung der Löschung erfolgt im Dialogfeld **Warning** durch Klicken auf **Yes**.

Hinzufügen von Gruppenaktionen in Active IQ Unified Manager

Sie können Gruppenaktionen konfigurieren, die auf Storage Objekte in einer Gruppe angewendet werden sollen. Durch die Konfiguration von Aktionen für eine Gruppe sparen Sie Zeit, da Sie diese Aktionen nicht jedem Objekt einzeln hinzufügen müssen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Auf der Registerkarte **Group Actions** steht die Option **Add** zur Auswahl.
3. Im Dialogfeld **Gruppenaktion hinzufügen** werden ein Name und eine Beschreibung für die Aktion eingegeben.
4. Im Menü **Group** erfolgt die Auswahl der Gruppe, für die die Aktion konfiguriert werden soll.
5. Im Menü **Aktionstyp** wird ein Aktionstyp ausgewählt.

   Das Dialogfeld erweitert sich, sodass Sie den ausgewählten Aktionstyp mit den erforderlichen Parametern konfigurieren können.

6. Zur Konfiguration einer Gruppenaktion sind geeignete Werte für die erforderlichen Parameter einzugeben.

7. Klicken Sie auf **Add**.

Bearbeitung von Gruppenaktionen in Active IQ Unified Manager

Sie können die in Unified Manager konfigurierten Gruppenaktionsparameter bearbeiten, z. B. den Gruppenaktionsnamen, die Beschreibung, den zugehörigen Gruppennamen und die Parameter des Aktionstyps.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Auf der Registerkarte **Gruppenaktionen** können Sie die Gruppenaktion auswählen, die Sie bearbeiten möchten, und anschließend auf **Bearbeiten** klicken.
3. Im Dialogfeld **Gruppenaktion bearbeiten** können Sie nach Bedarf den Namen der Gruppenaktion, die Beschreibung, den zugehörigen Gruppennamen und die Parameter des Aktionstyps ändern.
4. Auf **Speichern** klicken.

Konfiguration von Schwellenwerten für den Volume-Zustand für Gruppen in Active IQ Unified Manager

Sie können Systemstatusschwellenwerte auf Gruppenebene für Volumes hinsichtlich Kapazität, Snapshot-Kopien, Qtree-Kontingenten, Wachstum und Inodes konfigurieren.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die Gruppenaktion des Typs „Volumen-Systemstatusschwelle“ wird nur auf Volumes einer Gruppe angewendet.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Auf der Registerkarte **Group Actions** steht die Option **Add** zur Auswahl.
3. Einen Namen und eine Beschreibung für die Gruppenaktion eingeben.
4. Im Dropdown-Menü **Gruppe** erfolgt die Auswahl einer Gruppe, für die die Gruppenaktion konfiguriert werden soll.
5. Als Systemstatusschwellenwert für das Volume wird **Action Type** ausgewählt.
6. Auswahl der Kategorie, für die der Schwellenwert festgelegt werden soll.
7. Die erforderlichen Werte für den Systemstatus-Schwellenwert werden eingegeben.
8. Klicken Sie auf **Add**.

Gruppenaktionen in Active IQ Unified Manager löschen

Sie können eine Gruppenaktion in Unified Manager löschen, wenn sie nicht mehr benötigt wird.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Wenn Sie die Gruppenaktion für den Volume Systemstatusschwellenwert löschen, werden globale Schwellenwerte auf die Storage Objekte in dieser Gruppe angewendet. Objektbezogene Systemstatusschwellenwerte, die für das Storage Objekt festgelegt sind, bleiben davon unberührt.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Auf der Registerkarte **Gruppenaktionen** ist die Gruppenaktion auszuwählen, die gelöscht werden soll, und anschließend **Löschen**.
3. Die Bestätigung der Löschung erfolgt im Dialogfeld **Warning** durch Klicken auf **Yes**.

Neuanordnung von Gruppenaktionen in Active IQ Unified Manager

Sie können die Reihenfolge der Gruppenaktionen ändern, die auf die Storage-Objekte in einer Gruppe angewendet werden sollen. Gruppenaktionen werden basierend auf ihrem Rang nacheinander auf Storage-Objekte angewendet. Der niedrigste Rang wird der Gruppenaktion zugewiesen, die Sie zuletzt konfiguriert haben. Sie können den Rang der Gruppenaktion entsprechend Ihren Anforderungen ändern.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können entweder eine einzelne Zeile oder mehrere Zeilen auswählen und anschließend mehrere Drag-and-Drop-Vorgänge ausführen, um die Rangfolge der Gruppenaktionen zu ändern. Die Änderungen müssen jedoch gespeichert werden, damit sich die Neupriorisierung im Raster der Gruppenaktionen widerspiegelt.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage Management** > **Gruppen**.
2. Auf der Registerkarte **Gruppenaktionen** auf **Neu anordnen** klicken.
3. Im Dialogfeld **Gruppenaktionen neu anordnen** können Sie die Zeilen per Drag & Drop verschieben, um die Reihenfolge der Gruppenaktionen nach Bedarf neu zu ordnen.
4. Auf **Speichern** klicken.

Speicherobjektereignisse mithilfe von Annotationen priorisieren

Weitere Informationen zu Annotationen

Informationen zu Annotationen in Active IQ Unified Manager

Eine Annotation ist ein Text-String (der Name), der einem anderen Text-String (dem Wert) zugeordnet ist. Jedes Annotationsname-Wert-Paar kann mithilfe von Annotationsregeln dynamisch Storage Objekten zugeordnet werden. Wenn Sie Storage Objekte vordefinierten Annotationen zuordnen, können Sie die damit verbundenen Ereignisse filtern und anzeigen. Sie können Annotationen auf Cluster, Volumes und Storage Virtual Machines (SVMs) anwenden.

Jeder Annotationsname kann mehrere Werte haben; jedes Name-Wert-Paar kann über Regeln einem Storage Objekt zugeordnet werden.

Sie können beispielsweise eine Annotation namens „`data-center`“ mit den Werten „`Boston`“ und „`Canada`“ erstellen. Anschließend können Sie die Annotation „`data-center`“ mit dem Wert „`Boston`“ auf Volume v1 anwenden. Wenn für ein beliebiges Ereignis auf Volume v1, das mit „`data-center`“ annotiert ist, eine Warnung generiert wird, gibt die generierte E-Mail den Standort des Volumes, „`Boston`“, an. Dadurch können Sie das Problem priorisieren und beheben.

Wie Annotationsregeln in Active IQ Unified Manager funktionieren

Eine Annotationsregel ist ein Kriterium, das Sie definieren, um Storage-Objekte (Volumes, Cluster oder Storage Virtual Machines (SVMs)) zu annotieren. Sie können entweder Bedingungsgruppen oder Bedingungen verwenden, um Annotationsregeln zu definieren.

- Sie müssen einer Annotation eine Annotationsregel zuordnen.
- Einer Annotationsregel muss ein Objekttyp zugeordnet sein; einer Annotationsregel kann nur ein Objekttyp zugeordnet werden.
- Unified Manager fügt Speicherobjekten nach jedem Überwachungszyklus oder beim Erstellen, Bearbeiten, Löschen oder Neuanordnen einer Regel Anmerkungen hinzu oder entfernt diese.
- Eine Annotationsregel kann eine oder mehrere Bedingungsgruppen haben, und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben.
- Speicherobjekte können mehrere Annotationen aufweisen. Eine Annotationsregel für eine bestimmte Annotation kann in den Regelbedingungen auch unterschiedliche Annotationen verwenden, um bereits annotierten Objekten eine weitere Annotation hinzuzufügen.

Bedingungen

Sie können mehrere Bedingungsgruppen erstellen, und jede Bedingungsgruppe kann eine oder mehrere Bedingungen enthalten. Sie können alle definierten Bedingungsgruppen in einer Annotationsregel einer Annotation anwenden, um Storage-Objekte zu annotieren.

Bedingungen innerhalb einer Bedingungsgruppe werden mit logischem UND verknüpft. Alle Bedingungen einer Bedingungsgruppe müssen erfüllt sein. Beim Erstellen oder Ändern einer Annotationsregel wird eine Bedingung erstellt, die nur auf diejenigen Storage-Objekte angewendet wird und nur diejenigen Storage-Objekte auswählt und annotiert, die alle Bedingungen der Bedingungsgruppe erfüllen. Sie können mehrere Bedingungen innerhalb einer Bedingungsgruppe verwenden, um den Umfang der zu annotierenden Storage-Objekte einzugrenzen.

Sie können Bedingungen mit Storage-Objekten erstellen, indem Sie die folgenden Operanden und Operatoren verwenden und den erforderlichen Wert angeben.

Storage-Objekttyp	Anwendbare Operanden
Volumen	• Objektname • Name des besitzenden Clusters • Name der zugehörigen SVM • Anmerkungen
SVM	• Objektname • Name des besitzenden Clusters • Anmerkungen

Storage-Objekttyp	Anwendbare Operanden
Cluster	• Objektname • Anmerkungen

Wenn Sie Annotation als Operanden für ein Storage-Objekt auswählen, steht Ihnen der Operator „Is“ zur Verfügung. Für alle anderen Operanden können Sie entweder „Is“ oder „Contains“ als Operator auswählen. Wenn Sie den Operator „Is“ auswählen, wird die Bedingung auf eine exakte Übereinstimmung des Operandenwerts mit dem für den ausgewählten Operanden angegebenen Wert geprüft. Wenn Sie den Operator „Contains“ auswählen, wird die Bedingung daraufhin geprüft, ob eines der folgenden Kriterien erfüllt ist:

- Der Operandenwert stimmt exakt mit dem Wert des ausgewählten Operanden überein.
- Der Operandenwert enthält den für den ausgewählten Operanden angegebenen Wert.

Beispiel einer Annotationsregel mit Bedingungen

Es liegt eine Annotationsregel mit einer Bedingungsgruppe für ein Volume mit den folgenden zwei Bedingungen vor:

- Der Name enthält “vol”
- Der SVM-Name lautet “data_svm”

Diese Annotationsregel versieht alle Volumes, deren Name „`vol`“ enthält und die auf SVMs mit dem Namen „`data_svm`“ gehostet werden, mit der ausgewählten Annotation und dem Annotationstyp.

Bedingungsgruppen

Bedingungsgruppen werden mit logischem ODER ausgeführt und anschließend auf Storage-Objekte angewendet. Die Storage-Objekte müssen die Anforderungen einer der Bedingungsgruppen erfüllen, um annotiert zu werden. Die Storage-Objekte, die die Bedingungen aller Bedingungsgruppen erfüllen, werden annotiert. Sie können Bedingungsgruppen verwenden, um den Umfang der zu annotierenden Storage-Objekte zu erweitern.

Beispiel einer Annotationsregel mit Bedingungsgruppen

Eine Annotationsregel für ein Volume mit zwei Bedingungsgruppen enthält in jeder Gruppe die folgenden zwei Bedingungen:

- Bedingungsgruppe 1
  - Der Name enthält “vol”
  - Der SVM-Name ist “data_svm” Diese Bedingungsgruppe annotiert alle Volumes, die “vol” in ihrem Namen enthalten und auf SVMs mit dem Namen “data_svm” gehostet sind.
- Bedingungsgruppe 2
  - Der Name enthält “vol”
  - Der Annotationswert von data-priority ist “critical” Diese Bedingungsgruppe annotiert alle Volumes, die “vol” in ihrem Namen enthalten und mit dem Annotationswert data-priority als “critical” annotiert sind.

Wenn eine Annotationsregel, die diese beiden Bedingungsgruppen enthält, auf Storage-Objekte angewendet wird, werden die folgenden Storage-Objekte annotiert:

- Alle Volumes, die “vol” in ihrem Namen enthalten und auf der SVM mit dem Namen “data_svm” gehostet sind.
- Alle Volumes, deren Namen “vol” enthalten und die mit dem Datenprioritäts-Anmerkungswert “critical” gekennzeichnet sind.

Vordefinierte Annotationswerte in Active IQ Unified Manager verstehen

Die **Datenpriorität** ist eine vordefinierte Annotation mit den Werten „geschäftskritisch“, „Hoch“ und „Niedrig“. Mit diesen Werten lassen sich Storage Objekte anhand der Priorität der darin enthaltenen Daten annotieren. Die vordefinierten Annotationswerte können nicht bearbeitet oder gelöscht werden.

- **Datenpriorität:Geschäftskritisch**

  Diese Annotation wird auf Storage Objekte angewendet, die geschäftskritische Daten enthalten. Beispielsweise können Objekte, die Produktionsanwendungen enthalten, als geschäftskritisch eingestuft werden.

- **Datenpriorität:Hoch**

  Diese Annotation gilt für Storage-Objekte, die Daten mit hoher Priorität enthalten. Beispielsweise können Objekte, die Geschäftsanwendungen hosten, als Objekte mit hoher Priorität eingestuft werden.

- **Datenpriorität:Niedrig**

  Diese Annotation wird auf Storage-Objekte angewendet, die Daten mit niedriger Priorität enthalten. Beispielsweise können Objekte auf Sekundär-Storage, wie etwa Sicherungs- und Spiegelungsziele, eine niedrige Priorität haben.

Dynamisches Hinzufügen von Anmerkungen in Active IQ Unified Manager

Beim Erstellen benutzerdefinierter Annotationen ordnet Unified Manager Cluster, Storage Virtual Machines (SVMs) und Volumes den Annotationen mithilfe von Regeln dynamisch zu. Diese Regeln weisen die Annotationen Storage-Objekten automatisch zu.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Annotations**.
2. Auf der Seite **Anmerkungen** kann **Anmerkung hinzufügen** ausgewählt werden.
3. Im Dialogfeld **Anmerkung hinzufügen** können Sie einen Namen und eine Beschreibung für die Anmerkung eingeben.
4. Optional: Im Abschnitt **Anmerkungswerte** können Sie der Anmerkung Werte hinzufügen, indem Sie auf **Hinzufügen** klicken.
5. Auf **Speichern** klicken.

Werte zu Anmerkungen in Active IQ Unified Manager hinzufügen

Sie können Annotationen Werte hinzufügen und anschließend Storage-Objekte mit einem

bestimmten Annotationsname-Wert-Paar verknüpfen. Das Hinzufügen von Werten zu Annotationen hilft Ihnen, Storage-Objekte effektiver zu managen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können vordefinierten Annotationen keine Werte hinzufügen.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Annotations**.
2. Auf der Seite **Anmerkungen** können Sie die Anmerkung auswählen, der Sie einen Wert hinzufügen möchten, und anschließend im Abschnitt **Werte** auf **Hinzufügen** klicken.
3. Im Dialogfeld **Anmerkungswert hinzufügen** ist für die Anmerkung ein Wert anzugeben.

   Der von Ihnen angegebene Wert muss für die ausgewählte Annotation eindeutig sein.

4. Klicken Sie auf **Add**.

Anmerkungen in Active IQ Unified Manager löschen

Benutzerdefinierte Anmerkungen und deren Werte können gelöscht werden, wenn sie nicht mehr benötigt werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Die Annotationswerte dürfen nicht in anderen Annotationen oder Gruppenregeln verwendet werden.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Annotations**.
2. Im Tab **Annotations** ist die Anmerkung auszuwählen, die gelöscht werden soll.

   Es erscheinen die Details der ausgewählten Annotation.

3. Zum Löschen der ausgewählten Annotation und ihres Werts **Actions** > **Delete** auswählen.
4. Im Warnungsdialogfeld erfolgt die Bestätigung der Löschung durch Klicken auf **Ja**.

Die Liste der Anmerkungen und Details in Active IQ Unified Manager anzeigen

Sie können die Liste der Annotationen anzeigen, die dynamisch Clustern, Volumes und Storage Virtual Machines (SVMs) zugeordnet sind. Außerdem können Sie Details wie die Beschreibung, erstellt von, Erstellungsdatum, Werte, Regeln und die mit der Annotation verknüpften Objekte einsehen.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Annotations**.
2. Im Reiter **Anmerkungen** zeigt ein Klick auf den Namen der Anmerkung die zugehörigen Details an.

Werte aus Anmerkungen in Active IQ Unified Manager löschen

Sie können Werte löschen, die mit benutzerdefinierten Annotationen verknüpft sind, wenn der jeweilige Wert nicht mehr auf die Annotation zutrifft.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Der Annotationswert darf keiner Annotationsregel oder Gruppenregel zugeordnet sein.

Werte aus vordefinierten Annotationen können nicht gelöscht werden.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Annotations**.
2. In der Liste der Anmerkungen auf der Registerkarte **Anmerkungen** können Sie die Anmerkung auswählen, aus der ein Wert gelöscht werden soll.
3. Im Bereich **Werte** der Registerkarte **Anmerkungen** ist der zu löschende Wert auszuwählen; anschließend ist auf **Löschen** zu klicken.
4. Im Dialogfeld **Warning** erfolgt die Auswahl von **Yes**.

   Der Wert wird gelöscht und in der Liste der Werte für die ausgewählte Annotation nicht mehr angezeigt.

Erstellen von Annotationsregeln in Active IQ Unified Manager

Sie können Annotationsregeln erstellen, die Unified Manager verwendet, um Storage-Objekte wie Volumes, Cluster oder Storage Virtual Machines (SVMs) dynamisch zu annotieren.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Storage-Objekte, die aktuell überwacht werden, werden sofort nach Erstellung der Annotationsregel annotiert. Neue Objekte werden erst nach Abschluss des Überwachungszyklus annotiert.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Annotations**.
2. Im Reiter **Anmerkungsregeln** erfolgt die Auswahl von **Hinzufügen**.
3. Im Dialogfeld **Add Annotation Rule** wird ein Name für die Anmerkungsregel angegeben.
4. Im Feld **Zielobjekttyp** erfolgt die Auswahl des Typs des Storage Objekts, das Sie annotieren möchten.
5. In den Feldern **Apply Annotation** können Sie die Annotation und den Annotationswert auswählen, die Sie verwenden möchten.
6. Im Abschnitt „Bedingungen“ erfolgt die entsprechende Aktion zum Erstellen einer Bedingung, einer Bedingungsgruppe oder von beidem:

Zum Erstellen…	Folgendes ist zu tun…
Eine Bedingung	a. Es ist ein Operand aus der Liste der Operanden auszuwählen. b. Als Operator stehen entweder **Enthält** oder **Ist** zur Auswahl. c. Es ist ein Wert einzugeben oder ein Wert aus der verfügbaren Liste auszuwählen.
Eine Bedingungsgruppe	a. **Bedingungsgruppe hinzufügen** auswählen. b. Es ist ein Operand aus der Liste der Operanden auszuwählen. c. Als Operator stehen entweder **Enthält** oder **Ist** zur Auswahl. d. Es ist ein Wert einzugeben oder ein Wert aus der verfügbaren Liste auszuwählen. e. Mit **Bedingung hinzufügen** lassen sich bei Bedarf weitere Bedingungen erstellen; die Schritte a bis d sind für jede Bedingung zu wiederholen.

7. Klicken Sie auf **Add**.

Beispiel für die Erstellung einer Annotationsregel

Im Dialogfeld „Add Annotation Rule“ sind zum Erstellen einer Anmerkungsregel die folgenden Schritte erforderlich, einschließlich der Konfiguration einer Bedingung und des Hinzufügens einer Bedingungsgruppe:

Schritte

1. Für die Annotationsregel einen Namen festlegen.
2. Als Zielobjekttyp sollte Storage Virtual Machine (SVM) ausgewählt werden.
3. Aus der Liste der Annotationen wird eine Annotation ausgewählt und ein Wert angegeben.
4. Im Abschnitt „Bedingungen“ ist **Object Name** als Operand auszuwählen.
5. Als Operator ist **Enthält** festzulegen.
6. Die Eingabe des Werts erfolgt als `svm_data`.
7. Auf **Bedingungsgruppe hinzufügen** klicken.
8. Als Operand wird **Object Name** ausgewählt.
9. Als Operator ist **Enthält** festzulegen.
10. Die Eingabe des Werts erfolgt als `vol`.
11. Anschließend erfolgt die Auswahl von **Bedingung hinzufügen**.
12. Die Schritte 8 bis 10 werden wiederholt, indem in Schritt 8 **data-priority** als Operand, in Schritt 9 **Is** als Operator und in Schritt 10 **mission-critical** als Wert ausgewählt wird.
13. Klicken Sie auf **Add**.

Anmerkungen in Active IQ Unified Manager manuell zu einzelnen Storage-Objekten hinzufügen

Sie können ausgewählte Volumes, Cluster und SVMs manuell annotieren, ohne Annotationsregeln zu verwenden. Sie können ein einzelnes Storage-Objekt oder mehrere Storage-Objekte annotieren und die erforderliche Name-Wert-Paar-Kombination für die Annotation angeben.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Wechseln Sie zu den Storage-Objekten, die Sie mit Anmerkungen versehen möchten:

Zum Hinzufügen von Anmerkungen…	Folgendes ist zu tun…
Cluster	a. Die Auswahl erfolgt über **Storage** > **Clusters**. b. Ein oder mehrere Cluster sind auszuwählen.
Volumes	a. Die Navigation erfolgt über **Storage** > **Volumes**. b. Auswahl eines oder mehrerer Volumes.
SVMs	a. Anschließend erfolgt die Auswahl von **Storage** > **SVMs**. b. Eine oder mehrere SVMs auswählen.

2. Nach einem Klick auf **Annotate** können Sie ein Name-Wert-Paar auswählen.
3. Auf **Anwenden** klicken.

Anmerkungsregeln in Active IQ Unified Manager bearbeiten

Sie können Annotationsregeln bearbeiten, um die Bedingungsgruppen und die Bedingungen innerhalb der Bedingungsgruppe zu ändern und so Annotationen zu Storage Objekten hinzuzufügen oder von ihnen zu entfernen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Annotationen werden von Storage-Objekten getrennt, wenn Sie die zugehörigen Annotationsregeln bearbeiten.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Annotations**.
2. Im Reiter **Annotation Rules** können Sie die Anmerkungsregel auswählen, die Sie bearbeiten möchten, und anschließend auf **Actions** > **Edit** klicken.
3. Im Dialogfeld **Anmerkungsregel bearbeiten** können Sie nach Bedarf den Regelnamen, den Anmerkungsnamen und -wert, die Bedingungsgruppen und die Bedingungen ändern.

   Der Zielobjekttyp einer Annotationsregel kann nicht geändert werden.

4. Auf **Speichern** klicken.

Konfiguration von Bedingungen für Annotationsregeln in Active IQ Unified Manager

Sie können eine oder mehrere Bedingungen konfigurieren, um Annotationsregeln zu erstellen, die Unified Manager auf die Storage-Objekte anwendet. Die Storage-Objekte, die die Annotationsregel erfüllen, erhalten den in der Regel angegebenen Wert als Annotation.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Annotations**.
2. Im Reiter **Anmerkungsregeln** erfolgt die Auswahl von **Hinzufügen**.
3. Im Dialogfeld **Add Annotation Rule** wird ein Name für die Regel eingegeben.
4. Ein Objekttyp ist aus der Liste „Zielobjekttyp“ auszuwählen; anschließend sind ein Anmerkungsname und ein Wert aus der Liste auszuwählen.
5. Im Abschnitt **Bedingungen** des Dialogfelds erfolgt die Auswahl eines Operanden und eines Operators aus der Liste sowie die Eingabe eines Bedingungswerts; mit **Bedingung hinzufügen** lässt sich eine neue Bedingung erstellen.
6. Dann die Option **Speichern und Hinzufügen** auswählen.

Beispiel für die Konfiguration einer Bedingung für eine Annotationsregel

Eine Bedingung für den Objekttyp SVM, bei der der Objektname “svm_data” enthält.

Im Dialogfeld „Anmerkungsregel hinzufügen“ sind die folgenden Schritte zur Konfiguration der Bedingung auszuführen:

Schritte

1. Einen Namen für die Annotationsregel eingeben.
2. Der Zielobjekttyp wird als SVM ausgewählt.
3. Eine Annotation aus der Liste der Annotationen sowie einen Wert auswählen.
4. Im Feld **Bedingungen** erfolgt die Auswahl von **Objektname** als Operand.
5. Als Operator ist **Enthält** festzulegen.
6. Die Eingabe des Werts erfolgt als `svm_data`.
7. Klicken Sie auf **Add**.

Anmerkungsregeln in Active IQ Unified Manager löschen

Annotationsregeln können aus Active IQ Unified Manager gelöscht werden, wenn sie nicht mehr erforderlich sind.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Beim Löschen einer Annotationsregel wird die Annotation von den Storage Objekten getrennt und entfernt.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Annotations**.
2. Auf der Registerkarte **Anmerkungsregeln** wählen Sie die Anmerkungsregel aus, die Sie löschen möchten, und klicken dann auf **Löschen**.
3. Im Dialogfeld **Warning** dient **Yes** zur Bestätigung des Löschvorgangs.

Neuordnung von Anmerkungsregeln in Active IQ Unified Manager

Sie können die Reihenfolge ändern, in der Unified Manager Annotationsregeln auf Storage-Objekte anwendet. Annotationsregeln werden entsprechend ihrer Priorität nacheinander auf Storage-Objekte angewendet. Beim Konfigurieren einer Annotationsregel ist ihr Rang der niedrigste. Sie können den Rang der Annotationsregel jedoch entsprechend Ihren Anforderungen ändern.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können entweder eine einzelne Zeile oder mehrere Zeilen auswählen und viele Drag-and-Drop-Vorgänge ausführen, um die Rangfolge der Anmerkungsregeln zu ändern. Die Änderungen müssen jedoch gespeichert werden, damit die Neugewichtung auf der Registerkarte Annotation Rules angezeigt wird.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Annotations**.
2. Auf der Registerkarte **Annotation Rules** kann auf **Reorder** geklickt werden.
3. Im Dialogfeld **Anmerkungsregeln neu anordnen** können Sie einzelne oder mehrere Zeilen per Drag & Drop verschieben, um die Reihenfolge der Anmerkungsregeln neu zu ordnen.
4. Auf **Speichern** klicken.

   Die Änderungen müssen gespeichert werden, damit die Neuanordnung angezeigt wird.

Versand eines Support-Bundles über die Web-Benutzeroberfläche und die Managementplattform

Über die Web-Benutzeroberfläche und die Wartungskonsole in Active IQ Unified Manager kann ein Supportpaket gesendet werden

Sie sollten ein Supportpaket senden, wenn das bei Ihnen aufgetretene Problem eine detailliertere Diagnose und Fehlerbehebung erfordert, als eine AutoSupport Nachricht bieten kann. Sie können ein Supportpaket mithilfe der Unified Manager Web-UI und der Managementplattform an den technischen Support senden.

Unified Manager kann maximal zwei vollständige Support-Bundles und drei Lightweight-Support-Bundles gleichzeitig speichern.

Verwandte Informationen

"Unified Manager Benutzerrollen und -Funktionen"

AutoSupport Meldungen an den technischen Support in

Die AutoSupport Seite ermöglicht es Ihnen, vordefinierte und bedarfsgesteuerte AutoSupport Nachrichten an Ihr technisches Supportteam zu senden, um den korrekten Betrieb Ihrer Umgebung sicherzustellen und Sie bei der Wahrung der Integrität Ihrer Umgebung zu unterstützen. AutoSupport ist standardmäßig aktiviert und sollte nicht deaktiviert werden, damit Sie die Vorteile von NetAppActive IQ nutzen können.

Sie können bei Bedarf diagnostische Systeminformationen und detaillierte Daten über den Unified Manager Server in einer Nachricht senden, den regelmäßigen Versand einer Nachricht planen oder sogar Support-Bundles generieren und an das Team des technischen Supports senden.

> Ein Benutzer mit der Rolle eines Storage Administrators kann bedarfsgesteuerte AutoSupport Nachrichten und Support-Bundles an den technischen Support senden. Allerdings kann nur ein Administrator oder Wartungsbenutzer die periodische AutoSupport Funktion aktivieren oder deaktivieren und die HTTP-Einstellungen wie im Abschnitt „Einrichten eines HTTP Proxyservers“ beschrieben konfigurieren. In einer Umgebung, in der ein HTTP Proxyserver verwendet werden muss, sollte die Konfiguration abgeschlossen sein, bevor ein Storage Administrator bedarfsgesteuerte AutoSupport Nachrichten und Support-Bundles an den technischen Support senden kann.

Senden von AutoSupport Nachrichten auf Abruf

Sie können eine Nachricht auf Abruf generieren und an den technischen Support, an einen bestimmten E-Mail-Empfänger oder an beide senden.

Schritte

1. Unter **Allgemein** > **AutoSupport** stehen eine oder beide der folgenden Aktionen zur Verfügung:
2. Falls die AutoSupport Nachricht an den technischen Support gesendet werden soll, ist das Kästchen **Send to Technical Support** auszuwählen.
3. Wenn die AutoSupport Nachricht an einen bestimmten E-Mail-Empfänger gesendet werden soll, ist das Kästchen **Send to Email Recipient** auszuwählen und die E-Mail-Adresse des Empfängers einzugeben.
4. Auf **Speichern** klicken.
5. **Generieren und Senden AutoSupport** auswählen.

Aktivierung von periodischem AutoSupport

Sie können regelmäßig spezifische, vordefinierte Nachrichten an den technischen Support senden, um Probleme zu diagnostizieren und zu beheben. Diese Funktion ist standardmäßig aktiviert. Falls sie deaktiviert ist, kann ein Administrator oder Wartungsbenutzer die Einstellungen aktivieren.

Schritte

1. Der Pfad lautet **Allgemein** > **AutoSupport**.
2. Im Abschnitt „Periodisch“ für AutoSupport erfolgt die Auswahl des Kästchens **Senden von AutoSupport Daten periodisch an Active IQ aktivieren**.
3. Falls erforderlich, lassen sich Name, Port und Authentifizierungsinformationen für den HTTP Proxyserver wie im Abschnitt „HTTP Proxyserver einrichten“ beschrieben definieren.
4. Auf **Speichern** klicken.

Hochladen des Support-Bundles bei Bedarf

Je nach Anforderung für die Fehlerbehebung kann ein Support-Paket erstellt und an den technischen Support gesendet werden. Unified Manager speichert nur die beiden zuletzt erstellten Support-Pakete. Das System löscht ältere Support-Pakete.

Da manche Arten von Supportdaten viele Clusterressourcen beanspruchen oder lange zur Fertigstellung benötigen können, lässt sich beim Auswählen des vollständigen Supportpakets die Größe des Supportpakets durch Ein- oder Ausschließen bestimmter Datentypen reduzieren. Alternativ kann ein schlankes Supportpaket erstellt werden, das nur 30 Tage an Protokollen und Konfigurationsdatenbankeinträgen enthält; Performance-Daten, Erfassungsaufzeichnungsdateien und Server-Heap-Dump sind nicht enthalten.

Schritte

1. Der Pfad lautet **Allgemein** > **AutoSupport**.
2. Im Abschnitt „On-Demand Support Bundle“ steht die Option **Generate and Send Support Bundle** zur Verfügung.
3. Zum Senden eines Light-Support-Bundles an den technischen Support ist im Popup-Fenster „Support Bundle generieren und senden“ das Kästchen **Light-Support-Bundle generieren** zu aktivieren.
4. Alternativ kann zum Senden eines vollständigen Supportpakets das Kästchen **Generate full support bundle** aktiviert werden. Anschließend können die spezifischen Datentypen ausgewählt werden, die in das Supportpaket aufgenommen oder daraus ausgeschlossen werden sollen.

   Auch wenn Sie keinen Datentyp auswählen, enthält das Support Bundle dennoch andere Daten von Unified Manager.

5. Durch Aktivieren des Kästchens **Send the bundle to technical support** wird das Bundle generiert und an den technischen Support gesendet. Wenn dieses Kästchen nicht aktiviert wird, wird das Bundle generiert und lokal auf dem Unified Manager Server gespeichert. Das generierte Support-Bundle ist zur späteren Verwendung im Verzeichnis /support auf VMware-Systemen, in `/opt/netapp/data/support/` auf Linux-Systemen und in `ProgramData\NetApp\OnCommandAppData\ocum\support` auf Windows-Systemen verfügbar.
6. Anschließend ist **Senden** auszuwählen.

Einrichten des HTTP Proxyservers

Sie können einen Proxy für den Internetzugang festlegen, um AutoSupport Inhalte an den Support zu senden, wenn Ihre Umgebung keinen direkten Zugriff vom Unified Manager Server ermöglicht. Dieser Abschnitt ist nur für Administratoren und Wartungsbenutzer verfügbar.

- **HTTP Proxy verwenden**

  Mit diesem Kästchen wird der als HTTP-Proxy verwendete Server angegeben.

  Sie geben den Hostnamen oder die IP-Adresse des Proxyservers sowie die für die Verbindung zum Server verwendete Portnummer ein.

- **Authentifizierung verwenden**

  Dieses Kästchen wird verwendet, wenn für den Zugriff auf den als HTTP Proxyserver verwendeten Server Informationen zur Authentifizierung angegeben werden müssen.

  Benutzername und Passwort, die für die Authentifizierung beim HTTP-Proxy erforderlich sind.

HTTP-Proxys mit ausschließlich Basic Authentication werden nicht unterstützt.

Zugriff auf die Wartungskonsole in Active IQ Unified Manager

Wenn die Unified Manager Benutzeroberfläche nicht in Betrieb ist oder wenn Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Wartungs-Managementplattform zugreifen, um Ihr Unified Manager System zu managen.

Bevor Sie beginnen

Sie müssen Unified Manager installiert und konfiguriert haben.

Nach 15 Minuten Inaktivität meldet die Wartungs-Managementplattform Sie ab.

Bei der Installation auf VMware ist eine gleichzeitige Anmeldung über Secure Shell nicht möglich, wenn Sie sich bereits als Wartungsbenutzer über die VMware Managementplattform angemeldet haben.

Schritt

1. Der Zugriff auf die Managementplattform erfolgt in den folgenden Schritten:

Auf diesem Betriebssystem…	Folgen Sie diesen Schritten…
VMware	a. Die Verbindung zur IP-Adresse oder zur vollqualifizierten Domain der virtuellen Unified Manager Appliance erfolgt mithilfe von Secure Shell. b. Zur Anmeldung bei der Managementplattform dienen Ihr Wartungsbenutzername und Ihr Passwort.
Linux	a. Die Verbindung mit der IP-Adresse oder dem vollqualifizierten Domainnamen des Unified Manager Systems erfolgt mithilfe von Secure Shell. b. Die Anmeldung am System erfolgt mit dem Benutzernamen und Passwort des Wartungsbenutzers (umadmin). c. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.
Windows	a. Für die Anmeldung am Unified Manager System werden Administratoranmeldedaten verwendet. b. Starten von PowerShell als Windows-Administrator. c. Den Befehl `maintenance_console` eingeben und die Eingabetaste drücken.

Das Menü der Unified Manager Wartungs-Managementplattform wird angezeigt.

Erstellen und Hochladen eines Support-Bundles aus Active IQ Unified Manager

Sie können ein Supportpaket mit Diagnoseinformationen erstellen, das Sie zur Unterstützung bei der Fehlerbehebung an den technischen Support senden können.

Ab Unified Manager 9.8 besteht, wenn Ihr Unified Manager Server mit dem Internet verbunden ist, auch die Möglichkeit, das Support-Bundle von der Wartungs-Managementplattform aus auf NetApp hochzuladen.

Bevor Sie beginnen

Sie müssen als Wartungsbenutzer Zugriff auf die Managementplattform haben.

Da einige Arten von Supportdaten viele Cluster-Ressourcen beanspruchen oder lange bis zum Abschluss benötigen können, können Sie beim Auswählen des vollständigen Supportpakets festlegen, welche Datentypen ein- oder ausgeschlossen werden sollen, um die Größe des Supportpakets zu reduzieren. Es besteht außerdem die Möglichkeit, ein schlankes Supportpaket zu erstellen, das nur Protokolle und Konfigurationsdatenbankeinträge der letzten 30 Tage enthält; Performance-Daten, Erfassungsaufzeichnungsdateien und Server-Heap-Dump sind nicht enthalten.

Unified Manager speichert nur die beiden zuletzt generierten Support-Bundles. Ältere Support-Bundles löscht das System.

Schritte

1. In der Managementplattform erfolgt die Auswahl von **Support/Diagnostics** im **Main Menu**.
2. Je nach gewünschtem Detaillierungsgrad im Support Bundle steht **Generate Light Support Bundle** oder **Generate Support Bundle** zur Auswahl.
3. Wenn Sie das vollständige Supportpaket wählen, stehen die folgenden Datentypen zum Ein- oder Ausschließen im Supportpaket zur Auswahl:

   - **Datenbank-Dump**

     Ein Dump der MySQL Server Datenbank.

   - **Heap-Dump**

     Eine Momentaufnahme des Status der wichtigsten Unified Manager Serverprozesse. Diese Option ist standardmäßig deaktiviert und sollte nur auf Anfrage des Kundensupports ausgewählt werden.

   - **Akquisitionsaufzeichnungen**

     Eine Aufzeichnung der gesamten Kommunikation zwischen Unified Manager und den überwachten Clustern.

   Wenn Sie alle Datentypen abwählen, wird das Support Bundle dennoch mit anderen Unified Manager Daten erstellt.

4. Durch Eingabe von `g` und anschließendes Drücken der Eingabetaste lässt sich das Support-Bundle generieren.

   Da die Generierung eines Support-Bundles ein speicherintensiver Vorgang ist, werden Sie aufgefordert, zu bestätigen, dass Sie das Support-Bundle zu diesem Zeitpunkt generieren möchten.

5. Die Eingabe von `y` sowie das anschließende Drücken der Eingabetaste generieren das Support-Bundle.

Wenn Sie das Support-Bundle jetzt nicht generieren möchten, ist `n` einzugeben; anschließend ist die Eingabetaste zu drücken.

6. Wenn Sie Datenbank-Dumpdateien in das vollständige Support-Bundle aufgenommen haben, erfolgt eine Aufforderung, den Zeitraum anzugeben, für den Performance Statistiken aufgenommen werden sollen. Das Einbeziehen von Performance Statistiken kann viel Zeit und Speicherplatz beanspruchen, daher kann die Datenbank auch ohne Performance Statistiken gedumpt werden:

   a. Das Startdatum ist im Format JJJJMMTT anzugeben.

      Beispielsweise entspricht `20210101` dem 1. Januar 2021. Wenn keine Performance-Statistiken einbezogen werden sollen, wird `n` verwendet.

   b. Einzugeben ist die Anzahl der Tage, die ab 0:00 Uhr des angegebenen Startdatums in die Statistiken einbezogen werden.

      Sie können eine Zahl von 1 bis 10 eingeben.

   Wenn Sie Performance Statistiken einschließen, zeigt das System den Zeitraum an, für den Performance Statistiken erfasst werden.

7. Nachdem das Support-Bundle erstellt wurde, werden Sie gefragt, ob Sie es zu NetApp hochladen möchten. Hierzu wird `y` eingegeben und anschließend die Eingabetaste gedrückt.

   Sie werden aufgefordert, die Nummer Ihres Supportfalls einzugeben.

8. Falls bereits eine Fallnummer vorhanden ist, wird die Nummer eingegeben und anschließend die Eingabetaste gedrückt. Andernfalls wird einfach die Eingabetaste gedrückt.

   Das Support-Paket wird auf NetApp hochgeladen.

Wenn Ihr Unified Manager Server nicht mit dem Internet verbunden ist oder Sie das Support-Bundle aus anderen Gründen nicht hochladen können, können Sie es manuell abrufen und senden. Sie können es mit einem SFTP-Client oder mithilfe von UNIX- oder Linux-CLI-Befehlen abrufen. Bei Windows Installationen können Sie Remote Desktop (RDP) verwenden, um das Support-Bundle abzurufen.

Das generierte Support-Bundle befindet sich auf VMware-Systemen im Verzeichnis /support, auf Linux-Systemen im Verzeichnis /opt/netapp/data/support/ und auf Windows-Systemen im Verzeichnis ProgramData\NetApp\OnCommandAppData\ocum\support.

Verwandte Informationen

"Unified Manager Benutzerrollen und -Funktionen"

Abrufen des Support Bundle mithilfe eines Windows Clients in Active IQ Unified Manager

Wenn Sie Windows Benutzer sind, können Sie ein Tool herunterladen und installieren, um das Support-Bundle von Ihrem Unified Manager Server abzurufen. Sie können das Support-Bundle an den technischen Support senden, um eine detailliertere Diagnose eines Problems zu erhalten. Filezilla oder WinSCP sind Beispiele für Tools, die Sie verwenden können.

Bevor Sie beginnen

Sie müssen der Wartungsbenutzer sein, um diese Aufgabe ausführen zu können.

Erforderlich ist ein Tool, das SCP oder SFTP unterstützt.

Schritte

1. Zum Abrufen des Support-Bundles wird ein Tool heruntergeladen und installiert.
2. Das Tool wird geöffnet.
3. Für die Verbindung zu Ihrem Unified Manager Verwaltungsserver wird SFTP verwendet.

   Das Tool zeigt den Inhalt des Verzeichnisses /support an und ermöglicht die Anzeige aller vorhandenen Support-Bundles.

4. Auswahl des Zielverzeichnisses für das Support Bundle, das kopiert werden soll.
5. Sie wählen das Support Bundle aus, das kopiert werden soll, und verwenden das Tool zum Kopieren der Datei vom Unified Manager Server auf Ihr lokales System.

Abrufen des Support-Bundles mithilfe eines UNIX- oder Linux-Clients in Active IQ Unified Manager

Wenn Sie UNIX- oder Linux-Benutzer sind, können Sie das Support-Bundle von Ihrer vApp über die Befehlszeilenschnittstelle (CLI) auf Ihrem Linux-Client-Server abrufen. Zum Abrufen des Support-Bundles können entweder SCP oder SFTP verwendet werden.

Bevor Sie beginnen

Sie müssen der Wartungsbenutzer sein, um diese Aufgabe ausführen zu können.

Sie müssen mithilfe der Managementplattform ein Support Bundle erstellt haben und der Name des Support Bundle muss verfügbar sein.

Schritte

1. Der Zugriff auf die CLI erfolgt über Telnet oder die Managementplattform mithilfe Ihres Linux Client-Servers.
2. Zugriff auf das `/support` Verzeichnis.
3. Der Abruf des Support-Bundles und das Kopieren in das lokale Verzeichnis erfolgen mit folgendem Befehl:

Wenn Sie … verwenden	Anschließend ist der folgende Befehl zu verwenden…
SCP	`scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`
SFTP	`sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`

   Der Name des Support-Bundles wird Ihnen bei der Generierung über die Managementplattform bereitgestellt.

4. Die Eingabe des Passworts für den Wartungsbenutzer ist erforderlich.

Beispiele

Das folgende Beispiel verwendet SCP, um das Support-Bundle abzurufen:

```
        `$ 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
```

Im folgenden Beispiel wird SFTP verwendet, um das Support Bundle abzurufen:

```
        `$ 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
```

Ein Supportpaket kann aus Active IQ Unified Manager an den technischen Support gesendet werden

Wenn ein Problem detailliertere Diagnose- und Fehlerbehebungsinformationen erfordert, als eine AutoSupport Nachricht liefern kann, können Sie ein Supportpaket an den technischen Support senden.

Bevor Sie beginnen

Sie benötigen Zugriff auf das Support-Bundle, um es an den technischen Support senden zu können.

Sie benötigen eine Fallnummer, die über die Website des technischen Supports erstellt wurde.

Schritte

1. Anmeldung bei der NetApp Support Site.
2. Hochladen der Datei.

   "Hochladen einer Datei auf NetApp"

Aufgaben und Informationen im Zusammenhang mit verschiedenen Arbeitsabläufen

Informationen zu Konflikten zwischen Clusterkomponenten in Active IQ Unified Manager

Cluster-Performance-Probleme lassen sich erkennen, wenn eine Clusterkomponente in einen Ressourcenkonflikt gerät. Die Performance der Workloads, die die Komponente nutzen, nimmt ab, und ihre Antwortzeit (Latenz) für Clientanfragen steigt, was ein Ereignis in Unified Manager auslöst.

Eine Komponente, die um Ressourcen konkurriert, kann nicht auf einem optimalen Level arbeiten. Ihre Performance hat abgenommen, und die Performance anderer Clusterkomponenten und Workloads, die als *victims* bezeichnet werden, kann eine erhöhte Latenz aufweisen. Eine Komponente lässt sich aus der Ressourcenkonkurrenz herausbringen, indem ihre Workload reduziert oder ihre Fähigkeit erhöht wird, mehr

Arbeit zu bewältigen, sodass die Performance wieder normale Werte erreicht. Da Unified Manager die Workload-Performance in Fünf-Minuten-Intervallen erfasst und analysiert, erkennt Unified Manager nur, wenn eine Clusterkomponente dauerhaft überbeansprucht wird. Vorübergehende Spitzen der Überbeanspruchung, die innerhalb des Fünf-Minuten-Intervalls nur kurz andauern, werden nicht erkannt.

Ein Storage-Aggregat kann beispielsweise überlastet sein, weil ein oder mehrere Workloads darauf um die Erfüllung ihrer E/A-Anforderungen konkurrieren. Andere Workloads auf dem Aggregat können dadurch beeinträchtigt werden, was zu einer geringeren Performance führt. Um den Aktivitätsgrad auf dem Aggregat zu verringern, stehen verschiedene Maßnahmen zur Verfügung, z. B. das Verschieben eines oder mehrerer Workloads auf ein weniger stark ausgelastetes Aggregat oder einen weniger stark ausgelasteten Knoten, um die Gesamtlast auf dem aktuellen Aggregat zu senken. Bei einer QoS-Richtliniengruppe kann die Durchsatzbegrenzung angepasst werden, oder Workloads können in eine andere Richtliniengruppe verschoben werden, sodass die Workloads nicht mehr gedrosselt werden.

Unified Manager überwacht die folgenden Clusterkomponenten und benachrichtigt Sie, wenn diese in Konflikt geraten:

- **Netzwerk**

  Stellt die Wartezeit von E/A-Anfragen durch die externen Netzwerkprotokolle im Cluster dar. Die Wartezeit entspricht der Zeit, die vergeht, bis „`transfer ready`"-Transaktionen abgeschlossen sind, bevor der Cluster auf eine E/A-Anfrage reagieren kann. Bei einer Überlastung der Netzwerkkomponente bedeutet dies, dass eine hohe Wartezeit auf der Protokollschicht die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **Netzwerkverarbeitung**

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen der Protokollschicht und dem Cluster beteiligt ist. Der Knoten, der die Netzwerkverarbeitung übernimmt, kann sich seit der Erkennung des Ereignisses geändert haben. Wenn die Netzwerkverarbeitungskomponente um Ressourcen konkurriert, bedeutet dies, dass eine hohe Auslastung des Netzwerkverarbeitungsknotens die Latenz eines oder mehrerer Workloads beeinträchtigt.

  Bei Verwendung eines All SAN Array Cluster in einer Aktiv/Aktiv-Konfiguration wird der Wert der Netzwerkverarbeitungslatenz für beide Knoten angezeigt, sodass Sie überprüfen können, ob die Knoten die Last gleichmäßig teilen.

- **Maximaler QoS-Grenzwert**

  Stellt die maximale Durchsatzeinstellung (Spitzenwert) der dem Storage Workload zugewiesenen QoS-Richtliniengruppe (Quality of Service) dar. Wenn die Richtliniengruppenkomponente um Ressourcen konkurriert, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch die festgelegte Durchsatzbegrenzung gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- **Mindest-QoS-Grenzwert**

  Stellt die Latenz einer Arbeitslast dar, die durch die für andere Arbeitslasten zugewiesene minimale QoS-Durchsatzeinstellung (erwartet) verursacht wird. Wenn die für bestimmte Arbeitslasten festgelegte minimale QoS-Vorgabe den Großteil der Bandbreite nutzt, um den zugesicherten Durchsatz zu gewährleisten, werden andere Arbeitslasten gedrosselt und weisen eine höhere Latenz auf.

- **Cluster-Verbindung**

  Stellt die Kabel und Adapter dar, mit denen Cluster-Knoten physisch verbunden sind. Wenn die Cluster-

Interconnect-Komponente ausgelastet ist, bedeutet dies, dass hohe Wartezeiten für E/A-Anforderungen am Cluster-Interconnect die Latenz eines oder mehrerer Workloads beeinträchtigen.

- **Data Processing**

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen dem Cluster und dem Storage-Aggregat beteiligt ist, das die Workload enthält. Der Knoten, der die Data Processing verarbeitet, hat sich seit der Erkennung des Ereignisses möglicherweise geändert. Wenn die Data Processing Komponente einen Ressourcenkonflikt aufweist, bedeutet dies, dass eine hohe Auslastung des Data Processing Knotens die Latenz einer oder mehrerer Workloads beeinträchtigt.

- **Volume Aktivierung**

  Stellt den Prozess dar, der die Nutzung aller aktiven Volumes verfolgt. In großen Umgebungen, in denen mehr als 1000 Volumes aktiv sind, verfolgt dieser Prozess, wie viele kritische Volumes gleichzeitig über den Knoten auf Ressourcen zugreifen müssen. Wenn die Anzahl gleichzeitig aktiver Volumes den empfohlenen maximalen Schwellenwert überschreitet, tritt bei einigen der nicht kritischen Volumes die hier angegebene Latenz auf.

- **MetroCluster Ressourcen**

  Stellt die MetroCluster Ressourcen dar, einschließlich NVRAM und Interswitch Links (ISLs), die zum Spiegeln von Daten zwischen Clustern in einer MetroCluster Konfiguration verwendet werden. Wenn bei der MetroCluster Komponente eine Ressourcenkonkurrenz besteht, bedeutet dies, dass ein hoher Schreibdurchsatz von Workloads im lokalen Cluster oder ein Problem mit dem Zustand einer Verbindung die Latenz eines oder mehrerer Workloads im lokalen Cluster beeinträchtigt. Wenn sich der Cluster nicht in einer MetroCluster Konfiguration befindet, erscheint dieses Symbol nicht.

- **Aggregat- oder SSD-Aggregat-Operationen**

  Stellt das Storage-Aggregat dar, auf dem die Workloads ausgeführt werden. Wenn die Aggregatkomponente in Konkurrenz steht, bedeutet dies, dass eine hohe Auslastung des Aggregats die Latenz eines oder mehrerer Workloads beeinträchtigt. Ein Aggregat besteht entweder ausschließlich aus HDDs, aus einer Mischung aus HDDs und SSDs (ein Flash Pool Aggregat) oder aus einer Mischung aus HDDs und einer Cloud-Tier-Ebene (ein FabricPool Aggregat). Ein „SSD Aggregate“ besteht ausschließlich aus SSDs (ein All-Flash-Aggregat) oder aus einer Mischung aus SSDs und einer Cloud-Tier-Ebene (ein FabricPool Aggregat).

- **Cloud-Latenz**

  Stellt die Softwarekomponente im Cluster dar, die für die E/A-Verarbeitung zwischen dem Cluster und dem Cloud-Tier zuständig ist, auf dem Benutzerdaten gespeichert werden. Wenn die Cloud-Latenzkomponente ausgelastet ist, bedeutet dies, dass eine große Anzahl von Lesezugriffen auf Volumes, die auf dem Cloud-Tier gehostet werden, die Latenz eines oder mehrerer Workloads beeinträchtigt.

- **Synchrones SnapMirror**

  Stellt die Softwarekomponente im Cluster dar, die an der Replikation von Benutzerdaten vom primären Volume zum sekundären Volume in einer synchronen SnapMirror Beziehung beteiligt ist. Wenn die synchrone SnapMirror Komponente um Ressourcen konkurriert, bedeutet dies, dass die Aktivität synchroner SnapMirror Operationen die Latenz eines oder mehrerer Workloads beeinträchtigt.

Die Seite mit den Volume / Health-Details in Active IQ Unified Manager

Auf der Seite „Volume/Systemstatus-Details“ lassen sich detaillierte Informationen zu

einem ausgewählten Volume anzeigen, z. B. Kapazität, Storage Effizienz, Konfiguration, Schutz, Annotationen und generierte Ereignisse. Außerdem lassen sich Informationen zu den zugehörigen Objekten und zugehörigen Warnungen für dieses Volume anzeigen.

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Befehlsschaltflächen

Mit den Befehlsschaltflächen lassen sich die folgenden Aufgaben für das ausgewählte Volume ausführen:

- **Zur Performance Ansicht wechseln**

  Ermöglicht die Navigation zur Seite mit den Volume-/Performancedetails.

- **Aktionen**
  - Benachrichtigung hinzufügen

    Ermöglicht das Hinzufügen einer Warnmeldung zum ausgewählten Volume.

  - Bearbeiten von Schwellenwerten

    Ermöglicht die Änderung der Schwellenwerteinstellungen für das ausgewählte Volume.

  - Annotieren

    Ermöglicht das Annotieren des ausgewählten Volumes.

  - Schützen

    Zum Erstellen von Beziehungen des Typs SnapMirror oder SnapVault für das ausgewählte Volume.

  - Beziehung

    Sie können damit die folgenden Schutzbeziehungsvorgänge ausführen:

    - Bearbeiten

      Öffnet das Dialogfeld „Beziehung bearbeiten“, mit dem Sie bestehende SnapMirror Richtlinien, Zeitpläne und maximale Übertragungsraten für eine bestehende Schutzbeziehung ändern können.

    - Abbrechen

      Bricht laufende Übertragungen für eine ausgewählte Beziehung ab. Optional ist das Entfernen des Neustart-Checkpoints für andere Übertragungen als den Basistransfer möglich. Der Checkpoint für einen Basistransfer kann nicht entfernt werden.

    - Anhalten

      Vorübergehende Deaktivierung geplanter Aktualisierungen für eine ausgewählte Beziehung. Bereits laufende Übertragungen müssen abgeschlossen sein, bevor die Beziehung in den Ruhezustand versetzt wird.

    - Unterbrechen

Unterbricht die Beziehung zwischen Quell- und Ziel-Volumes und ändert das Ziel-Volume in ein Lese-/Schreib-Volume.

- Entfernen

  Die Beziehung zwischen der ausgewählten Quelle und dem Ziel wird dauerhaft gelöscht. Die Volumes werden nicht zerstört, und die Snapshot Kopien auf den Volumes werden nicht entfernt. Dieser Vorgang kann nicht rückgängig gemacht werden.

- Fortsetzen

  Ermöglicht geplante Übertragungen für eine angehaltene Beziehung. Beim nächsten geplanten Übertragungsintervall wird ein Neustart-Checkpoint verwendet, sofern ein solcher vorhanden ist.

- Resynchronisieren

  Ermöglicht die Neusynchronisierung einer zuvor unterbrochenen Beziehung.

- Initialisieren/Aktualisieren

  Ermöglicht Ihnen, einen erstmaligen Basistransfer für eine neue Schutzbeziehung durchzuführen oder eine manuelle Aktualisierung vorzunehmen, wenn die Beziehung bereits initialisiert ist.

- Reverse Resync

  Ermöglicht die Wiederherstellung einer zuvor unterbrochenen Schutzbeziehung, wobei die Funktionen von Quelle und Ziel umgekehrt werden, indem die Quelle als Kopie des ursprünglichen Ziels festgelegt wird. Der Inhalt der Quelle wird durch den Inhalt des Ziels überschrieben, und alle Daten, die neuer sind als die Daten in der gemeinsamen Snapshot Kopie, werden gelöscht.

◦ Wiederherstellen

Ermöglicht die Wiederherstellung von Daten von einem Volume auf ein anderes Volume. Informationen hierzu enthält "Wiederherstellen von Daten mithilfe der Seite „Volume / Systemstatus-Details“".

> Die Schaltfläche „Wiederherstellen“ und die Schaltflächen für Beziehungsvorgänge sind für Volumes, die sich in synchronen Schutzbeziehungen befinden, nicht verfügbar.

- **Volumes anzeigen**

  Öffnet die Ansicht „Systemstatus: Alle Volumes“.

Registerkarte Kapazität

Die Registerkarte „Kapazität“ zeigt Details zum ausgewählten Volume an, wie z. B. dessen physische Kapazität, logische Kapazität, Schwellenwerteinstellungen, Kontingentkapazität und Informationen über etwaige Verschiebevorgänge von Volumes:

- **Physische Kapazität**

  Details zur physischen Kapazität des Volumens:

  ◦ Snapshot-Überlauf

  Zeigt den von den Snapshot Kopien belegten Speicherplatz an.

- Gebraucht

  Zeigt den von den Daten im Volume belegten Speicherplatz an.

- Warnung

  Zeigt an, dass der Speicherplatz im Volume nahezu voll ist. Wenn dieser Schwellenwert überschritten wird, wird das Ereignis „Speicherplatz nahezu voll“ generiert.

- Fehler

  Zeigt an, dass der Speicherplatz im Volume voll ist. Bei Überschreitung dieses Schwellenwerts wird das Ereignis „Speicherplatz voll“ ausgelöst.

- Unbrauchbar

  Zeigt an, dass das Ereignis „Thin-Provisioned Volume Space At Risk“ generiert wird und dass der Speicherplatz im Thin-Provisioned-Volume aufgrund von Kapazitätsproblemen gefährdet ist. Die nicht nutzbare Kapazität wird nur für Thin-Provisioned-Volumes angezeigt.

- Datendiagramm

  Zeigt die gesamte Datenkapazität und die belegte Datenkapazität des Volume an.

  Wenn die automatische Vergrößerung aktiviert ist, zeigt das Datendiagramm auch den im Aggregat verfügbaren Speicherplatz an. Das Datendiagramm zeigt den effektiven Storage, der von den Daten im Volume genutzt werden kann. Dieser kann einer der folgenden Werte sein:

  - Tatsächliche Datenkapazität des Volumes unter folgenden Bedingungen:
    - Die automatische Vergrößerung ist deaktiviert.
    - Das für Autogrow aktivierte Volume hat die maximale Größe erreicht.
    - Ein mit Autogrow aktiviertes Thick Provisioning-Volume kann nicht weiter wachsen.
  - Datenkapazität des Volumes unter Berücksichtigung der maximalen Größe des Volumes (für Thin-Provisioned-Volumes und für Thick-Provisioned-Volumes, wenn das Aggregat über genügend Speicherplatz verfügt, damit das Volume seine maximale Größe erreichen kann)
  - Datenkapazität des Volumes unter Berücksichtigung der nächstmöglichen autogrow Größe (für thick provisionierte Volumes mit einem autogrow Prozentsatzschwellenwert)

- Grafik der Snapshot Kopien

  Dieses Diagramm wird nur angezeigt, wenn die genutzte Snapshot-Kapazität oder die Snapshot-Reserve nicht null ist.

Beide Diagramme zeigen die Kapazität, um die die Snapshot Kapazität die Snapshot Reserve überschreitet, wenn die verwendete Snapshot Kapazität die Snapshot Reserve überschreitet.

- **Logische Kapazität**

  Zeigt die Eigenschaften des logischen Speicherplatzes des Volume an. Der logische Speicherplatz gibt die tatsächliche Größe der auf der Festplatte gespeicherten Daten an, ohne die Einsparungen durch ONTAP Storage Effizienztechnologien zu berücksichtigen.

  - Berichterstellung zum logischen Speicherplatz

Zeigt an, ob für das Volume die logische Speicherplatzberichterstattung konfiguriert ist. Der Wert kann „Aktiviert“, „Deaktiviert“ oder „Nicht zutreffend“ sein. „Nicht zutreffend“ wird für Volumes auf älteren Versionen von ONTAP oder für Volumes angezeigt, die die logische Speicherplatzberichterstattung nicht unterstützen.

- Gebraucht

  Zeigt den von den Daten im Volume belegten logischen Speicherplatz sowie den prozentualen Anteil des belegten logischen Speicherplatzes an der gesamten Datenkapazität an.

- Durchsetzung des logischen Speicherplatzes

  Zeigt an, ob die logische Speicherplatzdurchsetzung für dünn bereitgestellte Volumes konfiguriert ist. Wenn die Einstellung auf Aktiviert gesetzt ist, darf die logisch genutzte Größe des Volumes nicht größer sein als die aktuell festgelegte physische Volume-Größe.

- **Automatische Vergrößerung**

  Zeigt an, ob das Volume automatisch wächst, wenn kein Speicherplatz mehr verfügbar ist.

- **Speicherplatzzusage**

  Zeigt das Steuerelement für die Einstellungen des FlexVol volume an, wenn ein Volume freie Blöcke aus einem Aggregat entfernt. Diese Blöcke stehen dann garantiert für Schreibvorgänge in Dateien auf dem Volume zur Verfügung. Die Speicherplatzzusage kann auf einen der folgenden Werte eingestellt werden:

  - Keine

    Für das Volume ist keine Speicherplatzzusage konfiguriert.

  - Datei

    Die volle Größe von Sparse-Dateien (zum Beispiel LUNs) ist gewährleistet.

  - Volumen

    Die volle Volumengröße ist garantiert.

  - Teilweise

    Das FlexCache volume reserviert Speicherplatz entsprechend seiner Größe. Wenn die Größe des FlexCache volume 100 MB oder mehr beträgt, ist die minimale Speicherplatzzusage standardmäßig auf 100 MB festgelegt. Wenn die Größe des FlexCache volume weniger als 100 MB beträgt, ist die minimale Speicherplatzzusage auf die Größe des FlexCache volume festgelegt. Wenn die Größe des FlexCache volume später erhöht wird, wird die minimale Speicherplatzzusage nicht erhöht.

  Die Speicherplatzzusage ist Partial, wenn das Volume vom Typ Data-Cache ist.

- **Details (Physische Merkmale)**

  Zeigt die physikalischen Eigenschaften des Volumens an.

- **Gesamtkapazität**

  Zeigt die gesamte physische Kapazität im Volume an.

- **Datenkapazität**

  Zeigt den vom Volumen belegten physischen Raum (genutzte Kapazität) und den noch verfügbaren physischen Raum (freie Kapazität) im Volumen an. Diese Werte werden auch als Prozentsatz der gesamten physischen Kapazität angezeigt.

  Wenn das Ereignis „Thin-Provisioned Volume Space At Risk“ für Thin Provisioning Volumes generiert wird, werden die vom Volume belegte Speichermenge (belegte Kapazität) und die Speichermenge, die im Volume verfügbar ist, aber aufgrund von Kapazitätsproblemen des Aggregats nicht genutzt werden kann (nicht nutzbare Kapazität), angezeigt.

- **Snapshot-Reserve**

  Zeigt den von den Snapshot-Kopien belegten Speicherplatz (belegte Kapazität) und den für Snapshot-Kopien verfügbaren Speicherplatz (freie Kapazität) im Volume an. Diese Werte werden auch als Prozentsatz der gesamten Snapshot-Reserve angezeigt.

  Wenn das Ereignis „Thin-Provisioned Volume Space At Risk“ für Thin Provisioned Volumes generiert wird, werden die von den Snapshot Kopien verwendete Speichermenge (verwendete Kapazität) und die im Volume verfügbare, aufgrund von Aggregatkapazitätsproblemen jedoch nicht für die Erstellung von Snapshot Kopien nutzbare Speichermenge (nicht nutzbare Kapazität) angezeigt.

- **Volume-Schwellenwerte**

  Anzeige der folgenden Volumenkapazitätsschwellenwerte:

  - Schwellenwert für nahezu voll

    Gibt den Prozentsatz an, bei dem ein Volume nahezu voll ist.

  - Schwellenwert für voll

    Gibt den Prozentsatz an, bei dem ein Volume voll ist.

- **Weitere Details**

  - Maximale Größe für automatisches Wachstum

    Zeigt die maximale Größe an, bis zu der das Volume automatisch wachsen kann. Der Standardwert beträgt 120 % der Volume-Größe bei der Erstellung. Dieses Feld wird nur angezeigt, wenn Autogrow für das Volume aktiviert ist.

  - Zugesicherte Kapazität des Qtree Kontingents

    Zeigt den in den Kontingenten reservierten Speicherplatz an.

  - Qtree Kontingent mit überbuchter Kapazität

    Zeigt die Menge an Speicherplatz an, die genutzt werden kann, bevor das System das Ereignis „Volume Qtree Quota Overcommitted“ generiert.

  - Teilreserve

    Steuert die Größe der Überschreibungsreserve. Standardmäßig ist die anteilige Reserve auf 100 % eingestellt, was bedeutet, dass 100 % des erforderlichen reservierten Speicherplatzes reserviert sind, sodass die Objekte vollständig vor Überschreibungen geschützt sind. Wenn die anteilige Reserve

weniger als 100 % beträgt, wird der reservierte Speicherplatz für alle Dateien mit reserviertem Speicherplatz in diesem Volume auf den Prozentsatz der anteiligen Reserve reduziert.

- Tägliche Snapshot-Wachstumsrate

  Zeigt die Änderung (in Prozent oder in KB, MB, GB usw.) an, die alle 24 Stunden in den Snapshot Kopien im ausgewählten Volume auftritt.

- Snapshot Tage bis voll

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor der für die Snapshot-Kopien im Volume reservierte Speicherplatz den angegebenen Schwellenwert erreicht.

  Das Feld „Snapshot Days to Full“ zeigt den Wert „Nicht zutreffend“ an, wenn die Wachstumsrate der Snapshot Kopien im Volume null oder negativ ist oder wenn nicht genügend Daten zur Berechnung der Wachstumsrate vorliegen.

- Snapshot Autodelete

  Legt fest, ob Snapshot Kopien automatisch gelöscht werden, um Speicherplatz freizugeben, wenn ein Schreibvorgang auf ein Volume aufgrund von Speicherplatzmangel im Aggregat fehlschlägt.

- Snapshot Kopien

  Zeigt Informationen über die Snapshot-Kopien im Volume an.

  Die Anzahl der Snapshot-Kopien im Volume wird als Link angezeigt. Ein Klick auf den Link öffnet das Dialogfeld „Snapshot Copies on a Volume“, in dem Details zu den Snapshot-Kopien angezeigt werden.

Die Anzahl der Snapshot-Kopien wird ungefähr stündlich aktualisiert; die Liste der Snapshot-Kopien wird jedoch zu dem Zeitpunkt aktualisiert, zu dem Sie auf das Symbol klicken. Dies kann zu einer Abweichung zwischen der in der Topologie angezeigten Anzahl der Snapshot-Kopien und der Anzahl der Snapshot-Kopien führen, die aufgeführt werden, wenn Sie auf das Symbol klicken.

- **Volume Move**

  Zeigt den Status der aktuellen oder der letzten Volume-Verschiebungsoperation an, die auf dem Volume durchgeführt wurde, sowie weitere Details wie die aktuelle Phase der laufenden Volume-Verschiebungsoperation, Quellaggregat, Zielaggregat, Startzeit, Endzeit und geschätzte Endzeit.

  Außerdem wird die Anzahl der auf dem ausgewählten Volume durchgeführten Volume-Verschiebungsvorgänge angezeigt. Weitere Informationen zu den Volume-Verschiebungsvorgängen sind über den Link **Volume Move History** verfügbar.

Registerkarte „Konfiguration“

Die Registerkarte „Konfiguration“ zeigt Details zum ausgewählten Volume an, wie z. B. die Exportrichtlinie, den RAID-Typ, die Kapazität und die mit der Storage-Effizienz verbundenen Funktionen des Volumes:

- **Überblick**

  - Vollständiger Name

    Zeigt den vollständigen Namen des Volume an.

- Aggregate

  Zeigt den Namen des Aggregats an, auf dem sich das Volume befindet, oder die Anzahl der Aggregate, auf denen sich das FlexGroup Volume befindet.

- Tiering-Richtlinie

  Zeigt die für das Volume festgelegte Tiering-Richtlinie an, sofern das Volume auf einem FabricPool-aktivierten Aggregat bereitgestellt ist. Die Richtlinie kann None, Snapshot Only, Backup, Auto oder All sein.

- Speicher-VM

  Zeigt den Namen der SVM an, die das Volume enthält.

- Junction-Pfad

  Zeigt den Status des Pfades an, der aktiv oder inaktiv sein kann. Der Pfad in der SVM, in den das Volume eingebunden ist, wird ebenfalls angezeigt. Über den Link **History** lassen sich die fünf letzten Änderungen am Verbindungspfad anzeigen.

- Exportrichtlinie

  Zeigt den Namen der Exportrichtlinie an, die für das Volume erstellt wird. Über den Link lassen sich Details zu den Exportrichtlinien, Authentifizierungsprotokollen und den auf den Volumes aktivierten Zugriffsrechten anzeigen, die zur SVM gehören.

- Stil

  Zeigt den Volume-Stil an. Der Volume-Stil kann FlexVol oder FlexGroup sein.

- Typ

  Zeigt den Typ des ausgewählten Volumes an. Der Volume-Typ kann Read-write, Load-sharing, Data-Protection, Data-cache oder Temporary sein.

- RAID-Typ

  Zeigt den RAID-Typ des ausgewählten Volumes an. Mögliche RAID-Typen sind RAID0, RAID4, RAID-DP oder RAID-TEC.

  > Für FlexGroup Volumes können mehrere RAID-Typen angezeigt werden, da die einzelnen Volumes für FlexGroups auf Aggregaten unterschiedlicher Typen liegen können.

- SnapLock Typ

  Zeigt den SnapLock Typ des Aggregats an, das das Volume enthält.

- SnapLock Ablauf

  Zeigt das Ablaufdatum des SnapLock Volumens an.

- **Kapazität**
  - Thin Provisioning

Zeigt an, ob Thin Provisionierung für das Volume konfiguriert ist.

- Automatisches Wachstum

  Zeigt an, ob das flexible Volume innerhalb eines Aggregats automatisch wächst.

- Snapshot Autodelete

  Legt fest, ob Snapshot Kopien automatisch gelöscht werden, um Speicherplatz freizugeben, wenn ein Schreibvorgang auf ein Volume aufgrund von Speicherplatzmangel im Aggregat fehlschlägt.

- Kontingente

  Gibt an, ob die Quoten für das Volume aktiviert sind.

- **Effizienz**
  - Komprimierung

    Gibt an, ob die Komprimierung aktiviert oder deaktiviert ist.

  - Deduplizierung

    Gibt an, ob die Deduplizierung aktiviert oder deaktiviert ist.

  - Deduplizierungsmodus

    Legt fest, ob der für ein Volume aktivierte Deduplizierungsvorgang manuell, geplant oder richtlinienbasiert ist. Wenn der Modus auf „Geplant“ gesetzt ist, wird der Zeitplan angezeigt, und wenn der Modus auf eine Richtlinie gesetzt ist, wird der Name der Richtlinie angezeigt.

  - Deduplizierungstyp

    Gibt den Typ der Deduplizierungsoperation an, die auf dem Volume ausgeführt wird. Wenn sich das Volume in einer SnapVault Beziehung befindet, wird als Typ SnapVault angezeigt. Bei allen anderen Volumes wird der Typ als Regular angezeigt.

  - Richtlinie zur Storage-Effizienz

    Gibt den Namen der Storage Effizienzrichtlinie an, die diesem Volume über Unified Manager zugewiesen wurde. Diese Richtlinie kann die Komprimierungs- und Deduplizierungseinstellungen steuern.

- **Schutz**
  - Snapshot Kopien

    Legt fest, ob automatische Snapshot-Kopien aktiviert oder deaktiviert sind.

Registerkarte Schutz

Die Registerkarte „Schutz“ zeigt Schutzdetails zum ausgewählten Volume an, wie z. B. Verzögerungsinformationen, Beziehungstyp und Topologie der Beziehung.

- **Zusammenfassung**

  Zeigt die Eigenschaften von Schutzbeziehungen (SnapMirror, SnapVault oder Storage VM DR) für ein

ausgewähltes Volume an. Für jeden anderen Beziehungstyp wird nur die Eigenschaft „Beziehungstyp“ angezeigt. Wenn ein primäres Volume ausgewählt ist, werden nur die Managed- und Local-Snapshot-Kopierrichtlinien angezeigt. Die für SnapMirror- und SnapVault-Beziehungen angezeigten Eigenschaften umfassen Folgendes:

- Quellvolumen

  Zeigt den Namen des Quellvolumes des ausgewählten Volumes an, falls es sich bei dem ausgewählten Volume um ein Zielvolume handelt.

- Lag-Status

  Zeigt den Aktualisierungs- oder Übertragungsverzögerungsstatus für eine Schutzbeziehung an. Der Status kann „Fehler“, „Warnung“ oder „Kritisch“ lauten.

  Der Verzögerungsstatus ist für synchrone Beziehungen nicht anwendbar.

- Verzögerungsdauer

  Zeigt die Zeit an, um die die Daten auf dem Spiegel gegenüber der Quelle hinterherhinken.

- Letzte erfolgreiche Aktualisierung

  Zeigt Datum und Uhrzeit des letzten erfolgreichen Schutzupdates an.

  Das letzte erfolgreiche Update ist für synchrone Beziehungen nicht anwendbar.

- Mitglied des Storage Service

  Zeigt entweder Ja oder Nein an, um anzugeben, ob das Volume zu einem Storage Service gehört und von diesem verwaltet wird.

- Versionsflexible Replikation

  Es wird entweder „Ja“, „Ja mit Backup-Option“ oder „Keine“ angezeigt. „Ja“ bedeutet, dass die SnapMirror Replikation auch dann möglich ist, wenn auf Quell- und Ziel-Volumes unterschiedliche Versionen der ONTAP Software ausgeführt werden. „Ja mit Backup-Option“ bedeutet die Implementierung des SnapMirror Schutzes mit der Möglichkeit, mehrere Versionen von Backup-Kopien auf dem Ziel zu behalten. „Keine“ bedeutet, dass die versionsflexible Replikation nicht aktiviert ist.

- Beziehungsfunktion

  Zeigt die für die Schutzbeziehung verfügbaren ONTAP-Funktionen an.

- Schutzdienst

  Zeigt den Namen des Schutzdienstes an, wenn die Beziehung von einer Schutzpartner-Applikation verwaltet wird.

- Beziehungstyp

  Zeigt alle Beziehungstypen an, einschließlich Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync und Sync.

- Beziehungsstatus

Zeigt den Status der SnapMirror oder SnapVault Beziehung an. Der Status kann Uninitialized, SnapMirrored oder Broken-Off sein. Wenn ein Quellvolume ausgewählt ist, ist der Beziehungsstatus nicht anwendbar und wird nicht angezeigt.

- Übertragungsstatus

  Zeigt den Übertragungsstatus für die Schutzbeziehung an. Der Übertragungsstatus kann einer der folgenden sein:

  - Abbruch

    SnapMirror Übertragungen sind aktiviert; es wird jedoch derzeit ein Vorgang zum Abbruch einer Übertragung ausgeführt, der möglicherweise die Entfernung des Checkpoints umfasst.

  - Überprüfung

    Das Ziel-Volume wird derzeit diagnostisch überprüft, und es findet kein Datentransfer statt.

  - Finalisierung

    SnapMirror Übertragungen sind aktiviert. Das Volume befindet sich aktuell in der Nachübertragungsphase für inkrementelle SnapVault Übertragungen.

  - Leerlauf

    Transfers sind aktiviert, und es wird kein Transfer ausgeführt.

  - In-Sync

    Die Daten in den beiden Volumes in der synchronen Beziehung sind synchronisiert.

  - Nicht synchronisiert

    Die Daten im Ziel-Volume sind nicht mit dem Quell-Volume synchronisiert.

  - Vorbereitung

    SnapMirror Übertragungen sind aktiviert. Das Volume befindet sich aktuell in der Vorübertragungsphase für inkrementelle SnapVault Übertragungen.

  - In der Warteschlange

    SnapMirror Transfers sind aktiviert. Derzeit sind keine Transfers in Bearbeitung.

  - Ruhend

    SnapMirror Transfers sind deaktiviert. Es ist kein Transfer im Gange.

  - Anhalten

    Eine SnapMirror Übertragung ist im Gange. Zusätzliche Übertragungen sind deaktiviert.

  - Übertragung

    SnapMirror Datentransfers sind aktiviert, und ein Transfer wird ausgeführt.

- Übergang

  Der asynchrone Datentransfer vom Quell- zum Ziel-Volume ist abgeschlossen, und der Übergang zum synchronen Betrieb hat begonnen.

- Warten

  Ein SnapMirror Transfer wurde eingeleitet, aber einige zugehörige Aufgaben warten darauf, in die Warteschlange eingereiht zu werden.

◦ Maximale Transferrate

Zeigt die maximale Transferrate für die Beziehung an. Die maximale Transferrate kann als numerischer Wert in Kilobyte pro Sekunde (Kbps), Megabyte pro Sekunde (Mbps), Gigabit pro Sekunde (Gbit/s) oder Terabyte pro Sekunde (Tbps) angegeben werden. Wird „Kein Limit“ angezeigt, ist der Basistransfer zwischen Beziehungen unbegrenzt.

◦ SnapMirror Richtlinie

Zeigt die Datensicherungsstrategie für das Volume an. DPDefault steht für die standardmäßige asynchrone Spiegelungs-Datensicherungsstrategie, XDPDefault für die standardmäßige asynchrone Vault-Datensicherungsstrategie und DPSyncDefault für die standardmäßige asynchrone MirrorVault Datensicherungsstrategie. StrictSync steht für die standardmäßige synchrone strikte Datensicherungsstrategie, und Sync steht für die standardmäßige synchrone Datensicherungsstrategie. Durch Klicken auf den Namen der Datensicherungsstrategie können die zugehörigen Details angezeigt werden, einschließlich der folgenden Informationen:

- Transferpriorität
- Zugriffszeiteinstellung ignorieren
- Versuchslimit
- Kommentare
- SnapMirror Labels
- Aufbewahrungseinstellungen
- Tatsächliche Snapshot Kopien
- Snapshot Kopien aufbewahren
- Aufbewahrungswarnschwelle
- Snapshot-Kopien ohne Aufbewahrungseinstellungen In einer kaskadierenden SnapVault Beziehung, in der die Quelle ein Data Protection (DP)-Volume ist, gilt nur die Regel “sm_created”.

◦ Aktualisierungsplan

Zeigt den der Beziehung zugeordneten SnapMirror Zeitplan an. Beim Positionieren des Mauszeigers über dem Informationssymbol werden die Zeitplandetails angezeigt.

◦ Lokale Snapshot Richtlinie

Zeigt die Snapshot-Kopierrichtlinie für das Volume an. Die Richtlinie ist Default, None oder ein beliebiger Name für eine benutzerdefinierte Richtlinie.

◦ Geschützt durch

Zeigt den Typ des Schutzes an, der für das ausgewählte Volume verwendet wird. Wenn ein Volume

beispielsweise durch eine Konsistenzgruppe und SnapMirror Volume-Beziehungen geschützt ist, zeigt dieses Feld sowohl SnapMirror als auch die Konsistenzgruppe an. Dieses Feld enthält außerdem einen Link zur Seite „Beziehungen“, auf der der einheitliche Beziehungsstatus angezeigt wird. Der Link gilt nur für konstituierende Beziehungen.

- Konsistenzgruppe

  Bei Volumes, die durch SnapMirror active sync Beziehungen geschützt sind, zeigt diese Spalte die Konsistenzgruppe des Volumes an.

- **Ansichten**

  Zeigt die Schutztopologie des ausgewählten Volumes an. Die Topologie umfasst grafische Darstellungen aller Volumes, die mit dem ausgewählten Volume in Beziehung stehen. Das ausgewählte Volume ist durch einen dunkelgrauen Rahmen gekennzeichnet, und Linien zwischen den Volumes in der Topologie geben den Typ der Datensicherungsbeziehung an. Die Richtung der Beziehungen in der Topologie wird von links nach rechts angezeigt, wobei sich die Quelle jeder Beziehung links und das Ziel rechts befindet.

  Doppelte fette Linien kennzeichnen eine asynchrone Spiegelungsbeziehung, eine einzelne fette Linie kennzeichnet eine asynchrone Vault-Beziehung, zwei einfache Linien kennzeichnen eine asynchrone MirrorVault Beziehung, und eine fette sowie eine nicht fette Linie kennzeichnen eine synchrone Beziehung. Die folgende Tabelle zeigt an, ob die synchrone Beziehung StrictSync oder Sync ist.

  Ein Rechtsklick auf ein Volume öffnet ein Menü, in dem Sie das Volume schützen oder die Daten darauf wiederherstellen können. Ein Rechtsklick auf eine Beziehung öffnet ein Menü, in dem Sie die Beziehung bearbeiten, abbrechen, stilllegen, trennen, entfernen oder fortsetzen können.

  Die Menüs werden in den folgenden Fällen nicht angezeigt:

  - Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, beispielsweise wenn Sie nur über Bedienerrechte verfügen
  - Wenn sich das Volume in einer synchronen Schutzbeziehung befindet
  - Wenn die Volume-ID unbekannt ist, beispielsweise bei einer Cluster-übergreifenden Beziehung, und der Ziel-Cluster noch nicht erkannt wurde, werden beim Klicken auf ein anderes Volume in der Topologie Informationen zu diesem Volume ausgewählt und angezeigt. Ein Fragezeichen () in der oberen linken Ecke eines Volumes bedeutet, dass das Volume entweder fehlt oder noch nicht erkannt wurde. Es kann auch darauf hinweisen, dass die Kapazitätsinformationen fehlen. Befindet sich der Mauszeiger über dem Fragezeichen, werden zusätzliche Informationen einschließlich Vorschlägen für Abhilfemaßnahmen angezeigt.

  Die Topologie zeigt Informationen über Volume-Kapazität, Verzögerung, Snapshot-Kopien und den letzten erfolgreichen Datentransfer an, sofern sie einer von mehreren gängigen Topologievorlagen entspricht. Wenn eine Topologie keiner dieser Vorlagen entspricht, werden Informationen über die Volume-Verzögerung und den letzten erfolgreichen Datentransfer in einer Beziehungstabelle unterhalb der Topologie angezeigt. In diesem Fall kennzeichnet die hervorgehobene Zeile in der Tabelle das ausgewählte Volume, und in der Topologieansicht zeigen fett dargestellte Linien mit einem blauen Punkt die Beziehung zwischen dem ausgewählten Volume und seinem Quell-Volume an.

Topologieansichten enthalten folgende Informationen:

- Kapazität

  Zeigt die vom Volume belegte Gesamtkapazität an. Wenn Sie den Mauszeiger über ein Volume in der Topologie bewegen, werden im Dialogfeld „Current Threshold Settings“ die aktuellen Warn- und kritischen Schwellenwerteinstellungen für dieses Volume angezeigt. Sie können die Schwellenwerteinstellungen

auch bearbeiten, indem Sie im Dialogfeld „Current Threshold Settings“ auf den Link **Edit Thresholds** klicken. Wenn Sie das Kästchen **Capacity** deaktivieren, werden alle Kapazitätsinformationen für alle Volumes in der Topologie ausgeblendet.

- Verzögerung

  Zeigt die Verzögerungsdauer und den Verzögerungsstatus der eingehenden Schutzbeziehungen an. Durch Deaktivieren des Kästchens **Lag** werden alle Verzögerungsinformationen für alle Volumes in der Topologie ausgeblendet. Wenn das Kästchen **Lag** ausgegraut ist, werden die Verzögerungsinformationen für das ausgewählte Volume sowie die Verzögerungsinformationen für alle zugehörigen Volumes in der Beziehungstabelle unterhalb der Topologie angezeigt.

- Schnappschuss

  Zeigt die Anzahl der für ein Volume verfügbaren Snapshot-Kopien an. Durch Deaktivieren des **Snapshot** -Kästchens werden alle Informationen zu Snapshot-Kopien für alle Volumes in der Topologie ausgeblendet.

  Beim Klicken auf ein Snapshot-Kopiensymbol () wird die Liste der Snapshot-Kopien für ein Volume angezeigt. Die neben dem Symbol angezeigte Anzahl der Snapshot-Kopien wird etwa stündlich aktualisiert; die Liste der Snapshot-Kopien wird jedoch zu dem Zeitpunkt aktualisiert, zu dem auf das Symbol geklickt wird. Dies kann zu einer Abweichung zwischen der in der Topologie angezeigten Anzahl der Snapshot-Kopien und der Anzahl der Snapshot-Kopien in der Liste führen, die beim Klicken auf das Symbol angezeigt wird.

- Letzte erfolgreiche Übertragung

  Zeigt den Betrag, die Dauer, die Uhrzeit und das Datum des letzten erfolgreichen Datentransfers an. Wenn das Kästchen **Last Successful Transfer** abgeblendet ist, werden die Informationen zur letzten erfolgreichen Übertragung für das ausgewählte Volume in der Beziehungstabelle unterhalb der Topologie sowie die Informationen zur letzten erfolgreichen Übertragung für alle zugehörigen Volumes angezeigt.

  - **Geschichte**

    Zeigt in einem Diagramm den Verlauf der eingehenden SnapMirror und SnapVault Datensicherungsbeziehungen für das ausgewählte Volume an. Es stehen drei Verlaufsdiagramme zur Verfügung: Verzögerungsdauer eingehender Beziehungen, Übertragungsdauer eingehender Beziehungen und Übertragungsgröße eingehender Beziehungen. Verlaufsinformationen werden nur angezeigt, wenn Sie ein Zielvolume auswählen. Wenn Sie ein primäres Volume auswählen, sind die Diagramme leer, und die Meldung No data found wird angezeigt. Wenn die Volumes durch Consistency Group und SnapMirror synchron Beziehungen geschützt sind, werden Informationen zur Übertragungsdauer und Übertragungsgröße der Beziehungen nicht angezeigt.

  Sie können oben im Verlaufsbereich in der Dropdown-Liste einen Diagrammtyp auswählen. Außerdem können Sie Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme können Ihnen helfen, Trends zu erkennen: Wenn beispielsweise große Datenmengen zur gleichen Tages- oder Wochenzeit übertragen werden oder der Schwellenwert für Verzögerungswarnungen oder Verzögerungsfehler wiederholt überschritten wird, können Sie entsprechende Maßnahmen ergreifen. Zusätzlich können Sie auf die Schaltfläche **Export** klicken, um für das angezeigte Diagramm einen Bericht im CSV-Format zu erstellen.

Die Diagramme zur Schutzhistorie zeigen folgende Informationen an:

- **Beziehungsverzögerungsdauer**

  Die vertikale (y-)Achse zeigt Sekunden, Minuten oder Stunden an, und die horizontale (x-)Achse zeigt Tage, Monate oder Jahre an, abhängig vom gewählten Zeitraum. Der obere Wert auf der y-Achse gibt die maximale Verzögerungsdauer an, die im auf der x-Achse dargestellten Zeitraum erreicht wurde. Die

horizontale orangefarbene Linie im Diagramm stellt den Schwellenwert für den Verzögerungsfehler dar, und die horizontale gelbe Linie stellt den Schwellenwert für die Verzögerungswarnung dar. Beim Bewegen des Mauszeigers über diese Linien wird die Schwellenwerteinstellung angezeigt. Die horizontale blaue Linie stellt die Verzögerungsdauer dar. Details zu bestimmten Punkten im Diagramm werden beim Bewegen des Mauszeigers über einen interessierenden Bereich angezeigt.

- **Dauer des Beziehungs-Transfers**

  Die vertikale (y-)Achse zeigt Sekunden, Minuten oder Stunden an, die horizontale (x-)Achse Tage, Monate oder Jahre, abhängig vom gewählten Zeitraum. Der obere Wert auf der y-Achse gibt die maximale Übertragungsdauer innerhalb des auf der x-Achse dargestellten Zeitraums an. Details zu einzelnen Punkten im Diagramm können durch Positionieren des Mauszeigers über dem gewünschten Bereich angezeigt werden.

  > Dieses Diagramm ist für Volumes, die sich in synchronen Schutzbeziehungen befinden, nicht verfügbar.

- **Übertragene Größe der Beziehung**

  Die vertikale (y-)Achse zeigt je nach Übertragungsgröße Bytes, Kilobytes, Megabytes usw. an, und die horizontale (x-)Achse zeigt je nach ausgewähltem Zeitraum Tage, Monate oder Jahre an. Der obere Wert auf der y-Achse gibt die maximale Übertragungsgröße an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. Details zu einzelnen Punkten im Diagramm sind verfügbar, wenn Sie den Mauszeiger über einen Bereich von Interesse bewegen.

  > Dieses Diagramm ist für Volumes, die sich in synchronen Schutzbeziehungen befinden, nicht verfügbar.

Verlaufsbereich

Im Bereich „Verlauf“ werden Diagramme angezeigt, die Informationen zur Kapazität und zu den Platzreservierungen des ausgewählten Volumens liefern. Zusätzlich können Sie auf die Schaltfläche **Export** klicken, um einen Bericht im CSV-Format für das angezeigte Diagramm zu erstellen.

Diagramme können leer sein, und die Meldung „Keine Daten gefunden“ kann erscheinen, wenn die Daten oder der Zustand des Volumens über einen bestimmten Zeitraum unverändert bleiben.

Sie können in der Dropdown-Liste oben im Verlaufsbereich einen Diagrammtyp auswählen. Außerdem können Sie Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme können Ihnen helfen, Trends zu erkennen, beispielsweise wenn die Speicherauslastung den Schwellenwert „Nahezu voll“ regelmäßig überschreitet, können Sie geeignete Maßnahmen ergreifen.

Verlaufsdiagramme zeigen folgende Informationen an:

- **Verwendete Volume-Kapazität**

  Zeigt die belegte Kapazität im Volume und den Trend der Nutzung der Volume-Kapazität anhand des Nutzungsverlaufs als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen (y-)Achse an. Der Zeitraum wird auf der horizontalen (x-)Achse dargestellt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende Volume Used Capacity klicken, wird die Diagrammlinie Volume Used

Capacity ausgeblendet.

- **Verwendete Volume Kapazität im Vergleich zur Gesamtkapazität**

  Zeigt den Trend der Speicherauslastung basierend auf dem Nutzungsverlauf sowie die belegte Kapazität, die Gesamtkapazität und die Details der durch Deduplizierung und Komprimierung erzielten Speicherplatzeinsparungen als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen (y-)Achse an. Der Zeitraum wird auf der horizontalen (x-)Achse angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Die Details für bestimmte Punkte im Diagramm können durch Positionieren des Cursors über einem bestimmten Bereich angezeigt werden. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende Trend Capacity Used klicken, wird die Diagrammlinie Trend Capacity Used ausgeblendet.

- **Genutzte Volume-Kapazität (%)**

  Die im Volume verwendete Kapazität sowie der Trend der Volume-Kapazitätsnutzung auf Grundlage des Nutzungsverlaufs werden als Liniendiagramme in Prozent auf der vertikalen (y-)Achse angezeigt. Der Zeitraum wird auf der horizontalen (x-)Achse dargestellt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Die Details für bestimmte Punkte im Diagramm lassen sich anzeigen, indem Sie den Mauszeiger über einen bestimmten Bereich bewegen. Ein Liniendiagramm kann durch Klicken auf die entsprechende Legende aus- oder eingeblendet werden. Wenn Sie beispielsweise auf die Legende „Volume Used Capacity“ klicken, wird die Diagrammlinie „Volume Used Capacity“ ausgeblendet.

- **Auslastung der Snapshot-Kapazität (%)**

  Die Snapshot Reserve und der Snapshot-Warnschwellenwert werden als Liniendiagramme und die von den Snapshot Kopien genutzte Kapazität als Flächendiagramm in Prozent auf der vertikalen (y-)Achse dargestellt. Der Snapshot-Überlauf wird mit unterschiedlichen Farben dargestellt. Der Zeitraum wird auf der horizontalen (x-)Achse angezeigt. Sie können einen Zeitraum von einer Woche, einem Monat oder einem Jahr auswählen. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Mauszeiger über einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende Snapshot Reserve klicken, wird die Diagrammlinie für Snapshot Reserve ausgeblendet.

Ereignisliste

Die Ereignisliste zeigt Details zu neuen und bestätigten Ereignissen an:

- **Schweregrad**

  Zeigt den Schweregrad des Ereignisses an.

- **Ereignis**

  Zeigt den Ereignisnamen an.

- **Auslösezeit**

  Zeigt die seit der Generierung des Ereignisses verstrichene Zeit an. Wenn die verstrichene Zeit mehr als eine Woche beträgt, wird der Zeitstempel angezeigt, zu dem das Ereignis generiert wurde.

Bereich „Verwandte Anmerkungen“

Im Bereich „Zugehörige Anmerkungen“ lassen sich die Anmerkungsdetails anzeigen, die dem ausgewählten Volume zugeordnet sind. Zu diesen Details gehören der Name der Anmerkung und die Anmerkungswerte, die auf das Volume angewendet werden. Manuelle Anmerkungen lassen sich im Bereich „Zugehörige Anmerkungen“ ebenfalls entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie die SVMs, Aggregate, Qtrees, LUNs und Snapshot Kopien anzeigen und zu ihnen navigieren, die mit dem Volume verknüpft sind:

- **Storage Virtual Machine**

  Zeigt die Kapazität und den Systemstatus der SVM an, die das ausgewählte Volume enthält.

- **Aggregat**

  Zeigt die Kapazität und den Systemstatus des Aggregats an, das das ausgewählte Volume enthält. Bei FlexGroup Volumes wird die Anzahl der Aggregate aufgelistet, aus denen sich die FlexGroup zusammensetzt.

- **Volumina im Aggregat**

  Zeigt die Anzahl und Kapazität aller Volumes an, die zum übergeordneten Aggregat des ausgewählten Volumes gehören. Der Systemstatus der Volumes wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Enthält ein Aggregat beispielsweise zehn Volumes, von denen fünf den Status „Warnung“ und die restlichen fünf den Status „Kritisch“ aufweisen, wird der Status „Kritisch“ angezeigt. Diese Komponente wird für FlexGroup Volumes nicht angezeigt.

- **Qtrees**

  Zeigt die Anzahl der qtrees an, die das ausgewählte Volume enthält, sowie die Kapazität der qtrees mit Quota, die das ausgewählte Volume enthält. Die Kapazität der qtrees mit Quota wird im Verhältnis zur Datenkapazität des Volumes angezeigt. Der Systemstatus der qtrees wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn ein Volume beispielsweise zehn qtrees hat, fünf mit dem Status „Warnung“ und die übrigen fünf mit dem Status „Kritisch“, wird der Status „Kritisch“ angezeigt.

- **NFS Freigaben**

  Zeigt die Anzahl und den Status der mit dem Volume verknüpften NFS-Freigaben an.

- **SMB Freigaben**

  Zeigt die Anzahl und den Status der SMB/CIFS-Freigaben an.

- **LUNs**

  Zeigt die Anzahl und Gesamtgröße aller LUNs im ausgewählten Volume an. Der Systemstatus der LUNs wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad.

- **Benutzer- und Gruppenkontingente**

  Zeigt die Anzahl und den Status der Benutzer- und Benutzergruppenquoten an, die dem Volume und seinen qtrees zugeordnet sind.

- **FlexClone Bände**

  Zeigt die Anzahl und Kapazität aller geklonten Volumes des ausgewählten Volumes an. Anzahl und Kapazität werden nur angezeigt, wenn das ausgewählte Volume geklonte Volumes enthält.

- **Übergeordnetes Volume**

  Zeigt den Namen und die Kapazität des übergeordneten Volume eines ausgewählten FlexClone Volume an. Das übergeordnete Volume wird nur angezeigt, wenn das ausgewählte Volume ein FlexClone Volume ist.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ ist die Liste der Gruppen zu sehen, die dem ausgewählten Volume zugeordnet sind.

Bereich „Zugehörige Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der für das ausgewählte Volume erstellten Warnungen anzeigen. Sie können außerdem eine Warnung hinzufügen, indem Sie auf den Link „Warnung hinzufügen“ klicken, oder eine vorhandene Warnung bearbeiten, indem Sie auf den Warnungsnamen klicken.

Die Seite Storage VM / Health-Details in Active IQ Unified Manager

Auf der Seite „Storage VM / Systemstatusdetails“ können Sie detaillierte Informationen zur ausgewählten Storage VM anzeigen, z. B. deren Systemstatus, Kapazität, Konfiguration, Datenrichtlinien, logische Schnittstellen (LIFs), LUNs, qtrees, Benutzer, Benutzergruppenkontingente und Schutzdetails. Außerdem können Sie Informationen zu den zugehörigen Objekten und zugehörigen Warnungen für die Storage VM anzeigen.

Sie können nur die Daten-Storage-VM überwachen.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie die folgenden Aufgaben für die ausgewählte Storage VM ausführen:

- **Zur Performance Ansicht wechseln**

  Ermöglicht die Navigation zur Seite mit den Details zu Storage VM und Performance.

- **Aktionen**
  - Benachrichtigung hinzufügen

    Damit können Sie der ausgewählten Storage VM eine Warnung hinzufügen.

  - Annotieren

    Ermöglicht Ihnen, die ausgewählte storage VM mit Anmerkungen zu versehen.

- **Storage VMs anzeigen**

  Ermöglicht die Navigation zur Ansicht „Systemstatus: Alle Storage VMs“.

Registerkarte „Systemstatus“

Die Registerkarte „Systemstatus“ zeigt detaillierte Informationen über Datenverfügbarkeit, Datenkapazität und Schutzprobleme verschiedener Objekte wie Volumes, Aggregate, NAS LIFs, SAN LIFs, LUNs, Protokolle, Services, NFS-Freigaben und CIFS-Freigaben an.

Sie können auf das Diagramm eines Objekts klicken, um die gefilterte Liste der Objekte anzuzeigen. Beispielsweise können Sie auf das Diagramm zur Volumenkapazität klicken, das Warnungen anzeigt, um die Liste der Volumes mit Kapazitätsproblemen mit dem Schweregrad „Warnung“ anzuzeigen.

- **Verfügbarkeitsprobleme**

  Zeigt als Diagramm die Gesamtzahl der Objekte an, einschließlich der Objekte mit Verfügbarkeitsproblemen und der Objekte ohne Verfügbarkeitsprobleme. Die Farben im Diagramm stehen für die unterschiedlichen Schweregrade der Probleme. Die Informationen unterhalb des Diagramms enthalten Details zu Verfügbarkeitsproblemen, die die Datenverfügbarkeit in der Storage VM beeinträchtigen können oder bereits beeinträchtigt haben. Beispielsweise werden Informationen zu NAS LIFs und SAN LIFs angezeigt, die ausgefallen sind, sowie zu Volumes, die offline sind.

  Sie können außerdem Informationen über die zugehörigen Protokolle und Services, die aktuell ausgeführt werden, sowie über die Anzahl und den Status der NFS- und CIFS-Freigaben anzeigen.

- **Kapazitätsprobleme**

  Die Gesamtzahl der Objekte, einschließlich Objekten mit Kapazitätsproblemen und Objekten ohne kapazitätsbezogene Probleme, wird grafisch dargestellt. Die Farben im Diagramm stehen für die verschiedenen Schweregrade der Probleme. Die Informationen unterhalb des Diagramms enthalten Details zu Kapazitätsproblemen, die sich auf die Datenkapazität in der storage VM auswirken können oder bereits ausgewirkt haben. Beispielsweise werden Informationen zu Aggregaten angezeigt, die die festgelegten Schwellenwerte voraussichtlich überschreiten.

- **Schutzprobleme**

  Bietet einen schnellen Überblick über den Systemstatus in Bezug auf den Schutz der Storage VM, indem in einem Dialogfeld die Gesamtzahl der Beziehungen angezeigt wird, einschließlich Beziehungen mit Schutzproblemen und Beziehungen ohne schutzbezogene Probleme. Außerdem kann der Status der Storage VM DR Beziehung für die ausgewählte Storage VM angezeigt werden. Die Ereignisse der Storage VM DR Beziehungen werden hier angezeigt, und durch Klicken auf die Ereignisse wird die Seite mit den Ereignisdetails geöffnet. Wenn ungeschützte Volumes vorhanden sind, wird durch Klicken auf den Link die Ansicht „Systemstatus: Alle Volumes“ geöffnet, in der eine gefilterte Liste der ungeschützten Volumes auf der Storage VM angezeigt werden kann. Die Farben im Diagramm stehen für die verschiedenen Schweregrade der Probleme. Durch Klicken auf ein Diagramm wird die Ansicht „Beziehung: Alle Beziehungen“ geöffnet, in der eine gefilterte Liste der Details zu Schutzbeziehungen angezeigt werden kann. Die Informationen unterhalb des Diagramms enthalten Details zu Schutzproblemen, die den Schutz der Daten in der Storage VM beeinträchtigen können oder bereits beeinträchtigt haben. Beispielsweise werden Informationen zu Volumes angezeigt, deren Reserve für Snapshot Kopien fast voll ist, oder zu Problemen mit der Verzögerung von SnapMirror Beziehungen.

Registerkarte Kapazität

Die Registerkarte „Kapazität“ zeigt detaillierte Informationen zur Datenkapazität der ausgewählten SVM an.

Die folgenden Informationen werden für eine Storage VM mit FlexVol volume oder FlexGroup volume angezeigt:

- **Kapazität**

  Der Bereich „Kapazität“ zeigt Details zur genutzten und verfügbaren Kapazität an, die aus allen Volumes zugewiesen wurde:

  - Gesamtkapazität

    Zeigt die Gesamtkapazität der Storage VM an.

  - Gebraucht

    Zeigt den von den Daten in den Volumes belegten Speicherplatz an, die zur Storage VM gehören.

  - Garantiert verfügbar

    Zeigt den garantiert verfügbaren Speicherplatz für Daten in Volumes der Storage VM an.

  - Nicht garantiert

    Zeigt den verbleibenden verfügbaren Speicherplatz für Daten an, die für Thin Provisioning Volumes in der Storage VM zugewiesen sind.

- **Volumina mit Kapazitätsproblemen**

  Die Liste „Volumes mit Kapazitätsproblemen“ zeigt in Tabellenform Details zu den Volumes an, die Kapazitätsprobleme aufweisen:

  - Status

    Weist darauf hin, dass das Volume ein kapazitätsbezogenes Problem mit dem angegebenen Schweregrad aufweist.

    Beim Bewegen des Mauszeigers auf den Status erscheinen weitere Informationen zu dem oder den für das Volume generierten kapazitätsbezogenen Ereignissen.

    Wenn der Status des Volume durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, Datum und Uhrzeit der Auslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Mit der Schaltfläche **View Details** können Sie weitere Informationen zum Ereignis anzeigen.

    Wenn der Status des Volume durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum der Auslösung sowie dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Weitere Details zu jedem dieser Ereignisse können durch Klicken auf den Ereignisnamen angezeigt werden. Außerdem kann über den Link **View All Events** die Liste der generierten Ereignisse angezeigt werden.

    > Ein Volume kann mehrere Ereignisse mit demselben Schweregrad oder mit unterschiedlichen Schweregraden aufweisen. Es wird jedoch nur der höchste Schweregrad angezeigt. Wenn ein Volume beispielsweise zwei Ereignisse mit den Schweregraden „Fehler“ und „Warnung“ aufweist, wird nur der Schweregrad „Fehler“ angezeigt.

  - Volumen

    Zeigt den Namen des Volumes an.

- Genutzte Datenkapazität

  Stellt Informationen zur Kapazitätsauslastung des Volumes (in Prozent) grafisch dar.

- Tage bis voll

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bis das Volume seine volle Kapazität erreicht.

- Thin-provisioniert

  Zeigt an, ob für das ausgewählte Volume eine Speicherplatzzusage festgelegt ist. Gültige Werte sind Ja und Nein.

- Aggregate

  Bei FlexVol Volumes wird der Name des Aggregats angezeigt, das das Volume enthält. Bei FlexGroup Volumes wird die Anzahl der Aggregate angezeigt, die die FlexGroup verwendet.

Registerkarte „Konfiguration“

Die Registerkarte „Konfiguration“ zeigt Konfigurationsdetails zur ausgewählten Storage VM an, z. B. ihren Cluster, ihr Root-Volume, den Typ der enthaltenen Volumes (FlexVol Volumes), Richtlinien und den auf der Storage VM erstellten Schutz:

- **Überblick**
  - Cluster

    Zeigt den Namen des Clusters an, zu dem die Storage VM gehört.

  - Zulässiger Volumentyp

    Zeigt die Arten von Volumes an, die in der Storage VM erstellt werden können. Der Typ kann FlexVol oder FlexVol/FlexGroup sein.

  - Root-Volume

    Zeigt den Namen des Root-Volumes der storage VM an.

  - Zulässige Protokolle

    Zeigt die auf der Storage VM konfigurierbaren Protokolltypen an. Außerdem wird angezeigt, ob ein Protokoll aktiv (), inaktiv () oder nicht konfiguriert () ist.

- **Datennetzwerkschnittstellen**
  - NAS

    Zeigt die Anzahl der NAS-Schnittstellen an, die der Storage VM zugeordnet sind. Außerdem zeigt dies an, ob die Schnittstellen aktiv () oder inaktiv () sind.

  - SAN

    Zeigt die Anzahl der SAN-Schnittstellen an, die der Storage VM zugeordnet sind. Außerdem wird angezeigt, ob die Schnittstellen aktiv () oder inaktiv () sind.

  - FC-NVMe

Zeigt die Anzahl der FC-NVMe-Schnittstellen an, die der Storage VM zugeordnet sind. Außerdem wird angezeigt, ob die Schnittstellen aktiv (●) oder inaktiv (●) sind.

- **Management Netzwerkschnittstellen**
  - Verfügbarkeit

    Zeigt die Anzahl der Verwaltungsschnittstellen an, die der Storage VM zugeordnet sind. Außerdem wird angezeigt, ob die Verwaltungsschnittstellen aktiv (●) oder inaktiv (●) sind.

- **Richtlinien**
  - Snapshots

    Zeigt den Namen der Snapshot-Richtlinie an, die auf der Storage VM erstellt wird.

  - Exportrichtlinien

    Zeigt entweder den Namen der Exportrichtlinie an, wenn nur eine Richtlinie erstellt wurde, oder die Anzahl der Exportrichtlinien, wenn mehrere Richtlinien erstellt wurden.

- **Schutz**
  - Storage VM DR

    Zeigt an, ob die ausgewählte Storage VM geschützt, Ziel oder ungeschützt ist, sowie den Namen des Ziels, auf dem die Storage VM geschützt ist. Wenn die ausgewählte Storage VM ein Ziel ist, werden die Details der Quell-Storage VM angezeigt. Im Fall von Fan-out zeigt dieses Feld die Gesamtzahl der Ziel-Storage VMs an, auf denen die Storage VM geschützt ist. Der Link „Anzahl“ führt zur Storage VM Beziehungsübersicht, gefiltert nach der Quell-Storage VM.

  - Geschützte Volumes

    Zeigt die Anzahl der geschützten Volumes auf der ausgewählten Storage VM im Verhältnis zur Gesamtzahl der Volumes an. Wenn Sie eine Ziel Storage VM anzeigen, bezieht sich der Zahlenlink auf die Ziel-Volumes der ausgewählten Storage VM.

  - Ungeschützte Volumes

    Zeigt die Anzahl der ungeschützten Volumes auf der ausgewählten storage VM an.

- **Services**
  - Typ

    Zeigt den auf der Storage VM konfigurierten Diensttyp an. Mögliche Typen sind Domain Name System (DNS) oder Network Information Service (NIS).

  - Status

    Zeigt den Status des Dienstes an, der entweder Aktiv (●), Inaktiv (●) oder Nicht konfiguriert (●) sein kann.

  - Domainname

    Zeigt die vollqualifizierten Domainnamen (FQDNs) des DNS-Servers für die DNS Services bzw. des NIS-Servers für die NIS Services an. Wenn der NIS-Server aktiviert ist, wird der aktive FQDN des NIS-Servers angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller FQDNs angezeigt.

- IP-Adresse

  Zeigt die IP-Adressen des DNS- oder NIS-Servers an. Wenn der NIS-Server aktiviert ist, wird dessen aktive IP-Adresse angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller IP-Adressen angezeigt.

Registerkarte „Netzwerkschnittstellen“

Die Registerkarte „Netzwerkschnittstellen“ zeigt Details zu den Datennetzwerkschnittstellen (LIFs) an, die auf der ausgewählten Storage VM erstellt wurden:

- **Netzwerkschnittstelle**

  Zeigt den Namen der Schnittstelle an, die auf der ausgewählten storage VM erstellt wird.

- **Betriebsstatus**

  Zeigt den Betriebsstatus der Schnittstelle an, der Aktiv (), Inaktiv () oder Unbekannt () sein kann. Der Betriebsstatus einer Schnittstelle hängt vom Status ihrer physischen Ports ab.

- **Verwaltungsstatus**

  Zeigt den administrativen Status der Schnittstelle an, der „Up“ (), „Down“ () oder „Unknown“ () sein kann. Der administrative Status einer Schnittstelle wird vom Storage Administrator gesteuert, um Änderungen an der Konfiguration vorzunehmen oder Wartungsarbeiten durchzuführen. Der administrative Status kann vom Betriebsstatus abweichen. Ist der administrative Status einer Schnittstelle jedoch „Down“, ist der Betriebsstatus standardmäßig ebenfalls „Down“.

- **IP-Adresse / WWPN**

  Zeigt die IP-Adresse für Ethernet-Schnittstellen und den World Wide Port Name (WWPN) für FC LIFs an.

- **Protokolle**

  Zeigt die Liste der für die Schnittstelle angegebenen Datenprotokolle an, wie z. B. CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe und FlexCache.

- **Rolle**

  Zeigt die Schnittstellenrolle an. Die Rollen können Data oder Management sein.

- **Home-Port**

  Zeigt den physischen Port an, dem die Schnittstelle ursprünglich zugeordnet war.

- **Aktueller Port**

  Zeigt den physischen Port an, dem die Schnittstelle aktuell zugeordnet ist. Wenn die Schnittstelle migriert wird, kann der aktuelle Port vom ursprünglichen Port abweichen.

- **Portsatz**

  Zeigt den Portsatz an, dem die Schnittstelle zugeordnet ist.

- **Failover Richtlinie**

Zeigt die für die Schnittstelle konfigurierte Failover-Richtlinie an. Für NFS-, CIFS- und FlexCache Schnittstellen ist die Standard-Failover-Richtlinie Next Available. Die Failover-Richtlinie gilt nicht für FC- und iSCSI-Schnittstellen.

- **Routing-Gruppen**

  Zeigt den Namen der Routing-Gruppe an. Über den Namen der Routing-Gruppe lassen sich weitere Informationen zu den Routen und dem Ziel-Gateway anzeigen.

  Routing-Gruppen werden für ONTAP 8.3 oder höher nicht unterstützt, daher wird für diese Cluster eine leere Spalte angezeigt.

- **Failover Gruppe**

  Zeigt den Namen der Failover-Gruppe an.

Registerkarte Qtrees

Die Registerkarte „Qtrees“ zeigt Details zu Qtrees und ihren Kontingenten an. Wenn Sie die Systemstatus-Schwellenwerteinstellungen für die Qtree-Kapazität für einen oder mehrere Qtrees bearbeiten möchten, können Sie auf die Schaltfläche „Schwellenwerte bearbeiten“ klicken.

Mit der Schaltfläche **Exportieren** wird eine Datei mit kommagetrennten Werten (.csv) erstellt, die die Details aller überwachten qtrees enthält. Beim Export in eine CSV-Datei kann ein qtrees-Bericht für die aktuelle Storage VM, für alle Storage VMs im aktuellen Cluster oder für alle Storage VMs aller Cluster in Ihrem Datacenter erstellt werden. In der exportierten CSV-Datei werden einige zusätzliche qtrees-Felder angezeigt.

- **Status**

  Zeigt den aktuellen Status des qtree an. Der Status kann Kritisch (), Fehler (), Warnung () oder Normal () sein.

  Sie können den Mauszeiger über das Statussymbol bewegen, um weitere Informationen über das oder die für den qtree generierten Ereignisse anzuzeigen.

  Wenn ein einzelnes Ereignis den Status des qtree bestimmt, können Informationen wie der Ereignisname, Datum und Uhrzeit der Auslösung, der Name des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses angezeigt werden. Mit **View Details** können weitere Informationen zu dem Ereignis angezeigt werden.

  Wird der Status des qtree durch mehrere Ereignisse desselben Schweregrads bestimmt, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum der Auslösung sowie dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Weitere Details zu jedem dieser Ereignisse lassen sich durch Klicken auf den Ereignisnamen anzeigen. Auch **View All Events** kann zum Anzeigen der Liste der generierten Ereignisse verwendet werden.

  > Ein Qtree kann mehrere Ereignisse mit demselben oder mit unterschiedlichen Schweregraden aufweisen. Es wird jedoch nur der höchste Schweregrad angezeigt. Wenn ein Qtree beispielsweise zwei Ereignisse mit den Schweregraden „Fehler“ und „Warnung“ aufweist, wird nur der Schweregrad „Fehler“ angezeigt.

- **Qtree**

  Zeigt den Namen des qtree an.

- **Cluster**

  Zeigt den Namen des Clusters an, der den qtree enthält. Erscheint nur in der exportierten CSV-Datei.

- **Storage Virtual Machine**

  Zeigt den Namen der Storage Virtual Machine (SVM) an, die den qtree enthält. Erscheint nur in der exportierten CSV-Datei.

- **Volumen**

  Zeigt den Namen des Volumes an, das den qtree enthält.

  Weitere Informationen zum Volume werden angezeigt, wenn sich der Mauszeiger über dem Volume-Namen befindet.

- **Kontingentsatz**

  Zeigt an, ob ein Kontingent auf dem qtree aktiviert oder deaktiviert ist.

- **Quotenart**

  Gibt an, ob das Kontingent für einen Benutzer, eine Benutzergruppe oder einen qtree gilt. Wird nur in der exportierten CSV-Datei angezeigt.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Für jeden Benutzer und jede Benutzergruppe werden mehrere Zeilen angezeigt. Bei Quota-Typ qtree oder wenn kein Quota festgelegt ist, ist die Spalte leer. Sie ist nur in der exportierten CSV-Datei enthalten.

- **Festplattenauslastung %**

  Zeigt den prozentualen Anteil des belegten Festplattenspeichers an. Wenn ein endgültiges Festplatten-Limit festgelegt ist, basiert dieser Wert auf diesem endgültigen Festplatten-Limit. Wenn das Kontingent ohne endgültiges Festplatten-Limit festgelegt ist, basiert der Wert auf dem Datenspeicherplatz des Volume. Wenn das Kontingent nicht festgelegt ist oder wenn Kontingente auf dem Volume, zu dem der qtree gehört, deaktiviert sind, wird auf der Rasterseite “Not applicable” angezeigt, und das Feld ist in den CSV-Exportdaten leer.

- **Endgültiges Limit für Datenträger**

  Zeigt den maximalen dem Qtree zugewiesenen Speicherplatz an. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht wird und keine weiteren Schreibvorgänge auf den Datenträger zulässig sind. Der Wert wird unter den folgenden Bedingungen als “Unlimited” angezeigt: wenn das Kontingent ohne endgültiges Limit für den Datenträger festgelegt ist, wenn kein Kontingent festgelegt ist oder wenn Kontingente für das Volume, zu dem der Qtree gehört, deaktiviert sind.

- **Soft Limit für Datenträger**

  Zeigt den für den qtree zugewiesenen Speicherplatz an, bevor ein Warnereignis generiert wird. Der Wert wird unter folgenden Bedingungen als “Unlimited” angezeigt: wenn das Quota ohne Softlimit für den Speicherplatz festgelegt ist, wenn kein Quota festgelegt ist oder wenn Quotas auf dem Volume, zu dem der qtree gehört, deaktiviert sind. Standardmäßig ist diese Spalte ausgeblendet.

- **Festplattenschwellenwert**

  Zeigt den für den Speicherplatz festgelegten Schwellenwert an. Der Wert wird unter den folgenden Bedingungen als “Unlimited” angezeigt: wenn das Kontingent ohne Grenzwert für den Speicherplatzschwellenwert festgelegt ist, wenn kein Kontingent festgelegt ist oder wenn Kontingente auf dem Volume, zu dem der qtree gehört, deaktiviert sind. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im qtree verwendeten Dateien an. Wenn das endgültige Dateilimit festgelegt ist, basiert dieser Wert auf dem endgültigen Dateilimit. Wenn das Kontingent ohne endgültiges Dateilimit festgelegt ist, wird kein Wert angezeigt. Wenn das Kontingent nicht festgelegt ist oder wenn Kontingente auf dem Volume, zu dem der qtree gehört, deaktiviert sind, wird auf der Rasterseite “Not applicable” angezeigt, und das Feld in den CSV-Exportdaten bleibt leer.

- **Endgültiges Dateilimit**

  Zeigt das endgültige Limit für die Anzahl der auf den qtrees zulässigen Dateien an. Der Wert wird unter den folgenden Bedingungen als „`Unlimited`“ angezeigt: wenn das Quota ohne endgültiges Dateilimit festgelegt ist, wenn das Quota nicht festgelegt ist oder wenn Quotas auf dem Volume, zu dem der qtree gehört, deaktiviert sind.

- **Datei-Soft-Limit**

  Zeigt das Soft-Limit für die Anzahl der auf den qtrees zulässigen Dateien an. Der Wert wird unter den folgenden Bedingungen als “Unlimited” angezeigt: wenn das Quota ohne Soft-Limit für Dateien festgelegt ist, wenn das Quota nicht festgelegt ist oder wenn Quotas auf dem Volume deaktiviert sind, zu dem der qtree gehört. Standardmäßig ist diese Spalte ausgeblendet.

Registerkarte „Benutzer- und Gruppenkontingente“

Zeigt Details zu den Benutzer- und Benutzergruppenkontingenten für die ausgewählte Storage VM an. Sie können Informationen wie den Status des Kontingents, den Namen des Benutzers oder der Benutzergruppe, die für Festplatten und Dateien festgelegten Soft Limits und endgültigen Limits, den belegten Speicherplatz und die Anzahl der verwendeten Dateien sowie den Festplattenschwellenwert anzeigen. Außerdem kann die einem Benutzer oder einer Benutzergruppe zugeordnete E-Mail-Adresse geändert werden.

- **Schaltfläche „E-Mail-Adresse bearbeiten“**

  Öffnet das Dialogfeld „E-Mail-Adresse bearbeiten“, in dem die aktuelle E-Mail-Adresse des ausgewählten Benutzers oder der ausgewählten Benutzergruppe angezeigt wird. Die E-Mail-Adresse lässt sich ändern. Wenn das Feld „E-Mail-Adresse bearbeiten“ leer ist, wird die Standardregel verwendet, um eine E-Mail-Adresse für den ausgewählten Benutzer oder die ausgewählte Benutzergruppe zu generieren.

  Wenn mehrere Benutzer das gleiche Kontingent haben, werden ihre Namen durch Kommas getrennt angezeigt. Die Standardregel wird nicht zur Generierung der E-Mail-Adresse verwendet; daher müssen Sie die erforderliche E-Mail-Adresse für den Versand von Benachrichtigungen angeben.

- **Befehlsschaltfläche „E-Mail-Regeln konfigurieren“**

  Ermöglicht das Erstellen oder Ändern von Regeln zur Generierung einer E-Mail-Adresse für die auf der Storage VM konfigurierten Benutzer- oder Benutzergruppenkontingente. Bei einer Kontingentüberschreitung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

- **Status**

Zeigt den aktuellen Status des Kontingents an. Der Status kann Kritisch (), Warnung () oder Normal () sein.

Sie können den Mauszeiger über das Statussymbol bewegen, um weitere Informationen zu dem oder den für das Kontingent generierten Ereignissen anzuzeigen.

Wenn der Kontingentstatus durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, Datum und Uhrzeit der Auslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses einsehen. Mit **View Details** können Sie weitere Informationen zum Ereignis einsehen.

Wenn der Status des Kontingents durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum der Auslösung sowie dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Weitere Details zu jedem dieser Ereignisse können durch Klicken auf den Ereignisnamen angezeigt werden. Außerdem kann **View All Events** verwendet werden, um die Liste der generierten Ereignisse anzuzeigen.

> Ein Kontingent kann mehrere Ereignisse mit demselben oder mit unterschiedlichen Schweregraden enthalten. Es wird jedoch nur der höchste Schweregrad angezeigt. Wenn ein Kontingent beispielsweise zwei Ereignisse mit den Schweregraden „Fehler“ und „Warnung“ enthält, wird nur der Schweregrad „Fehler“ angezeigt.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Wenn mehrere Benutzer dasselbe Kontingent haben, erscheinen die Benutzernamen als kommagetrennte Werte.

  Der Wert wird als “Unknown” angezeigt, wenn ONTAP aufgrund von SecD-Fehlern keinen gültigen Benutzernamen angibt.

- **Typ**

  Gibt an, ob das Kontingent für einen Benutzer oder eine Benutzergruppe gilt.

- **Volume oder Qtree**

  Zeigt den Namen des Volumes oder qtree an, für den das Benutzer- oder Gruppenkontingent festgelegt ist.

  Sie können den Mauszeiger über den Namen des Volumes oder qtree bewegen, um weitere Informationen über das Volume oder den qtree anzuzeigen.

- **Festplattenauslastung %**

  Zeigt den Prozentsatz des belegten Speicherplatzes an. Der Wert wird als “Nicht anwendbar” angezeigt, wenn das Kontingent ohne endgültiges Limit festgelegt ist.

- **Endgültiges Limit für Datenträger**

  Zeigt den maximal für das Kontingent reservierten Speicherplatz an. Unified Manager löst ein kritisches Ereignis aus, sobald dieses Limit erreicht ist; weitere Schreibvorgänge sind dann nicht mehr möglich. Der Wert wird als “Unlimited” angezeigt, wenn für das Kontingent kein endgültiges Limit für den Speicherplatz festgelegt ist.

- **Soft Limit für Datenträger**

Zeigt die dem Kontingent zugewiesene Speichermenge an, bevor ein Warnereignis generiert wird. Der Wert wird als “Unlimited” angezeigt, wenn das Kontingent ohne Softlimit für den Speicherplatz festgelegt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Festplattenschwellenwert**

  Zeigt den für den Speicherplatz festgelegten Schwellenwert an. Der Wert wird als “Unlimited” angezeigt, wenn das Kontingent ohne Speicherplatz-Schwellenwertlimit festgelegt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im Qtree verwendeten Dateien an. Der Wert wird als “Not applicable” angezeigt, wenn das Kontingent ohne endgültiges Limit für Dateien festgelegt ist.

- **Endgültiges Dateilimit**

  Zeigt das endgültige Limit für die Anzahl der im Rahmen des Kontingents zulässigen Dateien an. Der Wert wird als “Unlimited” angezeigt, wenn das Kontingent ohne endgültiges Limit für Dateien festgelegt ist.

- **Datei-Soft-Limit**

  Zeigt das weiche Limit für die Anzahl der im Kontingent zulässigen Dateien an. Der Wert wird als “Unlimited” angezeigt, wenn das Kontingent ohne weiches Dateilimit festgelegt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **E-Mail-Adresse**

  Zeigt die E-Mail-Adresse des Benutzers oder der Benutzergruppe an, an die Benachrichtigungen bei einer Kontingentüberschreitung gesendet werden.

Registerkarte NFS-Freigaben

Die Registerkarte „NFS-Freigaben“ zeigt Informationen zu NFS-Freigaben an, z. B. deren Status, den dem Volume zugeordneten Pfad (FlexGroup Volumes oder FlexVol Volumes), die Zugriffsebenen von Clients auf die NFS-Freigaben und die Exportrichtlinie, die für die exportierten Volumes definiert ist. NFS-Freigaben werden unter folgenden Bedingungen nicht angezeigt: wenn das Volume nicht eingebunden ist oder wenn die der Exportrichtlinie für das Volume zugeordneten Protokolle keine NFS-Freigaben enthalten.

- **Status**

  Zeigt den aktuellen Status der NFS-Freigaben an. Der Status kann Error () oder Normal () sein.

- **Verbindungspfad**

  Zeigt den Pfad an, unter dem das Volume gemountet ist. Wenn eine explizite NFS-Exportrichtlinie auf einen Qtree angewendet wird, zeigt die Spalte den Pfad des Volumes an, über den auf den Qtree zugegriffen werden kann.

- **Verbindungspfad aktiv**

  Zeigt an, ob der Pfad für den Zugriff auf das gemountete Volume aktiv oder inaktiv ist.

- **Volume oder Qtree**

  Zeigt den Namen des Volumes oder Qtrees an, für den die NFS-Exportrichtlinie gilt. Wenn eine NFS-

Exportrichtlinie für einen Qtree im Volume gilt, zeigt die Spalte sowohl den Namen des Volumes als auch den des Qtrees an.

Über den Link lassen sich Details zum Objekt auf der entsprechenden Detailseite anzeigen. Wenn es sich bei dem Objekt um einen qtree handelt, werden Links sowohl für den qtree als auch für das Volume angezeigt.

- **Volume Status**

  Zeigt den Status des exportierten Volumes an. Der Status kann Offline, Online, Eingeschränkt oder Gemischt sein.

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht gestattet.

  - Online

    Lese- und Schreibzugriff auf das Volume ist zulässig.

  - Eingeschränkt

    Begrenzte Operationen wie Paritätsrekonstruktion sind zulässig, der Datenzugriff ist jedoch nicht gestattet.

  - Gemischt

    Die Bestandteile eines FlexGroup Volume befinden sich nicht alle im gleichen Zustand.

- **Sicherheitsstil**

  Zeigt die Zugriffsberechtigungen für die exportierten Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder Mixed sein.

  - UNIX (NFS Clients)

    Die Dateien und Verzeichnisse im Volume haben UNIX-Berechtigungen.

  - Vereinheitlicht

    Dateien und Verzeichnisse im Volume haben einen einheitlichen Sicherheitsstil.

  - NTFS (CIFS-Clients)

    Die Dateien und Verzeichnisse auf dem Volume verfügen über Windows NTFS-Berechtigungen.

  - Gemischt

    Dateien und Verzeichnisse im Volume können entweder UNIX-Berechtigungen oder Windows NTFS-Berechtigungen haben.

- **UNIX-Berechtigung**

  Zeigt die UNIX-Berechtigungsbits in einem Oktalstringformat an, die für die exportierten Volumes festgelegt sind. Sie ähneln den Berechtigungsbits im UNIX-Stil.

- **Exportrichtlinie**

  Zeigt die Regeln an, die die Zugriffsberechtigung für exportierte Volumes definieren. Über den Link lassen sich Details zu den mit der Exportrichtlinie verknüpften Regeln anzeigen, z. B. zu den Authentifizierungsprotokollen und der Zugriffsberechtigung.

Registerkarte „SMB-Freigaben“

Zeigt Informationen zu den SMB-Freigaben auf der ausgewählten Storage VM an. Sie können Informationen wie den Status der SMB-Freigabe, den Freigabenamen, den mit der Storage VM verknüpften Pfad, den Status des Verbindungspfads der Freigabe, das übergeordnete Objekt, den Status des übergeordneten Volumes, die Sicherheitsdaten der Freigabe und die für die Freigabe definierten Exportrichtlinien anzeigen. Außerdem können Sie feststellen, ob ein äquivalenter NFS-Pfad für die SMB-Freigabe existiert.

Auf der Registerkarte „SMB-Freigaben“ sind keine Freigaben in Ordnern sichtbar.

- **Befehlsschaltfläche „Benutzerzuordnung anzeigen“**

  Öffnet das Dialogfeld „Benutzerzuordnung“.

  Die Details der Benutzerzuordnung für die Storage VM lassen sich anzeigen.

- **Schaltfläche zum Anzeigen des ACL-Befehls**

  Öffnet das Dialogfeld „Zugriffskontrolle“ für die Freigabe.

  Sie können die Benutzer- und Berechtigungsdetails für die ausgewählte Freigabe anzeigen.

- **Status**

  Zeigt den aktuellen Status der Freigabe an. Der Status kann Normal ( ) oder Fehler ( ) sein.

- **Name der Freigabe**

  Zeigt den Namen der SMB-Freigabe an.

- **Pfad**

  Zeigt den Verbindungspfad an, auf dem die Freigabe erstellt wird.

- **Verbindungspfad aktiv**

  Zeigt an, ob der Pfad zum Zugriff auf die Freigabe aktiv oder inaktiv ist.

- **Enthaltendes Objekt**

  Zeigt den Namen des übergeordneten Objekts an, zu dem die Freigabe gehört. Das übergeordnete Objekt kann ein Volume oder ein qtree sein.

  Nach dem Klicken auf den Link zeigt die entsprechende Detailseite Details zum übergeordneten Objekt an. Wenn das übergeordnete Objekt ein qtree ist, werden Links sowohl für qtree als auch für Volume angezeigt.

- **Volume Status**

Zeigt den Status des exportierten Volumes an. Der Status kann Offline, Online, Eingeschränkt oder Gemischt sein.

- Offline

  Lese- oder Schreibzugriff auf das Volume ist nicht gestattet.

- Online

  Lese- und Schreibzugriff auf das Volume ist zulässig.

- Eingeschränkt

  Begrenzte Operationen wie Paritätsrekonstruktion sind zulässig, der Datenzugriff ist jedoch nicht gestattet.

- Gemischt

  Die Bestandteile eines FlexGroup Volume befinden sich nicht alle im gleichen Zustand.

- **Sicherheit**

  Zeigt die Zugriffsberechtigungen für die exportierten Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder Mixed sein.

  - UNIX (NFS Clients)

    Die Dateien und Verzeichnisse im Volume haben UNIX-Berechtigungen.

  - Vereinheitlicht

    Dateien und Verzeichnisse im Volume haben einen einheitlichen Sicherheitsstil.

  - NTFS (CIFS-Clients)

    Die Dateien und Verzeichnisse auf dem Volume verfügen über Windows NTFS-Berechtigungen.

  - Gemischt

    Dateien und Verzeichnisse im Volume können entweder UNIX-Berechtigungen oder Windows NTFS-Berechtigungen haben.

- **Exportrichtlinie**

  Zeigt den Namen der für die Freigabe geltenden Exportrichtlinie an. Wenn für die Storage VM keine Exportrichtlinie angegeben ist, wird der Wert als Not Enabled angezeigt.

  Über den Link lassen sich Details zu den mit der Exportrichtlinie verknüpften Regeln anzeigen, z. B. Zugriffsprotokolle und Berechtigungen. Der Link ist deaktiviert, wenn die Exportrichtlinie für die ausgewählte Storage VM deaktiviert ist.

- **NFS Äquivalent**

  Gibt an, ob es ein NFS-Äquivalent für die Freigabe gibt.

Registerkarte SAN

Zeigt Details zu LUNs, Initiatorgruppen und Initiatoren für die ausgewählte Storage VM an. Standardmäßig wird die LUN-Ansicht angezeigt. Details zu den Initiatorgruppen werden auf der Registerkarte „Initiator Groups“ und Details zu den Initiatoren auf der Registerkarte „Initiators“ angezeigt.

- **Registerkarte „LUNs“**

  Zeigt Details zu den LUNs an, die zur ausgewählten Storage VM gehören. Angezeigt werden Informationen wie der LUN-Name, der LUN-Status (online oder offline), der Name des Dateisystems (Volume oder qtree), das die LUN enthält, der Typ des Host-Betriebssystems, die gesamte Datenkapazität und die Seriennummer der LUN. Die Spalte „LUN Performance“ enthält einen Link zur Detailseite „LUN/Performance“.

  Sie können außerdem Informationen darüber anzeigen, ob Thin Provisionierung auf der LUN aktiviert ist und ob die LUN einer Initiatorgruppe zugeordnet ist. Falls sie einem Initiator zugeordnet ist, können Sie die Initiatorgruppen und Initiatoren anzeigen, die der ausgewählten LUN zugeordnet sind.

- **Registerkarte „Initiatorgruppen“**

  Zeigt Details zu Initiatorgruppen an. Es lassen sich Angaben wie der Name der Initiatorgruppe, der Zugriffsstatus, das von allen Initiatoren der Gruppe verwendete Host-Betriebssystem und das unterstützte Protokoll einsehen. Durch Klicken auf den Link in der Spalte „Zugriffsstatus“ lässt sich der aktuelle Zugriffsstatus der Initiatorgruppe einsehen.

  - **Normal**

    Die Initiatorgruppe ist mit mehreren Zugriffspfaden verbunden.

  - **Einzelpfad**

    Die Initiatorgruppe ist mit einem einzigen Zugriffspfad verbunden.

  - **Keine Pfade**

    Es ist kein Zugriffspfad mit der Initiatorgruppe verbunden.

    Es kann angezeigt werden, ob Initiatorgruppen über ein Portset allen Schnittstellen oder bestimmten Schnittstellen zugeordnet sind. Beim Klicken auf den Link für die Anzahl in der Spalte „Zugeordnete Schnittstellen“ werden entweder alle Schnittstellen oder bestimmte Schnittstellen für ein Portset angezeigt. Schnittstellen, die über das Zielportal zugeordnet sind, werden nicht angezeigt. Die Gesamtzahl der Initiatoren und LUNs, die einer Initiatorgruppe zugeordnet sind, wird angezeigt.

  Sie können auch die LUNs und Initiatoren anzeigen, die der ausgewählten Initiatorgruppe zugeordnet sind.

- **Registerkarte „Initiatoren“**

  Zeigt den Namen und Typ des Initiators sowie die Gesamtzahl der diesem Initiator zugeordneten Initiatorgruppen für die ausgewählte Storage VM an.

```
initiator groups that are mapped to the selected initiator group.
```

Bereich „Verwandte Anmerkungen“

Im Bereich „Zugehörige Anmerkungen“ können Sie die Anmerkungsdetails anzeigen, die der ausgewählten Storage VM zugeordnet sind. Zu den Details gehören der Anmerkungsname und die Anmerkungswerte, die auf die Storage VM angewendet werden. Im Bereich „Zugehörige Anmerkungen“ können Sie auch manuelle Anmerkungen entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Zugehörige Geräte“ lassen sich die Cluster, Aggregate und Volumes anzeigen, die mit der Storage VM verknüpft sind:

- **Cluster**

  Zeigt den Systemstatus des Clusters an, zu dem die Storage VM gehört.

- **Aggregate**

  Zeigt die Anzahl der Aggregate an, die zur ausgewählten Storage VM gehören. Der Systemstatus der Aggregate wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn eine Storage VM beispielsweise zehn Aggregate enthält, von denen fünf den Status „Warnung“ und die restlichen fünf den Status „Kritisch“ anzeigen, wird der Status „Kritisch“ angezeigt.

- **Zugewiesene Aggregate**

  Zeigt die Anzahl der Aggregate an, die einer Storage VM zugewiesen sind. Der Systemstatus der Aggregate wird ebenfalls basierend auf dem höchsten Schweregrad angezeigt.

- **Volumes**

  Die Anzahl und Kapazität der Volumes, die zur ausgewählten Storage VM gehören, werden angezeigt. Der Systemstatus der Volumes wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn in der Storage VM FlexGroup Volumes vorhanden sind, umfasst die Anzahl auch FlexGroups; FlexGroup Bestandteile sind nicht enthalten.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ kann die Liste der Gruppen angezeigt werden, die der ausgewählten Storage VM zugeordnet sind.

Bereich „Zugehörige Warnungen“

Im Bereich „Zugehörige Warnungen“ können Sie die Liste der für die ausgewählte Storage VM erstellten Warnungen anzeigen. Sie können außerdem eine Warnung hinzufügen, indem Sie auf den Link **Add Alert** klicken, oder eine vorhandene Warnung bearbeiten, indem Sie auf den Warnungsnamen klicken.

Die Seite mit den Cluster- und Integritätsdetails in Active IQ Unified Manager

Die Seite „Cluster-/Systemstatusdetails“ bietet detaillierte Informationen zu einem ausgewählten Cluster, z. B. zu Systemstatus, Kapazität und Konfigurationsdetails. Sie können außerdem Informationen zu den Netzwerkschnittstellen (LIFs), Knoten, Datenträgern, zugehörigen Geräten und zugehörigen Warnmeldungen für das Cluster einsehen.

Der Status neben dem Clusternamen, beispielsweise (Gut), gibt den Kommunikationsstatus an; er zeigt an, ob

Unified Manager mit dem Cluster kommunizieren kann. Er gibt weder den Failover-Status noch den Gesamtstatus des Clusters an.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können für den ausgewählten Cluster die folgenden Aufgaben ausgeführt werden:

- **Zur Performance Ansicht wechseln**

  Ermöglicht die Navigation zur Seite mit den Cluster-/Leistungsdetails.

- **Aktionen**

  - Warnung hinzufügen: Öffnet das Dialogfeld „Warnung hinzufügen“, mit dem Sie dem ausgewählten Cluster eine Warnung hinzufügen können.
  - Rediscover: Startet eine manuelle Aktualisierung des Clusters, sodass Unified Manager die letzten Änderungen am Cluster identifizieren kann.

    Wenn Unified Manager mit OnCommand Workflow Automation gekoppelt ist, ruft die erneute Identifizierung gegebenenfalls auch zwischengespeicherte Daten von WFA erneut ab.

  Nach dem Start des Vorgangs zur erneuten Identifizierung wird ein Link zu den zugehörigen Job-Details angezeigt, damit der Job-Status nachverfolgt werden kann.

  - Annotieren: Ermöglicht Ihnen, den ausgewählten Cluster zu annotieren.

- **Cluster anzeigen**

  Ermöglicht die Navigation zur Ansicht „Systemstatus: Alle Cluster“.

Registerkarte „Systemstatus“

Zeigt detaillierte Informationen zur Datenverfügbarkeit und Datenkapazität verschiedener Clusterobjekte wie Knoten, SVMs und Aggregate an. Verfügbarkeitsprobleme stehen im Zusammenhang mit der Fähigkeit der Clusterobjekte, Daten bereitzustellen. Kapazitätsprobleme stehen im Zusammenhang mit der Fähigkeit der Clusterobjekte, Daten zu speichern.

Sie können auf das Diagramm eines Objekts klicken, um eine gefilterte Liste der Objekte anzuzeigen. Beispielsweise können Sie auf das SVM Kapazitätsdiagramm klicken, das Warnungen anzeigt, um eine gefilterte Liste der SVMs anzuzeigen. Diese Liste enthält SVMs mit Volumes oder qtrees, die Kapazitätsprobleme mit dem Schweregrad Level Warning aufweisen. Sie können auch auf das SVM Verfügbarkeitsdiagramm klicken, das Warnungen anzeigt, um die Liste der SVMs anzuzeigen, die Verfügbarkeitsprobleme mit dem Schweregrad Level Warning haben.

Verfügbarkeitsprobleme

Die Grafik zeigt die Gesamtzahl der Objekte an, einschließlich Objekten mit Verfügbarkeitsproblemen und Objekten ohne Verfügbarkeitsprobleme. Die Farben im Diagramm stehen für die unterschiedlichen Schweregrade der Probleme. Die Informationen unterhalb des Diagramms liefern Details zu Verfügbarkeitsproblemen, die die Datenverfügbarkeit im Cluster beeinträchtigen können oder bereits beeinträchtigt haben. Beispielsweise werden Informationen über ausgefallene Disk Shelves und offline befindliche Aggregate angezeigt.

Die im SFO-Balkendiagramm angezeigten Daten basieren auf dem HA-Status der Knoten. Die

für alle anderen Balkendiagramme angezeigten Daten werden anhand der generierten Ereignisse berechnet.

Kapazitätsprobleme

Die Grafik zeigt die Gesamtzahl der Objekte an, einschließlich der Objekte mit Kapazitätsproblemen und der Objekte ohne kapazitätsbezogene Probleme. Die Farben im Diagramm stehen für die unterschiedlichen Schweregrade der Probleme. Die Informationen unterhalb des Diagramms liefern Details zu Kapazitätsproblemen, die sich auf die Datenkapazität im Cluster auswirken können oder bereits ausgewirkt haben. Beispielsweise werden Informationen zu Aggregaten angezeigt, die die festgelegten Schwellenwerte voraussichtlich überschreiten.

Registerkarte Kapazität

Zeigt detaillierte Informationen zur Kapazität des ausgewählten Clusters an.

Kapazität

Anzeige des Datenkapazitätsdiagramms zur genutzten und verfügbaren Kapazität aller zugewiesenen Aggregate:

- Belegter logischer Speicherplatz

  Die tatsächliche Größe der auf allen Aggregaten dieses Clusters gespeicherten Daten ohne Berücksichtigung der Einsparungen durch die Verwendung von ONTAP Storage-Effizienztechnologien. Dies schließt Snapshot Kopien nicht ein.

- Datenreduktion

  Zeigt das Verhältnis ohne Snapshot-Kopien und mit zwei signifikanten Stellen an, zum Beispiel 1,8 zu 1. Dieses Verhältnis basiert auf den konfigurierten ONTAP Storage-Effizienzeinstellungen.

- Gebraucht

  Die physische Kapazität, die von den Daten aller Aggregate genutzt wird. Dies umfasst nicht die Kapazität, die für Parität, richtiges Sizing und Reservierung verwendet wird.

- Verfügbar

  Zeigt die verfügbare Datenkapazität an.

- Ersatzteile

  Zeigt die in allen Ersatzfestplatten für Storage noch verfügbare Kapazität an.

- Bereitgestellt

  Zeigt die für alle zugrunde liegenden Volumes bereitgestellte Kapazität an.

Details

Zeigt detaillierte Informationen zur genutzten und verfügbaren Kapazität an. Die Berechnung schließt die Daten des Root-Aggregats aus.

- Gesamtkapazität

Zeigt die Gesamtkapazität des Clusters an. Dies schließt die für Parität zugewiesene Kapazität nicht ein.

- Gebraucht

  Zeigt die von Daten genutzte Kapazität an. Die für Parität, richtiges Sizing und Reservierung verwendete Kapazität ist hier nicht enthalten.

- Verfügbar

  Zeigt die verfügbare Datenkapazität an.

- Bereitgestellt

  Zeigt die für alle zugrunde liegenden Volumes bereitgestellte Kapazität an.

- Ersatzteile

  Zeigt die in allen Ersatzfestplatten für Storage noch verfügbare Kapazität an.

Cloud-Tier

Zeigt die insgesamt verwendete Cloud-Tier-Kapazität sowie die für jedes verbundene Cloud-Tier verwendete Kapazität für FabricPool aktivierte Aggregate im Cluster an. Ein FabricPool kann lizenziert oder nicht lizenziert sein.

Aufschlüsselung der physikalischen Kapazität nach Festplattentyp

Der Bereich „Aufschlüsselung der physischen Kapazität nach Festplattentyp“ zeigt detaillierte Informationen zur Festplattenkapazität der verschiedenen Festplattentypen im Cluster an. Wenn Sie auf den Festplattentyp klicken, können Sie auf der Registerkarte „Festplatten“ weitere Informationen dazu anzeigen.

- Gesamtnutzkapazität

  Zeigt die verfügbare Kapazität und die Reservekapazität der Datenfestplatten an.

- HDD

  Die Grafik zeigt die belegte und die verfügbare Kapazität aller HDD-Datenfestplatten im Cluster an. Die gestrichelte Linie stellt die Spare-Kapazität der Datenfestplatten in der HDD dar.

- Flash
  - SSD Data

    Grafische Darstellung der belegten und der verfügbaren Kapazität der SSD-Datenträger im Cluster.

  - SSD-Cache

    Zeigt grafisch die noch verfügbare Kapazität der SSD-Cache-Festplatten im Cluster an.

  - SSD-Spare

    Zeigt grafisch die freie Kapazität der SSD-, Daten- und Cache-Festplatten im Cluster an.

- Nicht zugewiesene Datenträger

Zeigt die Anzahl der nicht zugewiesenen Datenträger im Cluster an.

Liste der Aggregate mit Kapazitätsproblemen

Tabellarische Anzeige von Details zur genutzten und verfügbaren Kapazität der Aggregate mit Kapazitätsrisiken.

- Status

  Weist darauf hin, dass das Aggregat ein kapazitätsbezogenes Problem eines bestimmten Schweregrads aufweist.

  Sie können den Mauszeiger über den Status bewegen, um weitere Informationen zu den für das Aggregat generierten Ereignissen anzuzeigen.

  Wenn der Status des Aggregats durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, Datum und Uhrzeit der Auslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses einsehen. Über die Schaltfläche **View Details** können Sie weitere Informationen zum Ereignis einsehen.

  Wenn der Status des Aggregats durch mehrere Ereignisse desselben Schweregrads bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum, zu denen die Ereignisse ausgelöst werden, sowie dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Weitere Details zu jedem dieser Ereignisse sind durch Klicken auf den Ereignisnamen verfügbar. Über den Link **View All Events** kann die Liste der generierten Ereignisse angezeigt werden.

  > Ein Aggregat kann mehrere kapazitätsbezogene Ereignisse mit demselben Schweregrad oder mit unterschiedlichen Schweregraden aufweisen. Es wird jedoch nur der höchste Schweregrad angezeigt. Wenn ein Aggregat beispielsweise zwei Ereignisse mit den Schweregraden „Fehler“ und „Kritisch“ aufweist, wird nur der Schweregrad „Kritisch“ angezeigt.

- Aggregat

  Zeigt den Namen des Aggregats an.

- Genutzte Datenkapazität

  Zeigt grafisch Informationen zur Kapazitätsauslastung des Aggregats (in Prozent) an.

- Tage bis voll

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bis das Aggregat seine volle Kapazität erreicht.

Registerkarte „Konfiguration“

Details zum ausgewählten Cluster, z. B. IP-Adresse, Kontakt und Standort:

Clusterübersicht

- Verwaltungsschnittstelle

  Zeigt die Cluster-Management-LIF an, die Unified Manager zum Herstellen der Verbindung mit dem Cluster verwendet. Der Betriebsstatus der Schnittstelle wird ebenfalls angezeigt.

- Hostname oder IP-Adresse

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Cluster-Management-LIF an, den Unified Manager zur Verbindung mit dem Cluster verwendet.

- FQDN

  Zeigt die vollqualifizierte Domain (FQDN) des Clusters an.

- Betriebssystemversion

  Zeigt die ONTAP Version an, die im Cluster ausgeführt wird. Wenn auf den Knoten im Cluster unterschiedliche Versionen von ONTAP ausgeführt werden, wird die älteste ONTAP Version angezeigt.

- Kontakt

  Zeigt Details zu dem Administrator an, den Sie bei Problemen mit dem Cluster kontaktieren sollten.

- Standort

  Zeigt den Standort des Clusters an.

- Persönlichkeit

  Gibt an, ob es sich um einen als All SAN Array konfigurierten Cluster handelt.

Übersicht über den Remote-Cluster

Enthält Details zum Remote-Cluster in einer MetroCluster Konfiguration. Diese Informationen werden nur für MetroCluster Konfigurationen angezeigt.

- Cluster

  Zeigt den Namen des Remote-Clusters an. Durch Klicken auf den Clusternamen gelangen Sie zur Detailseite des Clusters.

- Hostname oder IP-Adresse

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Remote-Clusters an.

- Standort

  Zeigt den Standort des Remote-Clusters an.

MetroCluster Überblick

Enthält Details zum lokalen Cluster in MetroCluster over FC oder MetroCluster over IP Konfigurationen. Diese Informationen werden nur für MetroCluster over FC oder IP Konfigurationen angezeigt.

- Typ

  Zeigt an, ob der Typ MetroCluster aus zwei oder vier Knoten besteht. Für MetroCluster over IP wird nur die Variante mit vier Knoten unterstützt.

- Konfiguration

Zeigt die MetroCluster Konfiguration über FC und IP an, die folgende Werte annehmen kann:

Für FC

- Stretch Konfiguration mit SAS-Kabeln
- Stretch Konfiguration mit FC-SAS Bridge
- Fabric Konfiguration mit FC Switches

> Für ein MetroCluster mit vier Knoten wird nur die Fabric-Konfiguration mit FC-Switches unterstützt.

Für IP

- IP-Konfiguration mit Ethernet-Switches (L2 oder L3, je nach Konfiguration des Clusters)
  - Automatische ungeplante Umschaltung (AUSO)

    Zeigt an, ob die automatische ungeplante Umschaltung (AUSO) für den lokalen Cluster aktiviert ist. Standardmäßig ist AUSO für alle Cluster in einer Zwei-Knoten MetroCluster Konfiguration in Unified Manager aktiviert. Sie können die AUSO-Einstellung über die Befehlszeilenschnittstelle ändern. Dies wird nur für MetroCluster over FC unterstützt.

  - Umschaltmodus

    Zeigt den Umschaltmodus für die MetroCluster over IP Konfiguration an. Die verfügbaren Werte sind: `Active`, `Negotiated Switchover` und `Automatic Unplanned Switchover`.

Nodes

- Verfügbarkeit

  Zeigt die Anzahl der Knoten an, die im Cluster betriebsbereit (●) oder ausgefallen (●) sind.

- Betriebssystemversionen

  Zeigt die ONTAP Versionen an, die auf den Knoten ausgeführt werden, sowie die Anzahl der Knoten, auf denen eine bestimmte Version von ONTAP ausgeführt wird. Beispielsweise gibt 9.6 (2), 9.3 (1) an, dass zwei Knoten ONTAP 9.6 und ein Knoten ONTAP 9.3 ausführen.

Storage Virtual Machines

- Verfügbarkeit

  Zeigt die Anzahl der SVMs an, die im Cluster aktiv (●) oder inaktiv (●) sind.

Netzwerkschnittstellen

- Verfügbarkeit

  Zeigt die Anzahl der Nicht-Daten-LIFs an, die im Cluster aktiv (●) oder inaktiv (●) sind.

- Cluster-Management-Schnittstellen

  Zeigt die Anzahl der Cluster-Management-LIFs an.

- Knotenverwaltungsschnittstellen

  Zeigt die Anzahl der Knotenverwaltungs-LIFs an.

- Cluster-Schnittstellen

  Zeigt die Anzahl der Cluster-LIFs an.

- Intercluster-Schnittstellen

  Zeigt die Anzahl der Intercluster-LIFs an.

Protokolle

- Datenprotokolle

  Zeigt die Liste der für den Cluster aktivierten lizenzierten Datenprotokolle an. Zu den Datenprotokollen gehören iSCSI, CIFS, NFS, NVMe und FC/FCoE.

Schutz

- Mediatoren

  Zeigt an, ob der Cluster Mediatoren unterstützt und wie der Verbindungsstatus des Mediators ist. Es zeigt an, ob der Mediator konfiguriert ist, und falls ja, den Status der Mediatoren.

  - Nicht zutreffend

    Wird angezeigt, wenn der Cluster keine Mediatoren unterstützt.

  - Nicht konfiguriert

    Wird angezeigt, wenn der Cluster Mediatoren unterstützt, der Mediator aber nicht konfiguriert ist.

  - IP-Adresse

    Wird angezeigt, wenn der Cluster Mediatoren unterstützt und der Mediator konfiguriert ist. Der Mediatorstatus wird durch Farben angegeben. Die Farbe Grün zeigt an, dass der Mediatorstatus erreichbar ist. Die Farbe Rot zeigt an, dass der Mediatorstatus nicht erreichbar ist.

Cloud-Tiers

Listet die Namen der Cloud-Ebenen auf, mit denen dieser Cluster verbunden ist. Außerdem werden der Typ (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage oder StorageGRID) und der Status der Cloud-Ebenen (Verfügbar oder Nicht verfügbar) aufgeführt.

MetroCluster Registerkarte „Konnektivität“

Zeigt die Probleme und den Verbindungsstatus der Clusterkomponenten in der MetroCluster over FC Konfiguration an. Ein Cluster wird in einem roten Rahmen angezeigt, wenn der Disaster-Recovery-Partner des Clusters Probleme aufweist.

Die Registerkarte „Konnektivität“ für MetroCluster wird nur für Cluster angezeigt, die in einer MetroCluster over FC Konfiguration vorliegen.

Sie können zur Detailseite eines Remote-Clusters navigieren, indem Sie auf den Namen des Remote-Clusters klicken. Sie können die Details der Komponenten auch anzeigen, indem Sie auf den Anzahl-Link einer Komponente klicken. Wenn Sie beispielsweise auf den Anzahl-Link des Knotens im Cluster klicken, wird auf der Detailseite des Clusters die Registerkarte „Knoten“ angezeigt. Wenn Sie auf den Anzahl-Link der Festplatten im Remote-Cluster klicken, wird auf der Detailseite des Remote-Clusters die Registerkarte „Festplatten“ angezeigt.



Bei der Verwaltung einer MetroCluster Konfiguration mit acht Knoten werden durch Klicken auf den Link „Anzahl“ der Komponente „Disk Shelves“ nur die lokalen Shelves des standardmäßigen HA-Paares angezeigt. Es gibt keine Möglichkeit, die lokalen Shelves des anderen HA-Paares anzuzeigen.

Sie können den Mauszeiger über die Komponenten bewegen, um die Details und den Verbindungsstatus der Cluster bei Problemen anzuzeigen und weitere Informationen zu den Ereignissen anzuzeigen, die für das Problem generiert wurden.

Wenn der Status des Verbindungsproblems zwischen Komponenten durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, Datum und Uhrzeit der Auslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses einsehen. Die Schaltfläche View Details bietet weitere Informationen zum Ereignis.

Wird der Status des Verbindungsproblems zwischen Komponenten durch mehrere Ereignisse mit demselben Schweregrad bestimmt, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, dem Zeitpunkt und Datum der Auslösung der Ereignisse sowie dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Weitere Details zu jedem dieser Ereignisse lassen sich durch Klicken auf den Ereignisnamen anzeigen. Über den Link **View All Events** lässt sich die Liste der generierten Ereignisse anzeigen.

MetroCluster Registerkarte „Replikation“

Zeigt den Status der Daten an, die in einer MetroCluster over FC Konfiguration repliziert werden. Mit der Registerkarte MetroCluster Replikation lässt sich der Datenschutz sicherstellen, indem die Daten synchron mit den bereits per Peering verbundenen Clustern gespiegelt werden. Ein Cluster erscheint mit roter Umrandung, wenn der Disaster-Recovery-Partner des Clusters Probleme hat.



Die Registerkarte „Replikation“ MetroCluster wird nur für Cluster angezeigt, die sich in einer MetroCluster over FC Konfiguration befinden.

In einer MetroCluster Umgebung können Sie diese Registerkarte verwenden, um die logischen Verbindungen und das Peering des lokalen Clusters mit dem Remote Cluster zu überprüfen. Sie können die objektive Darstellung der Clusterkomponenten mit ihren logischen Verbindungen anzeigen. Dies hilft dabei, Probleme zu identifizieren, die bei der Spiegelung von Metadaten und Daten auftreten können.

Auf der Registerkarte MetroCluster Replikation bietet Lokaler Cluster die detaillierte grafische Darstellung des ausgewählten Clusters, während sich MetroCluster Partner auf den Remote-Cluster bezieht.

Registerkarte „Netzwerkschnittstellen“

Details zu allen Nicht-Daten-LIFs, die auf dem ausgewählten Cluster erstellt wurden.

Netzwerkschnittstelle

Zeigt den Namen der LIF an, die auf dem ausgewählten Cluster erstellt wird.

Betriebsstatus

Zeigt den Betriebsstatus der Schnittstelle an, der Up(), Down() oder Unknown() sein kann. Der Betriebsstatus einer Netzwerkschnittstelle wird durch den Status ihrer physischen Ports bestimmt.

Administrativer Status

Zeigt den administrativen Status der Schnittstelle an, der Up (), Down () oder Unknown () sein kann. Sie können den administrativen Status einer Schnittstelle bei Konfigurationsänderungen oder während Wartungsarbeiten steuern. Der administrative Status kann sich vom Betriebsstatus unterscheiden. Ist der administrative Status einer LIF jedoch Down, ist der Betriebsstatus standardmäßig ebenfalls Down.

IP-Adresse

Zeigt die IP-Adresse der Schnittstelle an.

Rolle

Zeigt die Rolle der Schnittstelle an. Mögliche Rollen sind Cluster-Management-LIFs, Knoten-Management-LIFs, Cluster-LIFs und Intercluster-LIFs.

Home-Port

Zeigt den physischen Port an, dem die Schnittstelle ursprünglich zugeordnet war.

Aktueller Port

Zeigt den physischen Port an, dem die Schnittstelle aktuell zugeordnet ist. Nach der LIF-Migration kann der aktuelle Port vom Home-Port abweichen.

Failover-Richtlinie

Zeigt die für die Schnittstelle konfigurierte Failover-Richtlinie an.

Routinggruppen

Zeigt den Namen der Routing-Gruppe an. Über den Namen der Routing-Gruppe lassen sich weitere Informationen zu den Routen und dem Ziel-Gateway anzeigen.

Routing-Gruppen werden für ONTAP 8.3 oder höher nicht unterstützt, daher wird für diese Cluster eine leere Spalte angezeigt.

Failover-Gruppe

Zeigt den Namen der Failover-Gruppe an.

Registerkarte Knoten

Zeigt Informationen zu den Knoten im ausgewählten Cluster an. Detaillierte Informationen zu den HA-Paaren, Disk Shelves und Ports können angezeigt werden:

HA-Details

Bietet eine grafische Darstellung des HA-Zustands und des Systemstatus der Knoten im HA-Paar. Der Systemstatus des Knotens wird durch die folgenden Farben angezeigt:

- **Grün**

  Der Knoten ist funktionsfähig.

- **Gelb**

  Der Knoten hat den Partnerknoten übernommen oder der Knoten weist Umgebungsprobleme auf.

- **Rot**

  Der Knoten ist ausgefallen.

Informationen zur Verfügbarkeit des HA-Paars können eingesehen und die erforderlichen Maßnahmen zur Vermeidung von Risiken ergriffen werden. Zum Beispiel wird im Fall eines möglichen Takeover-Vorgangs die folgende Meldung angezeigt: Storage failover possible.

Sie können eine Liste der Ereignisse im Zusammenhang mit dem HA-Paar und seiner Umgebung anzeigen, z. B. Lüfter, Netzteile, NVRAM-Batterie, Flash-Karten, Service Processor und die Konnektivität der Disk Shelves. Außerdem können Sie den Zeitpunkt anzeigen, zu dem die Ereignisse ausgelöst wurden.

Sie können weitere knotenbezogene Informationen, wie zum Beispiel die Modellnummer, anzeigen.

Bei Single-Node-Clustern können Sie auch Details zu den Knoten anzeigen.

Festplatten Shelves

Anzeige von Informationen über die Shelves im HA-Paar.

Sie können auch die für die Disk Shelves und die Umgebungskomponenten generierten Ereignisse sowie den Zeitpunkt anzeigen, zu dem die Ereignisse ausgelöst wurden.

- **Shelf-ID**

  Zeigt die ID des Shelf an, in dem sich die Disk befindet.

- **Komponentenstatus**

  Es werden Umgebungsdetails der Shelves angezeigt, z. B. Netzteile, Lüfter, Temperatursensoren, Stromsensoren, Festplattenkonnektivität und Spannungssensoren. Die Umgebungsdetails werden als Symbole in den folgenden Farben dargestellt:

  - **Grün**

    Die Umweltkomponenten funktionieren ordnungsgemäß.

  - **Grau**

    Für die Umgebungskomponenten liegen keine Daten vor.

  - **Rot**

    Einige der Umgebungskomponenten sind ausgefallen.

- **Zustand**

  Zeigt den Status des Disk Shelf an. Die möglichen Zustände sind Offline, Online, Kein Status,

Initialisierung erforderlich, Fehlend und Unbekannt.

- **Modell**

  Zeigt die Modellnummer des Shelf an.

- **Lokales Disk Shelf**

  Gibt an, ob sich das Disk Shelf im lokalen Cluster oder im Remote Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster Konfiguration angezeigt.

- **Einzigartige ID**

  Zeigt die eindeutige Kennung des Disk Shelf an.

- **Firmware-Version**

  Zeigt die Firmware-Version des Disk Shelf an.

Ports

Zeigt Informationen zu den zugehörigen FC-, FCoE- und Ethernet-Ports an. Details zu den Ports und den zugehörigen LIFs sind nach einem Klick auf die Port-Symbole verfügbar.

Auch die für die Ports generierten Ereignisse können angezeigt werden.

Sie können die folgenden Port-Details einsehen:

- Port-ID

  Zeigt den Namen des Ports an. Beispielsweise können die Portnamen e0M, e0a und e0b lauten.

- Rolle

  Zeigt die Rolle des Ports an. Die möglichen Rollen sind Cluster, Data, Intercluster, Node-Management und Undefined.

- Typ

  Zeigt das für den Port verwendete physikalische Protokoll an. Mögliche Typen sind Ethernet, Fibre Channel und FCoE.

- WWPN

  Zeigt den World Wide Port Name (WWPN) des Ports an.

- Firmware-Rev.

  Zeigt die Firmware-Revision des FC/FCoE-Ports an.

- Status

  Zeigt den aktuellen Status des Ports an. Mögliche Zustände sind Aktiv, Inaktiv, Link nicht verbunden oder Unbekannt ( ).

  Die portbezogenen Ereignisse können Sie in der Ereignisliste einsehen. Außerdem können Sie die

zugehörigen LIF-Details anzeigen, wie z. B. LIF-Name, Betriebsstatus, IP-Adresse oder WWPN, Protokolle, Name der dem LIF zugeordneten SVM, aktueller Port, Failover-Richtlinie und Failover-Gruppe.

Registerkarte „Datenträger“

Zeigt Details zu den Datenträgern im ausgewählten Cluster an. Es werden datenträgerbezogene Informationen wie die Anzahl der verwendeten, Ersatz-, defekten und nicht zugewiesenen Datenträger angezeigt. Außerdem werden weitere Details wie der Datenträgername, der Datenträgertyp und der Eigentümerknoten des Datenträgers angezeigt.

Zusammenfassung des Datenträgerpools

Die Anzahl der Datenträger, die nach effektiven Typen (FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN und VMDISK) kategorisiert sind, sowie der Status der Datenträger werden angezeigt. Außerdem können weitere Details angezeigt werden, z. B. die Anzahl der Aggregate, gemeinsam genutzten Datenträger, Ersatzdatenträger, defekten Datenträger, nicht zugewiesenen Datenträger und nicht unterstützten Datenträger. Beim Klicken auf den Link zur Anzahl des effektiven Datenträgertyps werden Datenträger mit dem ausgewählten Status und effektiven Typ angezeigt. Wenn beispielsweise auf den Zähllink für den Datenträgerstatus „Defekt“ und den effektiven Typ „SAS“ geklickt wird, werden alle Datenträger mit dem Datenträgerstatus „Defekt“ und dem effektiven Typ „SAS“ angezeigt.

Festplatte

Zeigt den Namen des Datenträgers an.

RAID-Gruppen

Zeigt den Namen der RAID-Gruppe an.

Eigentümerknoten

Zeigt den Namen des Knotens an, zu dem die Festplatte gehört. Wenn die Festplatte nicht zugewiesen ist, wird in dieser Spalte kein Wert angezeigt.

Status

Zeigt den Status der Festplatte an: Aggregate, Shared, Spare, Broken, Unassigned, Unsupported oder Unknown. Standardmäßig ist diese Spalte so sortiert, dass die Status in der folgenden Reihenfolge angezeigt werden: Broken, Unassigned, Unsupported, Spare, Aggregate und Shared.

Lokale Festplatte

Zeigt entweder „Ja“ oder „Nein“ an, um anzugeben, ob sich die Festplatte im lokalen oder im Remote-Cluster befindet. Diese Spalte ist nur für Cluster in einer MetroCluster Konfiguration sichtbar.

Position

Zeigt die Position der Festplatte basierend auf ihrem Containertyp an, z. B. Kopie, Daten oder Parität. Diese Spalte ist standardmäßig ausgeblendet.

Betroffene Aggregate

Zeigt die Anzahl der aufgrund des Festplattenausfalls betroffenen Aggregate an. Durch Bewegen des Mauszeigers über den Anzahllink werden die betroffenen Aggregate angezeigt; durch Klicken auf den

Aggregatnamen werden Details zum Aggregat angezeigt. Auch durch Klicken auf die Aggregatanzahl lässt sich die Liste der betroffenen Aggregate in der Ansicht „Systemstatus: Alle Aggregate“ anzeigen.

In dieser Spalte wird für die folgenden Fälle kein Wert angezeigt:

- Bei defekten Festplatten, wenn ein Cluster mit solchen Festplatten zu Unified Manager hinzugefügt wird
- Wenn keine Festplatten ausgefallen sind

Speicherpool

Zeigt den Namen des Storage Pools an, zu dem die SSD gehört. Wenn sich der Mauszeiger über dem Namen des Storage Pools befindet, sind Details des Storage Pools sichtbar.

Speicherkapazität

Zeigt die verfügbare Festplattenkapazität an.

Rohkapazität

Zeigt die Kapazität der unformatierten Festplatte vor dem richtigen Sizing und der RAID-Konfiguration an. Diese Spalte ist standardmäßig ausgeblendet.

Typ

Zeigt die Festplattentypen an: zum Beispiel ATA, SATA, FCAL oder VMDISK.

Effektiver Typ

Zeigt den von ONTAP zugewiesenen Festplattentyp an.

Bestimmte ONTAP Festplattentypen werden für die Erstellung und das Hinzufügen von Aggregaten sowie für die Ersatzplattenverwaltung als gleichwertig betrachtet. ONTAP weist jedem Festplattentyp einen effektiven Festplattentyp zu.

Verbrauchte Reserveblöcke %

Zeigt den prozentualen Anteil der verbrauchten Reserveblöcke auf der SSD an. Diese Spalte ist für andere Datenträger als SSDs leer.

Genutzte Nennlebensdauer %

Zeigt in Prozent eine Schätzung der verbrauchten SSD-Lebensdauer an, basierend auf der tatsächlichen SSD-Nutzung und der Prognose des Herstellers zur SSD-Lebensdauer. Ein Wert größer als 99 zeigt an, dass die geschätzte Lebensdauer verbraucht wurde, weist jedoch möglicherweise nicht auf einen SSD-Ausfall hin. Ist der Wert unbekannt, wird die Festplatte ausgelassen.

Firmware

Zeigt die Firmware-Version der Festplatte an.

RPM

Zeigt die Drehzahl der Festplatte in Umdrehungen pro Minute (RPM) an. Diese Spalte ist standardmäßig ausgeblendet.

Modell

Zeigt die Modellnummer der Festplatte an. Diese Spalte ist standardmäßig ausgeblendet.

Anbieter

Zeigt den Namen des Festplattenherstellers an. Diese Spalte ist standardmäßig ausgeblendet.

Shelf-ID

Zeigt die ID des Shelf an, in dem sich die Disk befindet.

Einschub

Zeigt die ID des Laufwerksschachts an, in dem sich die Festplatte befindet.

Bereich „Verwandte Anmerkungen“

Ermöglicht die Anzeige der dem ausgewählten Cluster zugeordneten Annotationsdetails. Diese Details umfassen den Annotationsnamen und die auf den Cluster angewendeten Annotationswerte. Außerdem lassen sich manuelle Annotationen im Bereich „Zugehörige Annotationen“ entfernen.

Bereich „Verwandte Geräte“

Ermöglicht die Anzeige von Gerätedetails, die dem ausgewählten Cluster zugeordnet sind.

Die Details umfassen Eigenschaften des mit dem Cluster verbundenen Geräts, wie Gerätetyp, Größe, Anzahl und Systemstatus. Über den Link für die Anzahl sind weitere Analysen zu diesem Gerät möglich.

Im Bereich MetroCluster Partner erhalten Sie die Anzahl sowie Details zum entfernten MetroCluster Partner zusammen mit den zugehörigen Clusterkomponenten wie Knoten, Aggregaten und SVMs. Der Bereich MetroCluster Partner wird nur für Cluster in einer MetroCluster Konfiguration angezeigt.

Im Bereich „Verwandte Geräte“ können Sie die Knoten, SVMs und Aggregate anzeigen und zu diesen navigieren, die mit dem Cluster verknüpft sind:

MetroCluster Partner

Zeigt den Systemstatus des MetroCluster Partners an. Mithilfe des Count-Links lassen sich weitere Informationen zum Systemstatus und zur Kapazität der Clusterkomponenten aufrufen.

Nodes

Zeigt die Anzahl, Kapazität und den Systemstatus der Knoten an, die zum ausgewählten Cluster gehören. Die Kapazität gibt die gesamte nutzbare Kapazität im Verhältnis zur verfügbaren Kapazität an.

Storage Virtual Machines

Zeigt die Anzahl der SVMs an, die zum ausgewählten Cluster gehören.

Aggregate

Zeigt die Anzahl, die Kapazität und den Systemstatus der Aggregate an, die zum ausgewählten Cluster gehören.

Bereich „Verwandte Gruppen“

Ermöglicht Ihnen die Anzeige der Liste der Gruppen, die den ausgewählten Cluster enthalten.

Bereich „Zugehörige Warnungen“

Im Bereich „Zugehörige Warnungen“ können Sie die Liste der Warnungen für den ausgewählten Cluster anzeigen. Sie können außerdem eine Warnung hinzufügen, indem Sie auf den Link „Warnung hinzufügen“ klicken, oder eine vorhandene Warnung bearbeiten, indem Sie auf den Warnungsnamen klicken.

Verwandte Informationen

"Seite „Volumes“" "Anzeigen der Clusterliste und Details"

Die Seite „Aggregat-/Zustandsdetails“ in Active IQ Unified Manager

Auf der Seite „Aggregat-/Statusdetails“ können Sie detaillierte Informationen zum ausgewählten Aggregat anzeigen, z. B. Kapazität, Festplatteninformationen, Konfigurationsdetails und generierte Ereignisse. Außerdem können Sie Informationen zu den zugehörigen Objekten und zugehörigen Warnungen für dieses Aggregat anzeigen.

Befehlsschaltflächen

> Bei der Überwachung eines mit FabricPool aktivierten Aggregats beziehen sich die auf dieser Seite angezeigten zugesicherten und überprovisionierten Werte ausschließlich auf die Kapazität der lokalen bzw. Performance-Ebene. Der in der Cloud-Ebene verfügbare Speicherplatz wird in den überprovisionierten Werten nicht berücksichtigt. Ebenso beziehen sich die Schwellenwerte des Aggregats nur auf die lokale Performance-Ebene.

Mithilfe der Befehlsschaltflächen können Sie die folgenden Aufgaben für das ausgewählte Aggregat ausführen:

- **Zur Performance Ansicht wechseln**

  Ermöglicht die Navigation zur Seite „Aggregate/Performance-Details“.

- **Aktionen**
  - Benachrichtigung hinzufügen

    Ermöglicht es Ihnen, dem ausgewählten Aggregat eine Warnung hinzuzufügen.

  - Bearbeiten von Schwellenwerten

    Damit können Sie die Schwellenwerteinstellungen für das ausgewählte Aggregat ändern.

- **Aggregate anzeigen**

  Ermöglicht die Navigation zur Ansicht „Gesundheit: Alle Aggregate“.

Registerkarte Kapazität

Die Registerkarte „Kapazität“ zeigt detaillierte Informationen zum ausgewählten Aggregat an, wie z. B. dessen Kapazität, Schwellenwerte und tägliche Wachstumsrate.

Standardmäßig werden keine Kapazitätsereignisse für Root-Aggregate generiert. Auch die vom Unified

Manager verwendeten Schwellenwerte gelten nicht für Node Root-Aggregate. Nur ein Mitarbeiter des technischen Supports kann die Einstellungen für die Generierung dieser Ereignisse ändern. Wenn die Einstellungen von einem Mitarbeiter des technischen Supports geändert werden, werden die Schwellenwerte auf das Node Root-Aggregat angewendet.

- **Kapazität**

  Zeigt das Datenkapazitätsdiagramm und das Diagramm der Snapshot-Kopien mit Kapazitätsdetails zum Aggregat an:

  - Belegter logischer Speicherplatz

    Die tatsächliche Größe der auf dem Aggregat gespeicherten Daten ohne Berücksichtigung der Einsparungen durch den Einsatz von ONTAP Storage-Effizienztechnologien.

  - Gebraucht

    Die von Daten im Aggregat genutzte physische Kapazität.

  - Überprovisioniert

    Wenn der Speicherplatz im Aggregat überprovisioniert ist, zeigt das Diagramm eine Kennzeichnung mit dem Umfang der Überprovisionierung an.

  - Warnung

    An der Position des Warnschwellenwerts wird eine gestrichelte Linie angezeigt; das bedeutet, dass der Speicherplatz im Aggregat nahezu voll ist. Bei Überschreitung dieses Schwellenwerts wird das Ereignis „Space Nearly Full“ generiert.

  - Fehler

    Zeigt an der Position, an der der Fehlerschwellenwert festgelegt ist, eine durchgezogene Linie an; dies bedeutet, dass der Speicherplatz im Aggregat voll ist. Wenn dieser Schwellenwert überschritten wird, wird das Ereignis „Space Full“ generiert.

  - Diagramm zu Snapshot-Kopien

    Dieses Diagramm wird nur angezeigt, wenn die genutzte Snapshot-Kapazität oder die Snapshot-Reserve nicht null ist.

  Beide Diagramme zeigen die Kapazität, um die die Snapshot Kapazität die Snapshot Reserve übersteigt, wenn die verwendete Snapshot Kapazität die Snapshot Reserve übersteigt.

- **Cloud-Tier**

  Zeigt den von Daten in der Cloud-Ebene für FabricPool aktivierte Aggregate belegten Speicherplatz an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

  Wenn das Cloud-Tier auf einen anderen Cloud-Provider gespiegelt wird (das „`mirror tier`“), werden beide Cloud-Tiers hier angezeigt.

- **Details**

  Zeigt detaillierte Informationen zur Kapazität an.

◦ Gesamtkapazität

Zeigt die Gesamtkapazität im Aggregat an.

◦ Datenkapazität

Zeigt die vom Aggregat verwendete Kapazität (genutzte Kapazität) und die im Aggregat verfügbare Kapazität (freie Kapazität) an.

◦ Snapshot Reserve

Zeigt die belegte und freie Snapshot Kapazität des Aggregats an.

◦ Überprovisionierte Kapazität

Zeigt die Überprovisionierung des Aggregats an. Die Überprovisionierung des Aggregats ermöglicht es, mehr Storage bereitzustellen, als in einem bestimmten Aggregat tatsächlich verfügbar ist, solange nicht der gesamte Storage aktuell genutzt wird. Bei Verwendung von Thin Provisioning kann die Gesamtgröße der Volumes im Aggregat die Gesamtkapazität des Aggregats überschreiten.



Wenn Sie Ihr Aggregat überprovisioniert haben, müssen Sie den verfügbaren Speicherplatz sorgfältig überwachen und bei Bedarf Storage hinzufügen, um Schreibfehler aufgrund unzureichenden Speicherplatzes zu vermeiden.

◦ Cloud-Tier

Zeigt den von Daten in der Cloud-Ebene für FabricPool aktivierte Aggregate belegten Speicherplatz an. Ein FabricPool kann lizenziert oder unlizenziert sein. Wenn die Cloud-Ebene auf einen anderen Cloud-Anbieter gespiegelt wird (die Spiegel-Ebene), werden hier beide Cloud-Ebenen angezeigt.

◦ Gesamter Cache-Speicherplatz

Zeigt den gesamten Speicherplatz der SSDs oder Zuordnungseinheiten an, die einem Flash Pool Aggregat hinzugefügt wurden. Wenn Sie Flash Pool für ein Aggregat aktiviert, aber keine SSDs hinzugefügt haben, wird der Cache-Speicherplatz mit 0 KB angezeigt.



Dieses Feld ist ausgeblendet, wenn Flash Pool für ein Aggregat deaktiviert ist.

◦ Aggregat-Schwellenwerte

Zeigt die folgenden Kapazitätsschwellenwerte des Aggregats an:

- Schwellenwert für nahezu voll

  Gibt den Prozentsatz an, bei dem ein Aggregat nahezu voll ist.

- Schwellenwert für voll

  Gibt den Prozentsatz an, bei dem ein Aggregat voll ist.

- Schwellenwert für nahezu erreichte Überprovisionierung

  Gibt den Prozentsatz an, bei dem ein Aggregat nahezu überprovisioniert ist.

        - Schwellenwert für Überprovisionierung

          Gibt den Prozentsatz an, bei dem ein Aggregat überprovisioniert ist.

    - Weitere Details: Tägliche Wachstumsrate

      Zeigt den im Aggregat belegten Speicherplatz an, wenn die Änderungsrate zwischen den letzten beiden Messwerten 24 Stunden lang anhält.

      Wenn beispielsweise ein Aggregat um 14 Uhr 10 GB Speicherplatz und um 18 Uhr 12 GB belegt, beträgt die tägliche Wachstumsrate (GB) für dieses Aggregat 2 GB.

    - Volume Move

      Anzeige der Anzahl der aktuell laufenden Volume-Verschiebungsvorgänge:

        - Ausgehende Volumes

          Zeigt die Anzahl und Kapazität der Volumes an, die aus dem Aggregat verschoben werden.

      Über den Link lassen sich weitere Details anzeigen, wie zum Beispiel der Name des Volumes, das Aggregat, in das das Volume verschoben wird, der Status des Volume-Verschiebungsvorgangs und die voraussichtliche Endzeit.

        - Volumes in

          Zeigt die Anzahl und die verbleibende Kapazität der Volumes an, die in das Aggregat verschoben werden.

  Über den Link können Sie weitere Details anzeigen, wie zum Beispiel den Namen des Volumes, das Aggregat, aus dem das Volume verschoben wird, den Status des Volume-Verschiebungsvorgangs und die voraussichtliche Endzeit.

    - Geschätzte genutzte Kapazität nach Volume-Verschiebung

      Zeigt die geschätzte Menge des belegten Speicherplatzes im Aggregat (als Prozentsatz und in KB, MB, GB usw.) an, nachdem die Volume-Verschiebungsvorgänge abgeschlossen sind.

- **Kapazitätsübersicht - Volumes**

  Es werden Diagramme angezeigt, die Informationen zur Kapazität der im Aggregat enthaltenen Volumes liefern. Der vom Volume belegte Speicherplatz (belegte Kapazität) und der im Volume verfügbare Speicherplatz (freie Kapazität) werden angezeigt. Wenn das Ereignis Thin-Provisioned Volume Space At Risk für Volumes mit Thin Provisioning generiert wird, werden der vom Volume belegte Speicherplatz (belegte Kapazität) und der im Volume verfügbare, aber aufgrund von Kapazitätsproblemen im Aggregat nicht nutzbare Speicherplatz (unbrauchbare Kapazität) angezeigt.

  Sie können das gewünschte Diagramm aus den Dropdown-Listen auswählen. Die im Diagramm angezeigten Daten lassen sich sortieren, um Details wie belegte Größe, provisionierte Größe, verfügbare Kapazität, höchste tägliche Wachstumsrate und niedrigste Wachstumsrate anzuzeigen. Sie können die Daten anhand der Storage Virtual Machines (SVMs) filtern, die die Volumes im Aggregat enthalten. Auch Details zu dünn provisionierten Volumes können angezeigt werden. Die Details bestimmter Punkte im Diagramm können angezeigt werden, indem der Mauszeiger über den gewünschten Bereich bewegt wird. Standardmäßig zeigt das Diagramm die Top 30 der gefilterten Volumes im Aggregat an.

Registerkarte Datenträgerinformationen

Zeigt detaillierte Informationen zu den Festplatten im ausgewählten Aggregat an, einschließlich des RAID-Typs und der RAID-Größe sowie der im Aggregat verwendeten Festplattentypen. Die Registerkarte stellt außerdem die RAID-Gruppen und die verwendeten Festplattentypen (z. B. SAS, ATA, FCAL, SSD oder VMDISK) grafisch dar. Weitere Informationen wie Einschub der Festplatte, Shelf und Drehzahl sind verfügbar, wenn Sie den Mauszeiger über die Paritätsfestplatten und Datenfestplatten bewegen.

- **Daten**

  Zeigt grafisch Details zu dedizierten Datenträgern, gemeinsam genutzten Datenträgern oder beiden an. Wenn die Datenträger gemeinsam genutzte Datenträger enthalten, werden deren grafische Details angezeigt. Wenn die Datenträger sowohl dedizierte als auch gemeinsam genutzte Datenträger enthalten, werden die grafischen Details sowohl der dedizierten Datenträger als auch der gemeinsam genutzten Datenträger angezeigt.

  - **RAID-Details**

    RAID-Details werden nur für dedizierte Festplatten angezeigt.

    - Typ

      Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

    - Gruppengröße

      Zeigt die maximal zulässige Anzahl von Festplatten in der RAID-Gruppe an.

    - Gruppen

      Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

  - **Verwendete Datenträger**
    - Effektiver Typ

      Zeigt die Typen der Datenfestplatten (z. B. ATA, SATA, FCAL, SSD oder VMDISK) im Aggregat an.

    - Daten-Disks

      Zeigt die Anzahl und Kapazität der einem Aggregat zugewiesenen Datenträger an. Details zu den Datenträgern werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Datenträger enthält.

    - Paritätsfestplatten

      Zeigt die Anzahl und Kapazität der einem Aggregat zugewiesenen Paritätsplatten an. Details zu Paritätsplatten werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Platten enthält.

    - Gemeinsam genutzte Festplatten

      Zeigt die Anzahl und Kapazität der gemeinsam genutzten Datenträger an, die einem Aggregat zugewiesen sind. Details zu gemeinsam genutzten Datenträgern werden nur angezeigt, wenn das Aggregat solche Datenträger enthält.

◦ **Ersatzfestplatten**

Zeigt den effektiven Datenträgertyp, die Anzahl und die Kapazität der für den Knoten im ausgewählten Aggregat verfügbaren Ersatzdatenträger an.

Wenn ein Aggregat auf den Partnerknoten übernommen wird, zeigt Unified Manager nicht alle mit dem Aggregat kompatiblen Ersatzfestplatten an.

- **SSD-Cache**

Enthält detaillierte Informationen zu dedizierten Cache-SSD-Festplatten und gemeinsam genutzten Cache-SSD-Festplatten.

Folgende Details zu den dedizierten Cache-SSD-Festplatten werden angezeigt:

◦ **RAID-Details**

▪ Typ

Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

▪ Gruppengröße

Zeigt die maximal zulässige Anzahl von Festplatten in der RAID-Gruppe an.

▪ Gruppen

Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

◦ **Verwendete Datenträger**

▪ Effektiver Typ

Zeigt an, dass die im Aggregat als Cache verwendeten Laufwerke vom Typ SSD sind.

▪ Daten-Disks

Zeigt die Anzahl und Kapazität der Datenträger an, die einem Aggregat für den Cache zugewiesen sind.

▪ Paritätsfestplatten

Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat für den Cache zugewiesen sind.

◦ **Ersatzfestplatten**

Zeigt den effektiven Festplattentyp, die Anzahl und die Kapazität der für den Knoten im ausgewählten Aggregat verfügbaren Ersatzfestplatten für den Cache an.

Wenn ein Aggregat auf den Partnerknoten übernommen wird, zeigt Unified Manager nicht alle mit dem Aggregat kompatiblen Ersatzfestplatten an.

Enthält die folgenden Details für den gemeinsam genutzten Cache:

- **Storage-Pool**

  Zeigt den Namen des Storage-Pools an. Beim Bewegen des Mauszeigers über den Namen des Storage-Pools erscheinen die folgenden Details:

  - Status

    Zeigt den Status des Storage Pools an, der in Ordnung oder nicht in Ordnung sein kann.

  - Gesamtzuweisungen

    Zeigt die Gesamtzahl der Zuordnungseinheiten und die Größe im Storage-Pool an.

  - Zuteilungseinheitsgröße

    Zeigt die minimale Speichermenge im Storage Pool an, die einem Aggregat zugewiesen werden kann.

  - Festplatten

    Zeigt die Anzahl der Festplatten an, die zum Erstellen des Storage Pool verwendet werden. Wenn die Festplattenanzahl in der Spalte „Storage Pool“ und die im Tab „Festplatteninformationen“ für diesen Storage Pool angezeigte Anzahl nicht übereinstimmen, weist dies darauf hin, dass eine oder mehrere Festplatten defekt sind und der Storage Pool nicht ordnungsgemäß funktioniert.

  - Verwendete Zuweisung

    Zeigt die Anzahl und Größe der von den Aggregaten verwendeten Zuordnungseinheiten an. Ein Klick auf den Aggregatnamen zeigt die Aggregatdetails an.

  - Verfügbare Zuweisung

    Zeigt die Anzahl und Größe der für die Knoten verfügbaren Zuordnungseinheiten an. Sie können auf den Node-Name klicken, um die Aggregatdetails anzuzeigen.

- **Zugewiesener Cache**

  Zeigt die Größe der vom Aggregat verwendeten Zuordnungseinheiten an.

- **Zuteilungseinheiten**

  Zeigt die Anzahl der vom Aggregat verwendeten Zuordnungseinheiten an.

- **Festplatten**

  Zeigt die Anzahl der im Storage-Pool enthaltenen Festplatten an.

- **Details**

  - Speicherpool

    Zeigt die Anzahl der Storage-Pools an.

  - Gesamtgröße

    Zeigt die Gesamtgröße der Storage Pools an.

- **Cloud-Tier**

  Zeigt den Namen des Cloud-Tiers an, sofern Sie ein für FabricPool aktiviertes Aggregat konfiguriert haben, und zeigt den insgesamt verwendeten Speicherplatz an. Wenn das Cloud-Tier auf einen anderen Cloud-Anbieter (das Mirror-Tier) gespiegelt wird, werden hier die Details für beide Cloud-Tiers angezeigt.

Registerkarte „Konfiguration“

Die Registerkarte „Konfiguration“ zeigt Details zum ausgewählten Aggregat an, wie z. B. dessen Clusterknoten, Blocktyp, RAID-Typ, RAID-Größe und die Anzahl der RAID-Gruppen:

- **Überblick**
  - Node

    Zeigt den Namen des Knotens an, der das ausgewählte Aggregat enthält.

  - Blocktyp

    Zeigt das Blockformat des Aggregats an: entweder 32-Bit oder 64-Bit.

  - RAID-Typ

    Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP, RAID-TEC oder Mixed RAID).

  - RAID-Größe

    Zeigt die Größe der RAID-Gruppe an.

  - RAID-Gruppen

    Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

  - SnapLock Typ

    Zeigt den SnapLock Typ des Aggregats an.

- **Cloud-Tier**

  Wenn es sich um ein FabricPool fähiges Aggregat handelt, werden die Details für das Cloud-Tier angezeigt. Einige Felder unterscheiden sich je nach Storage-Provider. Wenn das Cloud-Tier auf einen anderen Cloud-Provider gespiegelt wird (das „`mirror tier`“), werden hier beide Cloud-Tiers angezeigt.

  - Anbieter

    Zeigt den Namen des Storage-Providers an, zum Beispiel StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud, Google Cloud Storage oder Alibaba Cloud Object Storage.

  - Name

    Zeigt den Namen der Cloud-Ebene an, als sie von ONTAP erstellt wurde.

  - Server

    Zeigt den FQDN des Cloud-Tiers an.

- Port

  Der Port für die Kommunikation mit dem Cloud-Anbieter.

- Zugriffsschlüssel oder Konto

  Zeigt den Zugriffsschlüssel oder das Konto für die Cloud-Ebene an.

- Containername

  Zeigt den Bucket- oder Containernamen der Cloud-Ebene an.

- SSL

  Zeigt an, ob die SSL-Verschlüsselung für die Cloud-Ebene aktiviert ist.

Verlaufsbereich

Im Bereich „Verlauf“ werden Diagramme angezeigt, die Informationen zur Kapazität des ausgewählten Aggregats liefern. Zusätzlich können Sie auf die Schaltfläche **Export** klicken, um einen Bericht im CSV-Format für das angezeigte Diagramm zu erstellen.

Sie können in der Dropdown-Liste oben im Verlaufsbereich einen Diagrammtyp auswählen. Außerdem können Sie Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Verlaufsdiagramme helfen Ihnen, Trends zu erkennen: Wenn beispielsweise die Gesamtnutzung regelmäßig den Schwellenwert „Nahezu voll“ überschreitet, können Sie entsprechende Maßnahmen ergreifen.

Verlaufsdiagramme zeigen folgende Informationen an:

- **Verwendete Aggregatkapazität (%)**

  Das Diagramm zeigt die im Aggregat verwendete Kapazität und den Trend der Nutzung der Aggregatkapazität basierend auf dem Nutzungsverlauf als Liniendiagramme in Prozent auf der vertikalen (y-)Achse. Der Zeitraum wird auf der horizontalen (x-)Achse dargestellt. Es kann ein Zeitraum von einer Woche, einem Monat oder einem Jahr ausgewählt werden. Die Details zu bestimmten Punkten im Diagramm werden angezeigt, wenn der Cursor über einem entsprechenden Bereich positioniert wird. Ein Liniendiagramm kann durch Klicken auf die entsprechende Legende ein- oder ausgeblendet werden. Wenn beispielsweise auf die Legende Capacity Used geklickt wird, wird die Diagrammlinie Capacity Used ausgeblendet.

- **Verwendete Aggregatkapazität im Vergleich zur Gesamtkapazität**

  Zeigt den Trend der Nutzung der Aggregatkapazität auf der Grundlage des Nutzungsverlaufs sowie die genutzte Kapazität und die Gesamtkapazität als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen (y-)Achse an. Der Zeitraum wird auf der horizontalen (x-)Achse angezeigt. Es kann ein Zeitraum von einer Woche, einem Monat oder einem Jahr ausgewählt werden. Die Details für bestimmte Punkte im Diagramm können angezeigt werden, indem der Cursor über einen bestimmten Bereich positioniert wird. Ein Liniendiagramm kann durch Klicken auf die entsprechende Legende aus- oder eingeblendet werden. Wenn beispielsweise auf die Legende Trend Capacity Used geklickt wird, wird die Diagrammlinie Trend Capacity Used ausgeblendet.

- **Genutzte Aggregatkapazität (%) im Vergleich zu zugesagt (%)**

  Zeigt den Trend, wie die Aggregatkapazität auf der Grundlage des Nutzungsverlaufs verwendet wird, sowie den zugesagten Speicherplatz als Liniendiagramme in Prozent auf der vertikalen (y-)Achse an. Der Zeitraum wird auf der horizontalen (x-)Achse angezeigt. Sie können einen Zeitraum von einer Woche,

einem Monat oder einem Jahr auswählen. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen bestimmten Bereich positionieren. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende Space Committed klicken, wird die Diagrammlinie Space Committed ausgeblendet.

Ereignisliste

Die Ereignisliste zeigt Details zu neuen und bestätigten Ereignissen an:

- **Schweregrad**

  Zeigt den Schweregrad des Ereignisses an.

- **Ereignis**

  Zeigt den Ereignisnamen an.

- **Auslösezeit**

  Zeigt die seit der Ereignisgenerierung verstrichene Zeit an. Wenn mehr als eine Woche vergangen ist, wird der Zeitstempel angezeigt, zu dem das Ereignis generiert wurde.

Bereich „Verwandte Geräte“

Im Bereich „Zugehörige Geräte“ lassen sich der Cluster-Node, Volumes und Datenträger anzeigen, die dem Aggregat zugeordnet sind:

- **Knoten**

  Zeigt die Kapazität und den Systemstatus des Knotens an, der das Aggregat enthält. Die Kapazität gibt das Verhältnis der nutzbaren Kapazität zur verfügbaren Kapazität an.

- **Aggregate im Knoten**

  Zeigt die Anzahl und Kapazität aller Aggregate im Clusterknoten an, der das ausgewählte Aggregat enthält. Der Systemstatus der Aggregate wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Enthält ein Clusterknoten beispielsweise zehn Aggregate, von denen fünf den Status „Warnung“ und die restlichen fünf den Status „Kritisch“ aufweisen, wird der Status „Kritisch“ angezeigt.

- **Volumes**

  Zeigt die Anzahl und Kapazität der FlexVol Volumes und FlexGroup Volumes im Aggregat an; die Anzahl umfasst keine FlexGroup Bestandteile. Der Systemstatus der Volumes wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad.

- **Ressourcenpool**

  Zeigt die zum Aggregat gehörenden Ressourcenpools an.

- **Festplatten**

  Zeigt die Anzahl der Datenträger im ausgewählten Aggregat an.

Bereich „Zugehörige Warnungen“

Im Bereich „Verwandte Benachrichtigungen“ können Sie die Liste der für das ausgewählte Aggregat erstellten Benachrichtigungen anzeigen. Sie können außerdem eine Benachrichtigung hinzufügen, indem Sie auf den Link „Benachrichtigung hinzufügen“ klicken, oder eine vorhandene Benachrichtigung bearbeiten, indem Sie auf den Benachrichtigungsnamen klicken.

Verwandte Informationen

"Storage-Pool-Details anzeigen"

Daten schützen und wiederherstellen

Schutzbeziehungen erstellen und Fehler beheben

Arten des SnapMirror Schutzes in Active IQ Unified Manager

Je nach Deployment Ihrer Storage-Topologie ermöglicht Ihnen Unified Manager die Konfiguration mehrerer Arten von SnapMirror Schutzbeziehungen. Alle Varianten der SnapMirror Datensicherung bieten Failover- und Disaster-Recovery-Schutz, unterscheiden sich jedoch hinsichtlich Performance, Versionsflexibilität und des Schutzes durch mehrere Sicherungskopien.

Traditionelle SnapMirror asynchrone Schutzbeziehungen

Der traditionelle SnapMirror asynchrone Schutz bietet Spiegelungsschutz durch Blockreplikation zwischen Quell- und Ziel-Volumes.

In traditionellen SnapMirror Beziehungen werden Spiegelungsoperationen schneller ausgeführt als in alternativen SnapMirror Beziehungen, da die Spiegelungsoperation auf Blockreplikation basiert. Traditioneller SnapMirror Schutz erfordert jedoch, dass das Zielvolume mit derselben oder einer neueren Minor-Version der ONTAP Software wie das Quellvolume innerhalb derselben Hauptversion ausgeführt wird, z. B. Version 8.x zu 8.x oder 9.x zu 9.x. Die Replikation von einer 9.1 Quelle zu einem 9.0 Ziel wird nicht unterstützt, da auf dem Ziel eine ältere Hauptversion ausgeführt wird.

SnapMirror Asynchroner Schutz mit versionsflexibler Replikation

SnapMirror Asynchroner Schutz mit versionsflexibler Replikation bietet logischen Replikationsspiegelschutz zwischen Quell- und Ziel-Volumes, selbst wenn diese Volumes unter verschiedenen Versionen der Software ONTAP 8.3 oder höher ausgeführt werden (z. B. Version 8.3 bis 8.3.1, oder 8.3 bis 9.1, oder 9.2.2 bis 9.2).

In SnapMirror Beziehungen mit versionsflexibler Replikation werden Spiegelungsvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror Beziehungen.

Aufgrund der langsameren Ausführung ist SnapMirror mit versionsflexiblem Replikationsschutz in den folgenden Fällen nicht für die Implementierung geeignet:

- Das Quellobjekt enthält mehr als 10 Millionen zu schützende Dateien.
- Das Wiederherstellungspunktziel für die geschützten Daten beträgt zwei Stunden oder weniger. (Das heißt, das Ziel muss stets gespiegelte, wiederherstellbare Daten enthalten, die höchstens zwei Stunden älter sind als die Daten an der Quelle.)

Unter beiden genannten Umständen ist die schnellere, auf Blockreplikation basierende Ausführung des standardmäßigen SnapMirror Schutzes erforderlich.

SnapMirror Asynchroner Schutz mit versionsflexibler Replikation und Backup-Option

SnapMirror Asynchroner Schutz mit versionsflexibler Replikations- und Backup-Option bietet Spiegelschutz zwischen Quell- und Ziel-Volumes sowie die Möglichkeit, mehrere Kopien der gespiegelten Daten am Ziel zu speichern.

Der Storage Administrator kann festlegen, welche Snapshot-Kopien von der Quelle zum Ziel gespiegelt

werden, und auch, wie lange diese Kopien am Ziel aufbewahrt werden sollen, selbst wenn sie an der Quelle gelöscht werden.

In SnapMirror Beziehungen mit versionsflexibler Replikation und Backup-Option werden Spiegelungsvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror Beziehungen.

SnapMirror Einheitliche Replikation (Spiegelung und Vault)

SnapMirror Unified Replication ermöglicht die Konfiguration von Disaster Recovery und Archivierung auf demselben Zielvolume. Wie bei SnapMirror führt die einheitliche Datensicherung beim ersten Aufruf einen Basistransfer durch. Ein Basistransfer gemäß der standardmäßigen Datensicherungsstrategie „MirrorAndVault“ erstellt eine Snapshot Kopie des Quellvolumes und überträgt diese Kopie zusammen mit den Datenblöcken, auf die sie verweist, auf das Zielvolume. Wie bei SnapVault umfasst die einheitliche Datensicherung im Basistransfer keine älteren Snapshot Kopien.

SnapMirror synchroner Schutz mit strenger Synchronisierung

SnapMirror Synchronous protection mit der Synchronisierung “strict” stellt sicher, dass das primäre und das sekundäre Volume stets eine exakte Kopie voneinander sind. Wenn beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replikationsfehler auftritt, wird die Client-I/O auf dem primären Volume unterbrochen.

SnapMirror synchroner Schutz mit regelmäßiger Synchronisierung

SnapMirror Synchroner Schutz mit „`regular`“-Synchronisierung erfordert nicht, dass das primäre und das sekundäre Volume stets eine exakte Kopie voneinander sind; dadurch wird die Verfügbarkeit des primären Volumes sichergestellt. Wenn beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replikationsfehler auftritt, geraten das primäre und das sekundäre Volume außer Synchronisation, und die Client-E/A wird weiterhin an das primäre Volume geleitet.



Die Schaltfläche „Wiederherstellen“ und die Schaltflächen für Beziehungsvorgänge sind bei der Überwachung synchroner Schutzbeziehungen in der Ansicht „Zustand: Alle Volumes“ oder auf der Detailseite „Volume/Health“ nicht verfügbar.

SnapMirror Active Sync

Die SnapMirror active sync Funktion ist mit ONTAP 9.8 und höher verfügbar, und sie kann zum Schutz von Applikationen mit LUNs verwendet werden, sodass ein transparentes Failover von Applikationen möglich ist und die Geschäftskontinuität im Katastrophenfall gewährleistet bleibt.

Es ermöglicht die Identifizierung und Überwachung der synchronen SnapMirror Beziehungen für Konsistenzgruppen (CGs), die auf Clustern und Storage Virtual Machines in Unified Manager verfügbar sind. SnapMirror active sync wird auf AFF Clustern oder All SAN Array (ASA) Clustern unterstützt, wobei die primären und sekundären Cluster entweder AFF oder ASA sein können. SnapMirror active sync schützt Applikationen mit iSCSI oder FCP LUNs.

Wenn Sie die Volumes und LUNs anzeigen, die durch die SnapMirror active sync Beziehung geschützt sind, erhalten Sie eine einheitliche Übersicht über Datensicherungsbeziehungen, Konsistenzgruppen im Volume-Inventar, die Datensicherungstopologie für Konsistenzgruppenbeziehungen sowie historische Daten für Konsistenzgruppenbeziehungen für bis zu ein Jahr. Sie können den Bericht auch herunterladen. Außerdem können Sie die Zusammenfassung der Konsistenzgruppenbeziehungen anzeigen, nach Unterstützung für Konsistenzgruppenbeziehungen suchen und Informationen zu Volumes abrufen, die durch die Konsistenzgruppe geschützt sind.

Auf der Seite „Beziehungen“ können Sie außerdem die Quell- und Ziel-Storage-Objekte sowie deren Beziehung, die von der Consistency Group geschützt werden, sortieren, filtern und den Schutz erweitern.

Weitere Informationen zu SnapMirror active sync sind unter "ONTAP 9 Dokumentation für Snapmirror active sync (ehemals SM-BC)" verfügbar.

Einrichten von Schutzbeziehungen in Unified Manager

Einrichtung von Schutzbeziehungen in Active IQ Unified Manager

Es gibt mehrere Schritte, die Sie ausführen müssen, um Unified Manager und OnCommand Workflow Automation zum Einrichten von SnapMirror und SnapVault Beziehungen zum Schutz Ihrer Daten zu verwenden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Peer-Beziehungen zwischen zwei Clustern oder zwei Storage Virtual Machines (SVMs) eingerichtet haben.
- OnCommand Workflow Automation muss in Unified Manager integriert sein:
  - "Einrichtung von OnCommand Workflow Automation".
  - "Überprüfung des Unified Manager-Datenquellen-Cachings in Workflow Automation".

Schritte

1. Je nach Typ der Schutzbeziehung, die erstellt werden soll, ist eine der folgenden Optionen auszuwählen:
   - "Erstellung einer SnapMirror Schutzbeziehung".
   - "Erstellen einer SnapVault Schutzbeziehung".
2. Falls eine Richtlinie für die Beziehung erstellt werden soll, hängt das Vorgehen vom Typ der zu erstellenden Beziehung ab:
   - "Eine SnapVault Richtlinie erstellen".
   - "Erstellung einer SnapMirror Richtlinie".
3. "Erstellen eines SnapMirror oder SnapVault Zeitplans".

Konfiguration einer Verbindung zwischen Workflow Automation und Active IQ Unified Manager

Sie können eine sichere Verbindung zwischen OnCommand Workflow Automation (WFA) und Unified Manager konfigurieren. Die Verbindung zu Workflow Automation ermöglicht Ihnen die Nutzung von Schutzfunktionen wie SnapMirror- und SnapVault Konfigurationsworkflows sowie von Befehlen zum Verwalten von SnapMirror Beziehungen.

Bevor Sie beginnen

- Die installierte Version von Workflow Automation muss 5.1.1P6 oder höher sein.

> Das „WFA-Paket zur Verwaltung von Clustered Data ONTAP“ ist in WFA 5.1.1P6 enthalten, sodass es nicht mehr erforderlich ist, dieses Paket aus dem NetAppStorage Automation Store herunterzuladen und separat auf Ihrem WFA-Server zu installieren, wie es in der

Vergangenheit notwendig war. "WFA-Download"

- Sie benötigen den Namen des Datenbankbenutzers, den Sie in Unified Manager erstellt haben, um WFA und Unified Manager Verbindungen zu unterstützen.

  Diesem Datenbankbenutzer muss die Benutzerrolle „Integration Schema“ zugewiesen worden sein.

- Ihnen muss in Workflow Automation entweder die Administratorrolle oder die Architektenrolle zugewiesen sein.
- Für die Workflow Automation Einrichtung benötigen Sie die Hostadresse, die Portnummer 443, den Benutzernamen und das Passwort.
- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich wählen Sie **General** > **Workflow Automation**.
2. Im Bereich **Datenbankbenutzer** der **Workflow Automation Seite** erfolgt die Auswahl des Namens sowie die Eingabe des Passworts für den Datenbankbenutzer, den Sie zur Unterstützung von Verbindungen zwischen Unified Manager und Workflow Automation erstellt haben.
3. Im Bereich **Workflow Automation Credentials** der Seite sind der Hostname oder die IP-Adresse (IPv4 oder IPv6) sowie der Benutzername und das Passwort für die Workflow Automation Einrichtung einzugeben.

   Sie müssen den Unified Manager Server-Port (Port 443) verwenden.

4. Auf **Speichern** klicken.
5. Wenn Sie ein selbstsigniertes Zertifikat verwenden, erfolgt die Autorisierung des Sicherheitszertifikats durch Klicken auf **Ja**.

   Die Seite „Workflow Automation“ wird angezeigt.

6. Nach einem Klick auf **Yes** wird die Web UI neu geladen, und die Workflow Automation Funktionen werden hinzugefügt.

Verwandte Informationen

"NetApp Dokumentation: OnCommand Workflow Automation (aktuelle Versionen)"

Überprüfung des Caching der Active IQ Unified Manager Datenquelle in Workflow Automation

Sie können feststellen, ob das Caching der Datenquellen in Unified Manager ordnungsgemäß funktioniert, indem Sie prüfen, ob die Datenquellenerfassung in Workflow Automation erfolgreich ist. Dies empfiehlt sich beispielsweise bei der Integration von Workflow Automation mit Unified Manager, um sicherzustellen, dass die Funktionen von Workflow Automation nach der Integration verfügbar sind.

Bevor Sie beginnen

Um diese Aufgabe ausführen zu können, muss Ihnen in Workflow Automation entweder die Administratorrolle oder die Architektenrolle zugewiesen sein.

Schritte

1. In der Workflow Automation UI erfolgt die Auswahl von **Execution** > **Data Sources**.
2. Per Rechtsklick auf den Namen der Unified Manager Datenquelle und anschließendes Auswählen von **Acquire Now**.
3. Zu überprüfen ist, ob die Datenerfassung fehlerfrei verläuft.

   Für eine erfolgreiche Integration von Workflow Automation mit Unified Manager müssen Erfassungsfehler behoben werden.

Wie sich die Neuinstallation oder das Upgrade von OnCommand Workflow Automation auf Active IQ Unified Manager auswirken

Vor der Neuinstallation oder dem Upgrade von OnCommand Workflow Automation müssen Sie zunächst die Verbindung zwischen OnCommand Workflow Automation und Unified Manager entfernen und sicherstellen, dass alle derzeit ausgeführten oder geplanten Aufträge von OnCommand Workflow Automation gestoppt sind.

Sie müssen Unified Manager außerdem manuell aus OnCommand Workflow Automation löschen.

Nach der Neuinstallation oder dem Upgrade von OnCommand Workflow Automation müssen Sie die Verbindung mit Unified Manager erneut einrichten.

Entfernen der OnCommand Workflow Automation Einrichtung aus Active IQ Unified Manager

Die Einrichtung von OnCommand Workflow Automation kann aus Unified Manager entfernt werden, wenn Workflow Automation nicht mehr verwendet werden soll.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Die Auswahl erfolgt im linken Navigationsbereich über **General** > **Workflow Automation** im linken Setup-Menü.
2. Auf der Seite **Workflow Automation** erfolgt die Auswahl von **Remove Setup**.

Durchführen eines Failovers und Failbacks für eine Schutzbeziehung

Durchführen eines Failovers und Failbacks einer Schutzbeziehung in Active IQ Unified Manager

Wenn ein Quellvolume in Ihrer Schutzbeziehung aufgrund eines Hardwareausfalls oder einer Katastrophe deaktiviert wird, können Sie die Schutzbeziehungsfunktionen in Unified Manager verwenden, um das Schutzziel für lesen/schreiben zugänglich zu machen und ein Failover auf dieses Volume durchzuführen, bis die Quelle wieder online ist; anschließend können Sie ein Failback zur ursprünglichen Quelle durchführen, sobald diese wieder für die Datenbereitstellung verfügbar ist.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen OnCommand Workflow Automation eingerichtet haben, um diesen Vorgang durchzuführen.

Schritte

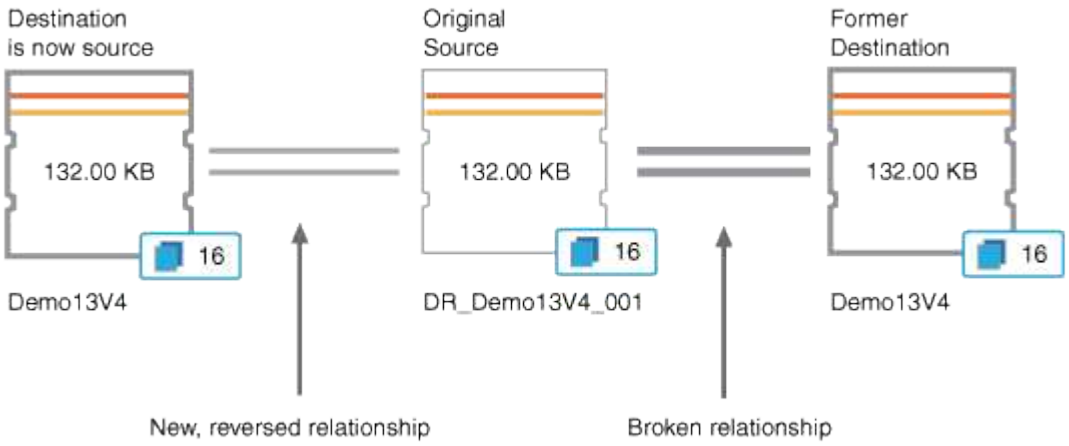
1. "Aufheben der SnapMirror Beziehung".

   Sie müssen die Beziehung aufheben, bevor Sie das Ziel von einem Datensicherungs-Volume in ein Volume mit lesen/schreiben konvertieren können und bevor Sie die Beziehung umkehren können.

2. "Umkehrung der Schutzbeziehung".

   Wenn das ursprüngliche Quellvolume wieder verfügbar ist, können Sie die ursprüngliche Schutzbeziehung wiederherstellen, indem Sie das Quellvolume wiederherstellen. Bevor Sie das Quellvolume wiederherstellen können, müssen Sie es mit den Daten synchronisieren, die auf das frühere Ziel geschrieben wurden. Mithilfe der umgekehrten Resynchronisierung erstellen Sie eine neue Schutzbeziehung, indem Sie die Rollen der ursprünglichen Beziehung umkehren und das Quellvolume mit dem früheren Ziel synchronisieren. Für die neue Beziehung wird eine neue Snapshot Basiskopie erstellt.

   Die umgekehrte Beziehung ähnelt einer Kaskadenbeziehung:



3. "Aufheben der umgekehrten SnapMirror Beziehung".

   Wenn das ursprüngliche Quellvolume erneut synchronisiert ist und wieder Daten bereitstellen kann, kann die umgekehrte Beziehung mit der Break-Operation aufgehoben werden.

4. "Beziehung entfernen".

   Wenn die umgekehrte Beziehung nicht mehr benötigt wird, sollte diese Beziehung entfernt werden, bevor die ursprüngliche Beziehung erneut eingerichtet wird.

5. "Neusynchronisieren der Beziehung".

   Die Resynchronisierungsoperation synchronisiert Daten von der Quelle zum Ziel und stellt die ursprüngliche Beziehung wieder her.

Eine SnapMirror Schutzbeziehung auf der Seite „Volume/Integrität“ von Active IQ Unified Manager trennen

Auf der Seite „Volume/Health-Details“ können Sie eine Schutzbeziehung aufheben und Datentransfers zwischen einem Quell- und einem Zielvolume in einer SnapMirror Beziehung beenden. Eine Beziehung kann aufgehoben werden, wenn Sie Daten migrieren möchten, für Disaster Recovery oder für Applikationstests. Das Zielvolume wird

in ein Volume mit lesen/schreiben geändert. Eine SnapVault Beziehung kann nicht aufgehoben werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Schritte

1. Auf der Registerkarte **Schutz** der Detailseite **Volume / Integrität** erfolgt die Auswahl der SnapMirror Beziehung, die in der Topologie getrennt werden soll.
2. Rechtsklick auf das Ziel und Auswahl von **Break** im Menü.

   Das Dialogfeld „Beziehung aufheben“ wird angezeigt.
3. Über **Weiter** lässt sich die Beziehung beenden.
4. In der Topologie lässt sich überprüfen, ob die Beziehung unterbrochen ist.

Umgekehrte Schutzbeziehungen auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager

Wenn ein Katastrophenfall das Quellvolume in Ihrer Schutzbeziehung außer Betrieb setzt, kann das Zielvolume zur Bereitstellung von Daten verwendet werden, indem es während der Reparatur oder des Austauschs des Quellvolumes in lesen/schreiben konvertiert wird. Sobald das Quellvolume wieder für den Datenempfang verfügbar ist, kann mit dem Vorgang der umgekehrten Resynchronisierung die Beziehung in umgekehrter Richtung hergestellt werden, wobei die Daten auf dem Quellvolume mit den Daten auf dem lesen/schreiben Zielvolume synchronisiert werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.
- Die Beziehung darf keine SnapVault Beziehung sein.
- Eine Schutzbeziehung muss bereits vorhanden sein.
- Die Schutzbeziehung muss getrennt werden.
- Sowohl Quelle als auch Ziel müssen online sein.
- Die Quelle darf nicht das Ziel eines anderen Datensicherungs-Volumes sein.
- Wenn Sie diese Aufgabe ausführen, werden auf der Quelle Daten gelöscht, die neuer sind als die Daten in der gemeinsamen Snapshot Kopie.
- Die in der umgekehrten Resynchronisierungsbeziehung erstellten Richtlinien und Zeitpläne entsprechen denen der ursprünglichen Schutzbeziehung.

  Falls keine Richtlinien und Zeitpläne existieren, werden sie erstellt.

Schritte

1. Auf der Registerkarte **Schutz** der Detailseite **Volume / Health** kann in der Topologie die SnapMirror Beziehung, für die Quelle und Ziel umgekehrt werden sollen, per Rechtsklick ausgewählt werden.
2. Sie wählen im Menü **Reverse Resync** aus.

Das Dialogfeld „Umgekehrte Resynchronisierung“ wird angezeigt.

3. Stellen Sie sicher, dass die im Dialogfeld **Reverse Resync** angezeigte Beziehung diejenige ist, für die Sie die umgekehrte Resynchronisierung durchführen möchten, und klicken Sie anschließend auf **Submit**.

   Das Dialogfeld „Resynchronisierung rückgängig machen“ wird geschlossen, und oben auf der Seite „Volume / Zustandsdetails“ wird ein Job-Link angezeigt.

4. **Optional:** Auf der Detailseite **Volume / Health** lässt sich über **View Jobs** der Status jedes umgekehrten Resynchronisierungsjobs verfolgen.

   Eine gefilterte Liste der Jobs wird angezeigt.

5. **Optional:** Über den **Back**-Pfeil in Ihrem Browser gelangen Sie zurück zur Detailseite **Volume / Health**.

   Der umgekehrte Resynchronisierungsvorgang ist abgeschlossen, wenn alle Jobaufgaben erfolgreich abgeschlossen sind.

Eine Schutzbeziehung wird auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager entfernt

Sie können eine Schutzbeziehung entfernen, um eine bestehende Beziehung zwischen der ausgewählten Quelle und dem Ziel dauerhaft zu löschen, beispielsweise wenn Sie eine Beziehung mit einem anderen Ziel erstellen möchten. Dieser Vorgang löscht alle Metadaten und kann nicht rückgängig gemacht werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Schritte

1. Auf der Registerkarte **Protection** der Detailseite **Volume / Health** wird in der Topologie die SnapMirror Beziehung ausgewählt, die entfernt werden soll.
2. Sie entfernen das Ziel, indem Sie mit der rechten Maustaste auf den Namen des Ziels klicken und im Menü **Entfernen** auswählen.

   Das Dialogfeld „Beziehung entfernen“ wird angezeigt.

3. Mit **Weiter** lässt sich die Beziehung entfernen.

   Die Beziehung wird von der Seite „Volume / Health details“ entfernt.

Neusynchronisierung von Schutzbeziehungen auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager

Sie können Daten in einer unterbrochenen SnapMirror oder SnapVault Beziehung neu synchronisieren, nachdem das Ziel auf lesen/schreiben gesetzt wurde, sodass die Daten auf der Quelle mit den Daten auf dem Ziel übereinstimmen. Eine erneute Synchronisierung kann auch erforderlich sein, wenn eine erforderliche gemeinsame Snapshot Kopie auf dem Quell-Volume gelöscht wurde und dadurch SnapMirror oder SnapVault Aktualisierungen fehlschlagen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Auf der Registerkarte **Protection** der Detailseite **Volume / Health** wird in der Topologie die Schutzbeziehung, die neu synchronisiert werden soll, mit der rechten Maustaste angeklickt.
2. Die Auswahl im Menü erfolgt über **Resynchronize**.

   Alternativ lässt sich im Menü **Aktionen** die Option **Beziehung** > **Neu synchronisieren** auswählen, um die Beziehung, deren Details aktuell angezeigt werden, erneut zu synchronisieren.

   Das Dialogfeld „Resynchronisieren“ wird angezeigt.
3. Auf der Registerkarte **Resynchronisierungsoptionen** lassen sich eine Übertragungspriorität und die maximale Transferrate auswählen.
4. Nach einem Klick auf **Source Snapshot Copies** ist in der Spalte **Snapshot Copy** auf **Default** zu klicken.

   Das Dialogfeld „Quell-Snapshot-Kopie auswählen“ wird angezeigt.
5. Zum Angeben einer vorhandenen Snapshot-Kopie anstelle der Standard-Snapshot-Kopie ist **Vorhandene Snapshot Copy** anzuklicken und eine Snapshot-Kopie aus der Liste auszuwählen.
6. Anschließend **Absenden** auswählen.

   Sie kehren zum Dialogfeld „Resynchronisieren“ zurück.
7. Bei Auswahl von mehr als einer Quelle für die Resynchronisierung wird für die nächste Quelle, für die eine vorhandene Snapshot-Kopie angegeben werden soll, **Default** ausgewählt.
8. Mit **Submit** wird der Resynchronisierungsvorgang gestartet.

   Der Resynchronisierungsauftrag wird gestartet, Sie kehren zur Seite „Volume / Health details“ zurück, und oben auf der Seite wird ein Link zu Jobs angezeigt.
9. **Optional:** Auf der Seite **Volume / Health details** lässt sich über **View Jobs** der Status jedes Resynchronisierungsauftrags nachverfolgen.

   Eine gefilterte Liste der Jobs wird angezeigt.
10. **Optional:** Über den **Back**-Pfeil in Ihrem Browser gelangen Sie zurück zur Detailseite **Volume / Health**.

    Der Resynchronisierungsvorgang ist beendet, wenn alle Jobaufgaben erfolgreich abgeschlossen sind.

Fehler in einem Schutzauftrag beheben

Beheben eines Fehlers bei einem Schutzauftrag in Active IQ Unified Manager

Dieser Workflow zeigt beispielhaft, wie sich ein Fehler bei einem Schutzauftrag im Unified Manager Dashboard identifizieren und beheben lässt.

Bevor Sie beginnen

Da einige Aufgaben in diesem Arbeitsablauf die Anmeldung mit der Administratorrolle erfordern, müssen Sie

mit den Rollen vertraut sein, die zur Nutzung der verschiedenen Funktionen erforderlich sind.

In diesem Szenario greifen Sie auf die Dashboard Seite zu, um festzustellen, ob es Probleme mit Ihren Schutzaufträgen gibt. Im Bereich Protection Incident stellen Sie fest, dass ein Job Terminated Incident vorliegt, der auf einem Volume einen Fehler Protection Job Failed anzeigt. Sie untersuchen diesen Fehler, um die mögliche Ursache und eine potenzielle Lösung zu ermitteln.

Schritte

1. Im Bereich „Ungelöste Vorfälle und Risiken“ des Dashboards im Fenster „Schutzvorfälle“ klicken Sie auf das Ereignis „**Protection job failed**“.

   Der verlinkte Text für das Ereignis ist in der Form `object_name:/object_name - Error Name` geschrieben, z. B. `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

   Die Seite mit den Ereignisdetails für den fehlgeschlagenen Schutzvorgang wird angezeigt.

2. Anhand der Fehlermeldung im Feld „Cause“ des Bereichs **Summary** lassen sich das Problem bestimmen und mögliche Korrekturmaßnahmen bewerten.

   Weitere Informationen finden Sie unter "Identifizierung des Problems und Durchführung von Korrekturmaßnahmen für einen fehlgeschlagenen Schutzjob".

Das Problem und die Korrekturmaßnahmen für einen fehlgeschlagenen Schutzauftrag in Active IQ Unified Manager werden identifiziert und durchgeführt

Sie prüfen die Fehlermeldung im Feld „Ursache“ auf der Seite mit den Ereignisdetails und stellen fest, dass der Auftrag aufgrund eines Fehlers bei der Snapshot Kopie fehlgeschlagen ist. Anschließend rufen Sie die Seite mit den Volume-/Integritätsdetails auf, um weitere Informationen zu erhalten.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Die im Feld „Ursache“ auf der Seite „Ereignisdetails“ angegebene Fehlermeldung enthält folgenden Text über den fehlgeschlagenen Job:

```
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
```

Diese Nachricht enthält folgende Informationen:

- Ein Sicherungs- oder Spiegelungsauftrag wurde nicht erfolgreich abgeschlossen.

  Die Aufgabe umfasste eine Schutzbeziehung zwischen dem Quellvolume `cluster2_src_vol2` auf dem

virtuellen Server `cluster2_src_svm` und dem Zielvolume `managed_svc2_vol3` auf dem virtuellen Server mit dem Namen `cluster3_dst_svm`.

- Ein Auftrag für eine Snapshot Kopie ist fehlgeschlagen für `0426cluster2_src_vol2snap` auf dem Quell-Volume `cluster2_src_svm:/cluster2_src_vol2`.

In diesem Szenario können Sie die Ursache und mögliche Korrekturmaßnahmen für den Jobfehler ermitteln. Für die Behebung des Fehlers müssen Sie jedoch entweder auf die System Manager Web-UI zugreifen oder ONTAP CLI-Befehle verwenden.

Schritte

1. Sie überprüfen die Fehlermeldung und stellen fest, dass ein Snapshot Kopierauftrag auf dem Quellvolume fehlgeschlagen ist, was darauf hindeutet, dass wahrscheinlich ein Problem mit Ihrem Quellvolume besteht.

   Optional wäre es möglich, am Ende der Fehlermeldung auf den Link **Job Details** zu klicken; in diesem Szenario wird jedoch darauf verzichtet.

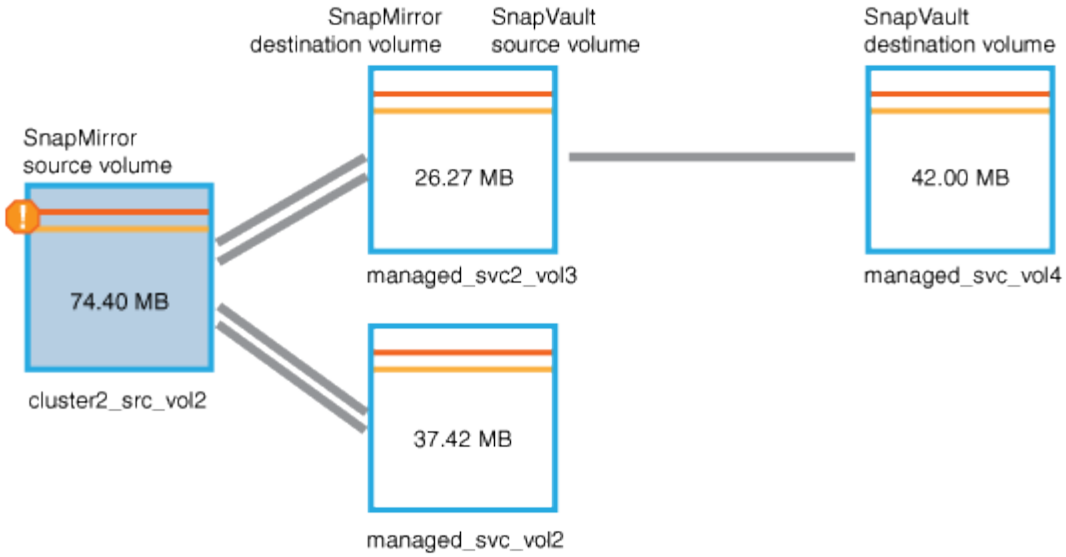
2. Sie beschließen, zu versuchen, das Ereignis zu beheben, und gehen daher wie folgt vor:
   a. Über die Schaltfläche **Zuweisen an** lässt sich im Menü **Ich** auswählen.
   b. Über die Schaltfläche **Acknowledge** lässt sich der weitere Erhalt wiederholter Warnungsbenachrichtigungen verhindern, sofern für das Ereignis Warnmeldungen eingerichtet wurden.
   c. Optional können Sie auch Notizen zum Ereignis hinzufügen.
3. Im Bereich **Zusammenfassung** können Sie das Feld **Quelle** auswählen, um Details zum Quellvolume anzuzeigen.

   Das Feld **Source** enthält den Namen des Quellobjekts: in diesem Fall das Volume, auf dem der Snapshot-Kopierauftrag geplant war.

   Die Seite „Volume / Statusdetails“ für `cluster2_src_vol2` wird angezeigt und zeigt den Inhalt der Registerkarte „Schutz“.

4. Beim Betrachten des Schutztopologiediagramms ist ein Fehlersymbol beim ersten Volume in der Topologie zu sehen, das das Quellvolume für die SnapMirror Beziehung darstellt.

   Außerdem sehen Sie die horizontalen Balken im Quell-Volume-Symbol, die die für dieses Volume festgelegten Warn- und Fehlerschwellenwerte anzeigen.



5. Wenn Sie den Mauszeiger über das Fehlersymbol bewegen, wird das Popup-Dialogfeld mit den Schwellenwerteinstellungen angezeigt, und Sie sehen, dass das Volume den Fehlerschwellenwert überschritten hat, was auf ein Kapazitätsproblem hinweist.
6. Die Auswahl erfolgt über die Registerkarte **Kapazität**.

   Kapazitätsinformationen zu Volume `cluster2_src_vol2`Anzeigen.

7. Im Bereich **Capacity** ist im Balkendiagramm ein Fehlersymbol zu sehen, das erneut darauf hinweist, dass die Volume-Kapazität den für das Volume festgelegten Schwellenwert überschritten hat.
8. Unterhalb des Kapazitätsdiagramms ist zu sehen, dass die automatische Volume Erweiterung deaktiviert und eine Volume Speicherplatzzusage festgelegt wurde.

   Es wäre möglich, die automatische Erweiterung zu aktivieren, für dieses Szenario fällt die Entscheidung jedoch darauf, vor einer Entscheidung zur Behebung des Kapazitätsproblems weitere Untersuchungen durchzuführen.

9. Beim Herunterscrollen zur Liste **Events** ist zu sehen, dass die Ereignisse Protection Job Failed, Volume Days Until Full und Volume Space Full generiert wurden.
10. In der **Ereignisliste** klicken Sie auf das Ereignis **Volume Space Full**, um weitere Informationen zu erhalten, da Sie entschieden haben, dass dieses Ereignis für Ihr Kapazitätsproblem am relevantesten erscheint.

    Auf der Seite „Ereignisdetails“ wird das Ereignis „Volume-Speicherplatz voll“ für das Quell-Volume angezeigt.

11. Im Bereich **Summary** befindet sich für das Ereignis das Feld „Cause“: `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Unterhalb des Zusammenfassungsbereichs sehen Sie die vorgeschlagenen Korrekturmaßnahmen.

    Die vorgeschlagenen Korrekturmaßnahmen werden nur für bestimmte Ereignisse angezeigt, daher ist dieser Bereich nicht bei allen Ereignistypen sichtbar.

    Sie klicken sich durch die Liste der vorgeschlagenen Aktionen, die Sie zur Behebung des Events „Volume Space Full“ ausführen können:

- Die automatische Vergrößerung für dieses Volume aktivieren.
- Größe des Volumens ändern.
- Aktivierung und Ausführung der Deduplizierung auf diesem Volume.
- Für dieses Volume lässt sich die Komprimierung aktivieren und ausführen.

13. Sie beschließen, das automatische Wachstum des Volumes zu aktivieren; dazu müssen Sie jedoch den verfügbaren freien Speicherplatz auf dem übergeordneten Aggregat und die aktuelle Wachstumsrate des Volumes ermitteln:
    a. Das übergeordnete Aggregat, `cluster2_src_aggr1`, befindet sich im Bereich **Verwandte Geräte**.

    Sie können auf den Namen des Aggregats klicken, um weitere Details zum Aggregat zu erhalten.

    Sie stellen fest, dass das Aggregat über ausreichend Speicherplatz verfügt, um die automatische Vergrößerung des Volumes zu ermöglichen.

    b. Oben auf der Seite ist das Symbol zu sehen, das einen kritischen Incident anzeigt, sowie der Text unterhalb des Symbols.

    Sie stellen fest, dass „Tage bis zur vollständigen Belegung: Weniger als ein Tag | Tägliche Wachstumsrate: 5,4 %“ angezeigt wird.

14. Die `volume autogrow`Option kann im System Manager oder über die ONTAP CLI aktiviert werden.

    Die Namen des Volumes und des Aggregats sollten notiert werden, damit sie beim Aktivieren von autogrow verfügbar sind.

15. Nach Behebung des Kapazitätsproblems ist die Unified Manager **Ereignis**-Detailseite wieder aufzurufen und das Ereignis als gelöst zu markieren.

Behebung von Verzögerungsproblemen in Active IQ Unified Manager

Dieser Workflow zeigt beispielhaft, wie Sie ein Verzögerungsproblem beheben können. In diesem Szenario sind Sie Administrator oder Operator und greifen auf die Unified ManagerDashboard Seite zu, um zu prüfen, ob Probleme mit Ihren Schutzbeziehungen bestehen und gegebenenfalls Lösungen zu finden.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Auf der Dashboard-Seite sehen Sie im Bereich „Ungelöste Incidents und Risiken“ im Bereich „Schutz“ unter „Schutzrisiken“ einen SnapMirror Lag-Fehler.

Schritte

1. Im Bereich **Schutz** auf der Seite **Dashboard** den Verzögerungsfehler der SnapMirror Beziehung suchen und anklicken.

   Die Seite mit den Ereignisdetails für das Lag-Fehlerereignis erscheint.

2. Auf der Detailseite **Event** können Sie eine oder mehrere der folgenden Aufgaben ausführen:

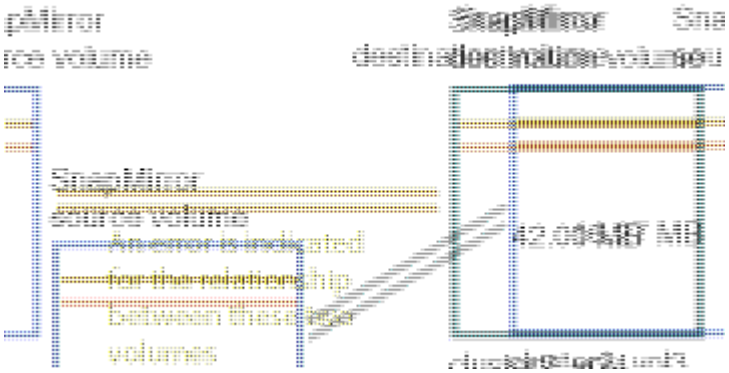
- Anhand der Fehlermeldung im Feld „Ursache“ des Zusammenfassungsbereichs lässt sich feststellen, ob eine Korrekturmaßnahme vorgeschlagen wird.
- Im Feld „Quelle“ des Bereichs „Zusammenfassung“ kann der Objektname, in diesem Fall ein Volume, ausgewählt werden, um Details zu diesem Volume zu erhalten.
- Möglicherweise wurden diesem Ereignis Notizen hinzugefügt.
- Dem Ereignis eine Notiz hinzufügen.
- Zuweisung des Ereignisses an einen bestimmten Benutzer.
- Das Ereignis bestätigen oder beheben.

3. In diesem Szenario klicken Sie im Feld „Quelle“ des Bereichs **Summary** auf den Objektnamen (in diesem Fall ein Volume), um Details zum Volume zu erhalten.

   Die Registerkarte „Schutz“ der Seite „Volume/Health-Details“ wird angezeigt.

4. Auf der Registerkarte **Schutz** sehen Sie das Topologiediagramm.

   Sie stellen fest, dass das Volume mit dem Lag-Fehler das letzte Volume in einer dreistufigen SnapMirror Kaskade ist. Das von Ihnen ausgewählte Volume ist dunkelgrau umrandet, und eine doppelte orange Linie vom Quell-Volume zeigt einen Fehler in der SnapMirror Beziehung an.



5. Jedes der Volumes in der SnapMirror Kaskade auswählen.

   Wenn Sie jedes Volume auswählen, ändern sich die Schutzinformationen in den Bereichen Zusammenfassung, Topologie, Verlauf, Ereignisse, Zugehörige Geräte und Zugehörige Warnungen und zeigen Details an, die für das ausgewählte Volume relevant sind.

6. Im Bereich **Zusammenfassung** liegt der Cursor für jedes Volume über dem Informationssymbol im Feld **Aktualisierungsplan**.

   In diesem Szenario stellen Sie fest, dass die SnapMirror Richtlinie DPDefault lautet und der SnapMirror Zeitplan stündlich fünf Minuten nach der vollen Stunde aktualisiert wird. Sie stellen fest, dass alle Volumes in der Beziehung versuchen, gleichzeitig einen SnapMirror Transfer abzuschließen.

7. Zur Behebung des Verzögerungsproblems werden die Zeitpläne für zwei der kaskadierten Volumes so geändert, dass jedes Ziel eine SnapMirror Übertragung startet, nachdem seine Quelle eine Übertragung abgeschlossen hat.

Schutzbeziehungen verwalten und überwachen

Informationen zur Verwaltung und Überwachung von Schutzbeziehungen in Active IQ Unified Manager

Active IQ Unified Manager ermöglicht es Ihnen, Schutzbeziehungen zu erstellen, SnapMirror- und SnapVault-Beziehungen auf verwalteten Clustern zu überwachen und Fehler zu beheben sowie Daten wiederherzustellen, wenn sie überschrieben wurden oder verloren gegangen sind.

Für SnapMirror Vorgänge gibt es zwei Replikationstypen:

- asynchron

  Die Replikation vom primären zum sekundären Volume wird durch einen Zeitplan gesteuert.

- Synchron

  Die Replikation erfolgt gleichzeitig auf dem primären und dem sekundären Volume.

Sie können bis zu 10 Schutzaufträge gleichzeitig ohne Performance-Einbußen ausführen. Bei 11 bis 30 gleichzeitig ausgeführten Aufträgen kann es zu Performance-Einbußen kommen. Die gleichzeitige Ausführung von mehr als 30 Aufträgen wird nicht empfohlen.

Anzeigen des Volume Schutzstatus in Active IQ Unified Manager

Die Seite „Datenschutz“ bietet einen ganzheitlichen Überblick über die Details zum Datenschutz für alle geschützten Volumes in einem einzelnen Cluster oder für alle Cluster in einem Datacenter.

Schritte

1. Im linken Navigationsbereich auf **Dashboard** klicken.
2. Je nachdem, ob Sie den Datenschutzstatus für alle überwachten Cluster oder für einen einzelnen Cluster anzeigen möchten, erfolgt die Auswahl im Dropdown-Menü über **Alle Cluster** oder über einen einzelnen Cluster.
3. Oben im Bereich Data Protection wählen Sie den Pfeil nach rechts aus. Die Seite **Data Protection** wird angezeigt.

Je nachdem, ob Sie einen einzelnen Cluster oder alle Cluster in Ihrem Datacenter ausgewählt haben, zeigt diese Seite den Datenschutzstatus der durch Snapshot-Kopien oder SnapMirror Richtlinien geschützten Volumes an und auch die Anzahl der ungeschützten Volumes.

Die Auswahl eines Clusters aus der Liste **Individual Cluster** zeigt den Snapshot-Schutz und den Status der SnapMirror Beziehung der geschützten Volumes in diesem Cluster an.

Ein Klick auf die Ereignisse auf dieser Seite führt zur Seite „Ereignisdetails“. Über den Link **View All** lassen sich alle aktiven Schutzereignisse auf der Inventarseite „Event Management“ anzeigen. Beim Bewegen des Mauszeigers darüber werden die jeweiligen Anzahlen und Legenden angezeigt. Folgendes kann angeklickt werden:

- Die Balkendiagramme für ungeschützte Volumes und durch Snapshot Kopien geschützte Volumes führen zur Seite „Volumes“, auf der die Details angezeigt werden.
- Die Balkendiagramme für alle Beziehungen führen zur Seite „Beziehungen“, auf der die Details nach dem Quell-Cluster gefiltert sind.

Schutzstatus der durch Snapshot Kopien geschützten Volumes

Überblick über Snapshot-Kopien: Ein Überblick über die durch Snapshot-Kopien geschützten Volumes, zum Beispiel:

- Die Gesamtzahl der Volumes, die durch Snapshot Kopien geschützt sind oder nicht.
- Die Gesamtzahl der Volumes, die den für die Snapshot Kopien reservierten Speicherplatz nutzen oder überschreiten.

Die **Analyse der Snapshot-Kopien** enthält folgende Informationen:

- Einzelne Ereignisse für Snapshot-Kopien, einschließlich der Ereignisse, die in den letzten 24 Stunden aufgetreten sind.
- Detailliertes Diagramm für durch Snapshot Kopien geschützte und nicht geschützte Volumes.
- Volumes, die die reservierte Snapshot-Kopiekapazität nutzen, nicht nutzen oder überschreiten.
- Aufschlüsselung der Volumenzahlen nach der Anzahl ihrer Snapshot Kopien.

Wichtige Hinweise zu Snapshot-Kopien

- Bei der Zählung der durch Snapshot Kopien geschützten Volumes werden sowohl Quell- als auch Ziel-Volumes berücksichtigt.
- Die Anzahl der zurückgegebenen Snapshot Kopien gilt nur für die Volumes, die online und verfügbar sind.
- Der Diagrammbereich für die Anzahl der Snapshot-Kopien ist dynamisch. Er wird basierend auf der Anzahl der im ausgewählten Cluster vorhandenen Snapshots generiert.
- Damit ein Volume als geschützt gilt, muss der Zeitplan für die Snapshot-Kopie des Volumes aktiviert sein.
- Der Wert für den reservierten Speicherplatz für Snapshot-Kopien ist wichtig, um die Menge des belegten Festplattenspeicherplatzes anzuzeigen oder den Speicherplatz zu berechnen, der freigegeben werden kann, wenn eine oder mehrere Snapshot-Kopien gelöscht werden.

Schutzstatus für SnapMirror Beziehungen

SnapMirror Übersicht: Ein Überblick über die durch SnapMirror Richtlinien geschützten Volumes, wie zum Beispiel:

- Die Anzahl der Volumes, die durch die jeweiligen SnapMirror Richtlinien geschützt sind, z. B. Volume SnapMirror Beziehungen, Storage VM Disaster Recovery (SVM-DR) und deren Kombinationen.
- Die Gesamtzahl der SnapMirror Beziehungen, die basierend auf dem Verzögerungsstatus eine Verzögerung des Recovery Point Objective (RPO) aufweisen.

SnapMirror Analyse enthält folgende Informationen:

- Einzelne Ereignisse, die für SnapMirror Beziehungen ausgelöst wurden, einschließlich der in den letzten 24 Stunden ausgelösten Ereignisse
- Die Anzahl der Volumes, die durch die jeweilige Art von SnapMirror Richtlinie geschützt sind.
- Die Anzahl der Beziehungen, die durch die SnapMirror Beziehungstypen geschützt sind, z. B. Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StricxtSync, SnapMirror Active Sync Konsistenzgruppe und Sync.
- Die Anzahl gesunder und ungesunder Beziehungen.
- Aufschlüsselung der Anzahl der Volume-Beziehungen. Die Diagramme lassen sich nach RPO-

Verzögerungszeit und Status umschalten.

- Verzögerungsschwellenwerte für eine nicht verwaltete Beziehung. Sie können auf das Einstellungssymbol ( ) klicken, um die Einstellungen für die Verzögerungsschwellenwerte zu konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von Lag-Schwellenwerteinstellungen für nicht gemanagte Schutzbeziehungen".

Wichtige Punkte für SnapMirror Beziehungen

- Für die Zählung von SnapMirror Beziehungen werden die Quell-Volumes gezählt, die für Lese- und Schreibzugriff aktiviert sind. Ziel- und Root-Volumes werden nicht berücksichtigt.
- Bei SnapMirror Beziehung werden die Ereignisse für den Quell-Cluster angezeigt.
- Die Anzahl der SnapMirror Beziehungen umfasst die Anzahl der Volumes mit Quellen und Zielen auf demselben oder auf verschiedenen Clustern.
- Die Verzögerungsdauer der RPO-Verzögerung bei der Datenreplizierung basiert auf der SnapMirror Beziehung. Der Status wird basierend auf dem festgelegten Schwellenwert der Beziehung als `ok`, `warning` oder `error` kategorisiert. Anhand des Status können Sie feststellen, ob die Parameter wie erwartet funktionieren oder ob Handlungsbedarf besteht.
- Wenn ein Volume mehrere SnapMirror Beziehungen aufweist, wird jeder Beziehungstyp für die RPO-Verzögerung mitgezählt.
- Volume-Beziehungen gelten als fehlerhaft, wenn es Probleme bei der Datenreplizierung zwischen Quelle und Ziel gibt, beispielsweise wenn die Beziehung unterbrochen ist.

Anzeige von Clustern, die durch die MetroCluster Konfiguration geschützt sind

Das Panel **MetroCluster Protection** auf der Seite **Data Protection** zeigt die Anzahl der Cluster an, die an Ihrem Standort durch MetroCluster über eine FC- oder IP-Konfiguration geschützt oder ungeschützt sind. Beim Klicken auf die Balkendiagramme in diesem Panel wird die Seite Clusters geöffnet, auf der die Clusterdetails anhand der geschützten oder ungeschützten Cluster gefiltert werden. Informationen zur Überwachung Ihrer MetroCluster Konfiguration finden Sie unter "Überwachung von MetroCluster Konfigurationen".

Anzeigen von Volumenschutzbeziehungen in Active IQ Unified Manager

In der Ansicht „Beziehungen: Alle Beziehungen“ und auf der Seite „Volumenbeziehungen“ können Sie den Status bestehender Volume SnapMirror und SnapVault Beziehungen anzeigen. Sie können außerdem Details zu Schutzbeziehungen prüfen, darunter Übertragungs- und Verzögerungsstatus, Quell- und Zieldetails sowie Informationen zu Zeitplan und Richtlinie.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können auch von dieser Seite aus Befehle für Beziehungen initiieren.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Beziehung** > **Alle Beziehungen**.

   Die Ansicht „Beziehung: Alle Beziehungen“ wird angezeigt.

3. Eine der folgenden Möglichkeiten steht zur Verfügung, um die Details zum Volume-Schutz anzuzeigen:
   - Aktuelle Informationen zu allen Volume-Beziehungen sind auf der Standardseite **Alle Beziehungen** verfügbar.
   - Detaillierte Informationen zu den Trends bei Volume-Übertragungen über einen bestimmten Zeitraum sind im Menü „Ansicht“ in der Ansicht „Beziehung: Übertragungsstatus des letzten Monats“ verfügbar.
   - Zum Anzeigen detaillierter Informationen über die Volume-Transfer-Aktivität auf Tagesbasis dient im Menü „View“ die Ansicht „Relationship: Last 1 month Transfer Rate“.

   Die Ansichten für Volumenübertragungen zeigen nur Informationen für Volumes in asynchronen Beziehungen an, Volumes in synchronen Beziehungen werden nicht angezeigt.

Überwachen von Consistency Group LUN Beziehungen in Active IQ Unified Manager

Wenn Ihre ONTAP Umgebung SnapMirror active sync zum Schutz von Anwendungen mit LUNs unterstützt, können Sie diese LUNs in Active IQ Unified Manager anzeigen und überwachen.

SnapMirror active sync gewährleistet beim Failover in SAN-Umgebungen ein Recovery Time Objective (RTO) von null. In einem typischen Deployment, das SnapMirror active sync unterstützt, werden die LUNs auf Volumes durch Konsistenzgruppenbeziehungen geschützt.

Diese primären und sekundären LUNs sind zusammengesetzte LUNs oder ein Replikat-LUN-Paar mit derselben UUID und Seriennummer. Die E/A-Vorgänge (sowohl lesen als auch schreiben) werden bei diesen zusammengesetzten LUNs über die Quell- und Zielstandorte multiplex ausgeführt, wodurch Transparenz gewährleistet ist.

Zum Anzeigen zusammengesetzter LUNs müssen sowohl der primäre als auch der sekundäre Cluster mit den LUNs, die Teil der Konsistenzgruppenbeziehung sind, in Unified Manager hinzugefügt und erkannt werden. Es werden nur iSCSI- und FCP-LUNs unterstützt.

Informationen zu SnapMirror active sync sind unter "ONTAP 9 Dokumentation für SnapMirror active sync (ehemals SM-BC)" verfügbar.

Die Anzeige zusammengesetzter LUNs in Ihrer Umgebung erfolgt in den folgenden Schritten:

Schritte

1. Im linken Navigationsbereich die Option **Storage** > **LUNs** auswählen.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Beziehung** > **Alle LUNs**.

   Die Ansicht „Beziehung: Alle LUNs“ wird angezeigt.

Sie können die LUN-Details anzeigen, z. B. den LUN-Namen, das Volume, die Storage VM, auf der die LUN gehostet wird, den Cluster, die Konsistenzgruppe und die Partner-LUN. Durch Klicken auf die einzelnen Komponenten gelangen Sie zu einer detaillierten Ansicht. Durch Klicken auf die Konsistenzgruppe gelangen Sie zur Seite „Beziehungen“.

Ein Klick auf die Partner-LUN zeigt deren Konfigurationsdetails auf der Registerkarte „SAN“ der Seite „Storage VM Details“ für die Storage VM an, auf der die Partner-LUN gehostet wird. Informationen wie Initiatoren und Initiatorgruppen sowie weitere Aspekte der Partner-LUN werden dort angezeigt.

Sie können die Standardfunktionen auf Grid-Ebene zum Sortieren, Filtern sowie zum Generieren und Hochladen von Berichten für die geschützten LUNs in Ihrer Umgebung ausführen.

Erstellung einer SnapVault Beziehung in der Ansicht „Gesundheit: Alle Volumes“ in Active IQ Unified Manager

Sie können die Ansicht „Integrität: Alle Volumes“ verwenden, um für ein oder mehrere Volumes auf derselben Storage VM SnapVault Beziehungen zu erstellen und so Datensicherungen zu Schutzzwecken zu ermöglichen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Das Menü **Protect** wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: beispielsweise wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn eine clusterübergreifende Beziehung besteht und der Ziel-Cluster noch nicht erkannt wurde

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. In der Ansicht **Integrität: Alle Volumes** können Sie ein Volume auswählen, das Sie schützen möchten, und auf **Schützen** klicken.

   Alternativ können Sie mehrere Schutzbeziehungen auf derselben Storage Virtual Machine (SVM) erstellen, indem Sie in der Ansicht „Health: All Volumes“ ein oder mehrere Volumes auswählen und in der Symbolleiste auf „Protect“ klicken.

3. Im Menü erfolgt die Auswahl von **SnapVault**.

   Das Dialogfeld „Schutz konfigurieren“ wird angezeigt.

4. Mit **SnapVault** lässt sich die Registerkarte **SnapVault** anzeigen und die Informationen zum sekundären Volume konfigurieren.
5. Über **Advanced** lassen sich Deduplizierung, Komprimierung, automatisches Wachstum und Speicherplatzzusage nach Bedarf festlegen; anschließend kann auf **Apply** geklickt werden.
6. Die Vervollständigung des Bereichs **Zielinformationen** und des Bereichs **Beziehungseinstellungen** erfolgt im **SnapVault** Tab.
7. Auf **Anwenden** klicken.

   Sie kehren zur Ansicht „Gesundheit: Alle Volumes“ zurück.

8. Der Link zum Schutzkonfigurationsjob befindet sich oben in der Ansicht **Integrität: Alle Volumes**.

   Wenn Sie nur eine Schutzbeziehung erstellen, wird die Seite „Auftragsdetails“ angezeigt. Wenn Sie jedoch mehr als eine Schutzbeziehung erstellen, wird eine gefilterte Liste aller Aufträge angezeigt, die mit dem Schutzvorgang verknüpft sind.

9. Führen Sie einen der folgenden Schritte aus:

- Wenn nur ein Auftrag vorhanden ist, kann die Aufgabenliste sowie die mit dem Schutzkonfigurationsauftrag verknüpften Aufgabendetails durch Klicken auf **Aktualisieren** aktualisiert werden, um festzustellen, wann der Auftrag abgeschlossen ist.
- Wenn Sie mehr als einen Job haben:
  i. In der Jobliste ist ein Job auszuwählen.
  ii. Mit **Aktualisieren** werden die Aufgabenliste und die mit dem Schutzkonfigurationsauftrag verbundenen Aufgabendetails aktualisiert, außerdem lässt sich feststellen, wann der Auftrag abgeschlossen ist.
  iii. Mit der Schaltfläche **Zurück** kehren Sie zur gefilterten Liste zurück und können einen anderen Job anzeigen.

Erstellung einer SnapVault Schutzbeziehung auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager

Sie können über die Seite „Volume / Integritätsdetails“ eine SnapVault Beziehung erstellen, sodass Datensicherungen zu Schutzzwecken auf Volumes aktiviert werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Voraussetzung für diese Aufgabe ist, dass Workflow Automation eingerichtet ist.

Das Menü **Protect** wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: beispielsweise wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn eine clusterübergreifende Beziehung besteht und der Ziel-Cluster noch nicht erkannt wurde

Schritte

1. Auf der Registerkarte **Schutz** der Detailseite **Volume / Health** lässt sich in der Topologieansicht ein Volume, das geschützt werden soll, mit der rechten Maustaste anklicken.
2. Die Auswahl erfolgt im Menü **Schützen** > **SnapVault**.

   Das Dialogfeld „Schutz konfigurieren“ wird angezeigt.
3. Durch Klicken auf **SnapVault** wird die **SnapVault** Registerkarte angezeigt, und die Informationen zur sekundären Ressource können konfiguriert werden.
4. Über **Advanced** lassen sich Deduplizierung, Komprimierung, automatisches Wachstum und Speicherplatzzusage nach Bedarf festlegen; anschließend kann auf **Apply** geklickt werden.
5. Im Dialogfeld **Schutz konfigurieren** sind die Bereiche **Zielinformationen** und **Beziehungseinstellungen** zu vervollständigen.
6. Auf **Anwenden** klicken.

   Sie gelangen zurück zur Seite „Volume / Health details“.
7. Oben auf der Detailseite **Volume / Health** befindet sich der Link zum Schutzkonfigurationsauftrag.

   Die Seite „Job details“ wird angezeigt.

8. Mit **Aktualisieren** werden die Aufgabenliste und die mit dem Schutzkonfigurationsauftrag verbundenen Aufgabendetails aktualisiert, außerdem lässt sich feststellen, wann der Auftrag abgeschlossen ist.

   Wenn die Aufgaben abgeschlossen sind, werden die neuen Beziehungen in der Topologieansicht der Detailseite „Volume / Health“ angezeigt.

Erstellung einer SnapMirror Beziehung in der Ansicht „Integrität: Alle Volumes“ in Active IQ Unified Manager

Die Ansicht „Integrität: Alle Volumes“ ermöglicht Ihnen, mehrere SnapMirror Schutzbeziehungen gleichzeitig zu erstellen, indem Sie mehr als ein Volume auf derselben Storage VM auswählen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Das Menü **Protect** wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: beispielsweise wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn eine clusterübergreifende Beziehung besteht und der Ziel-Cluster noch nicht erkannt wurde

Schritte

1. In der Ansicht **Health: All Volumes** wählen Sie das Volume aus, das Sie schützen möchten.

   Alternativ können Sie mehrere Schutzbeziehungen auf derselben SVM erstellen, indem Sie in der Ansicht „Integrität: Alle Volumes“ ein oder mehrere Volumes auswählen und in der Symbolleiste auf „Schützen“ > „SnapMirror“ klicken.

   Das Dialogfeld „Schutz konfigurieren“ wird angezeigt.

2. Durch Auswählen von **SnapMirror** lassen sich die Registerkarte **SnapMirror** anzeigen und die Zielinformationen konfigurieren.
3. Über **Erweitert** kann die Speicherplatzzusage bei Bedarf festgelegt werden; anschließend kann **Anwenden** ausgewählt werden.
4. Der Bereich **Destination Information** und der Bereich **Relationship Settings** werden in der Registerkarte **SnapMirror** vervollständigt.
5. Auf **Anwenden** klicken.

   Sie kehren zur Ansicht „Gesundheit: Alle Volumes“ zurück.

6. Oben in der Ansicht **Integrität: Alle Volumes** befindet sich der Link zum Konfigurationsauftrag für den Schutz.

   Wenn Sie nur eine Schutzbeziehung erstellen, wird die Seite mit den Jobdetails angezeigt; wenn Sie jedoch mehr als eine Schutzbeziehung erstellen, wird eine Liste aller Jobs angezeigt, die mit dem Schutzvorgang verknüpft sind.

7. Führen Sie einen der folgenden Schritte aus:

- Wenn nur ein Auftrag vorhanden ist, kann die Aufgabenliste sowie die mit dem Schutzkonfigurationsauftrag verknüpften Aufgabendetails durch Klicken auf **Aktualisieren** aktualisiert werden, um festzustellen, wann der Auftrag abgeschlossen ist.
- Wenn Sie mehr als einen Job haben:
  i. In der Jobliste ist ein Job auszuwählen.
  ii. Mit **Aktualisieren** werden die Aufgabenliste und die mit dem Schutzkonfigurationsauftrag verbundenen Aufgabendetails aktualisiert, außerdem lässt sich feststellen, wann der Auftrag abgeschlossen ist.
  iii. Mit der Schaltfläche **Zurück** kehren Sie zur gefilterten Liste zurück und können einen anderen Job anzeigen.

Abhängig von der Ziel-SVM, die Sie während der Konfiguration angegeben haben, oder von den Optionen, die Sie in Ihren erweiterten Einstellungen aktiviert haben, kann die resultierende SnapMirror Beziehung eine von mehreren möglichen Varianten aufweisen:

- Wenn Sie eine Ziel-SVM angegeben haben, die unter derselben oder einer neueren Version von ONTAP als das Quell-Volume ausgeführt wird, ist eine blockreplikationsbasierte SnapMirror Beziehung das Standardergebnis.
- Wenn Sie eine Ziel-SVM angegeben haben, die unter derselben oder einer neueren Version von ONTAP als das Quell-Volume ausgeführt wird, aber in den erweiterten Einstellungen die versionsflexible Replikation aktiviert haben, ist das Ergebnis eine SnapMirror Beziehung mit versionsflexibler Replikation.
- Wenn Sie eine Ziel-SVM angegeben haben, die unter einer früheren Version von ONTAP als das Quell-Volume ausgeführt wird, und wenn die frühere Version versionsflexible Replikation unterstützt, ist eine SnapMirror Beziehung mit versionsflexibler Replikation das automatische Ergebnis.

Erstellung einer SnapMirror Beziehung auf der Detailseite „Volume Health“ in Active IQ Unified Manager

Sie können die Seite „Volume-/Integritätsdetails“ verwenden, um eine SnapMirror Beziehung zu erstellen, sodass die Datenreplizierung zu Schutzzwecken aktiviert ist. SnapMirror Replizierung ermöglicht die Wiederherstellung von Daten aus dem Ziel-Volume bei Datenverlust auf dem Quell-Volume.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Das Menü **Protect** wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: beispielsweise wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn eine clusterübergreifende Beziehung besteht und der Ziel-Cluster noch nicht erkannt wurde

Sie können bis zu 10 Schutzaufträge gleichzeitig ohne Performance-Einbußen ausführen. Bei 11 bis 30 gleichzeitig ausgeführten Aufträgen kann es zu Performance-Einbußen kommen. Die gleichzeitige Ausführung von mehr als 30 Aufträgen wird nicht empfohlen.

Schritte

1. Auf der Detailseite **Volume / Health** ist auf der Registerkarte **Protection** in der Topologieansicht ein Rechtsklick auf den Namen des zu schützenden Volumes erforderlich.
2. Im Menü **Schützen** > **SnapMirror** auswählen.

   Das Dialogfeld „Schutz konfigurieren“ wird angezeigt.

3. Durch Auswählen von **SnapMirror** lassen sich die Registerkarte **SnapMirror** anzeigen und die Zielinformationen konfigurieren.
4. Über **Erweitert** kann die Speicherplatzzusage bei Bedarf festgelegt werden; anschließend kann **Anwenden** ausgewählt werden.
5. Im Dialogfeld **Schutz konfigurieren** sind die Bereiche **Zielinformationen** und **Beziehungseinstellungen** zu vervollständigen.
6. Auf **Anwenden** klicken.

   Sie gelangen zurück zur Seite „Volume / Health details“.

7. Oben auf der Detailseite **Volume / Health** befindet sich der Link zum Schutzkonfigurationsauftrag.

   Die Aufgaben und Details des Jobs werden auf der Seite „Job details“ angezeigt.

8. Auf der Seite **Auftragsdetails** aktualisiert **Aktualisieren** die Aufgabenliste und die mit dem Schutzkonfigurationsauftrag verknüpften Aufgabendetails; außerdem lässt sich damit feststellen, wann der Auftrag abgeschlossen ist.
9. Nach Abschluss der Aufgaben des Jobs gelangen Sie über **Back** in Ihrem Browser zur Detailseite **Volume / Health** zurück.

   Die neue Beziehung wird in der Topologieansicht der Seite „Volume / Gesundheitsdetails“ angezeigt.

Abhängig von der Ziel-SVM, die Sie während der Konfiguration angegeben haben, oder von den Optionen, die Sie in Ihren erweiterten Einstellungen aktiviert haben, kann die resultierende SnapMirror Beziehung eine von mehreren möglichen Varianten aufweisen:

- Wenn Sie eine Ziel-SVM angegeben haben, die unter derselben oder einer neueren Version von ONTAP als das Quell-Volume ausgeführt wird, ist eine blockreplikationsbasierte SnapMirror Beziehung das Standardergebnis.
- Wenn Sie eine Ziel-SVM angegeben haben, die unter derselben oder einer neueren Version von ONTAP als das Quell-Volume ausgeführt wird, aber in den erweiterten Einstellungen die versionsflexible Replikation aktiviert haben, ist das Ergebnis eine SnapMirror Beziehung mit versionsflexibler Replikation.
- Wenn Sie eine Ziel-SVM angegeben haben, die unter einer früheren Version von ONTAP oder unter einer Version ausgeführt wird, die höher ist als die des Quellvolumes, und wenn die frühere Version versionsflexible Replikation unterstützt, ist eine SnapMirror Beziehung mit versionsflexibler Replikation das automatische Ergebnis.

Erstellung einer SnapMirror Beziehung mit versionsflexibler Replikation in Active IQ Unified Manager

Eine SnapMirror Beziehung kann mit versionsflexibler Replikation erstellt werden. Die versionsflexible Replikation ermöglicht die Implementierung von SnapMirror Schutz, auch wenn Quell- und Zielvolumes unter unterschiedlichen Versionen von ONTAP ausgeführt werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.
- Sowohl die Quell- als auch die Ziel-SVMs müssen jeweils über eine aktivierte SnapMirror Lizenz verfügen.
- Die Quell- und Ziel-SVMs müssen jeweils unter einer Version der ONTAP Software ausgeführt werden, die versionsflexible Replikation unterstützt.

SnapMirror mit versionsflexibler Replikation ermöglicht die Implementierung von SnapMirror Schutz auch in heterogenen Storage Umgebungen, in denen nicht der gesamte Storage unter einer ONTAP Version ausgeführt wird. Spiegelungsvorgänge, die unter SnapMirror mit versionsflexibler Replikation ausgeführt werden, werden jedoch nicht so schnell ausgeführt wie unter der herkömmlichen Blockreplikation SnapMirror.

Schritte

1. Anzeige des Dialogfelds **Schutz konfigurieren** für das Volume, das geschützt werden soll.
   - Wenn die Registerkarte „Schutz“ auf der Seite „Volume-/Integritätsdetails“ angezeigt wird, können Sie in der Topologieansicht mit dem Namen eines Volumes, das geschützt werden soll, mit der rechten Maustaste klicken und im Menü **Schützen** > **SnapMirror** auswählen.
   - Wenn Sie die Ansicht „Integrität: Alle Volumes“ anzeigen, suchen Sie ein Volume, das Sie schützen möchten, klicken mit der rechten Maustaste darauf und wählen dann im Menü **Schützen** > **SnapMirror** aus. Daraufhin erscheint das Dialogfeld „Schutz konfigurieren“.
2. Zum Anzeigen der Registerkarte **SnapMirror** ist auf **SnapMirror** zu klicken.
3. Im Dialogfeld **Schutz konfigurieren** sind die Bereiche **Zielinformationen** und **Beziehungseinstellungen** zu vervollständigen.

   Wenn Sie eine Ziel-SVM angeben, auf der eine frühere Version von ONTAP ausgeführt wird als auf dem Quellvolume, das Sie schützen, und wenn diese frühere Version versionsflexible Replikation unterstützt, konfiguriert diese Aufgabe SnapMirror automatisch mit versionsflexibler Replikation.

4. Wenn Sie eine Ziel-SVM angeben, die mit derselben Version von ONTAP wie das Quell-Volume ausgeführt wird, aber SnapMirror dennoch mit versionsflexibler Replikation konfigurieren möchten, kann über **Advanced** die versionsflexible Replikation aktiviert und anschließend **Apply** ausgewählt werden.
5. Auf **Anwenden** klicken.

   Sie gelangen zurück zur Seite „Volume / Health details“.

6. Oben auf der Detailseite **Volume / Health** befindet sich der Link zum Schutzkonfigurationsauftrag.

   Die Aufgaben und Details des Jobs finden Sie auf der Seite „Job details“.

7. Auf der Seite **Auftragsdetails** aktualisiert **Aktualisieren** die Aufgabenliste und die mit dem Schutzkonfigurationsauftrag verknüpften Aufgabendetails; außerdem lässt sich damit feststellen, wann der Auftrag abgeschlossen ist.
8. Nach Abschluss der Aufgaben des Jobs gelangen Sie über **Back** in Ihrem Browser zur Detailseite **Volume / Health** zurück.

   Die neue Beziehung wird in der Topologieansicht der Seite „Volume / Gesundheitsdetails“ angezeigt.

Erstellung von SnapMirror Beziehungen mit versionsflexibler Replikation und Rückwärtsoptionsfunktion in Active IQ Unified Manager

Sie können eine SnapMirror Beziehung mit versionsflexibler Replikation und Backup-Option erstellen. Mit der Backup-Option können Sie SnapMirror Schutz implementieren und zudem mehrere Versionen von Backup-Kopien am Zielort aufbewahren.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.
- Sowohl die Quell- als auch die Ziel-SVMs müssen jeweils über eine aktivierte SnapMirror Lizenz verfügen.
- Sowohl die Quell- als auch die Ziel-SVMs müssen jeweils über eine aktivierte SnapVault Lizenz verfügen.
- Die Quell- und Ziel-SVMs müssen jeweils unter einer Version der ONTAP Software ausgeführt werden, die versionsflexible Replikation unterstützt.

Die Konfiguration von SnapMirror mit der Backup-Option ermöglicht es Ihnen, Ihre Daten mit Disaster-Recovery-Funktionen von SnapMirror, wie der Fähigkeit zum Volume Failover, zu schützen und gleichzeitig SnapVault Funktionen wie den Schutz mehrerer Backup-Kopien bereitzustellen.

Schritte

1. Anzeige des Dialogfelds **Schutz konfigurieren** für das Volume, das geschützt werden soll.
   - Wenn die Registerkarte „Schutz“ auf der Seite „Volume-/Integritätsdetails“ angezeigt wird, erfolgt in der Topologieansicht die Auswahl von **Protect** > **SnapMirror** im Kontextmenü des Namens eines Volumes, das geschützt werden soll.
   - Wenn die Ansicht „Health: All Volumes“ geöffnet ist, kann ein Volume, das geschützt werden soll, per Rechtsklick ausgewählt werden; anschließend ist im Menü **Protect** > **SnapMirror** zu wählen. Das Dialogfeld „Configure Protection“ wird angezeigt.
2. Zum Anzeigen der Registerkarte **SnapMirror** ist auf **SnapMirror** zu klicken.
3. Im Dialogfeld **Schutz konfigurieren** sind die Bereiche **Zielinformationen** und **Beziehungseinstellungen** zu vervollständigen.
4. Die Auswahl von **Erweitert** zeigt das Dialogfeld **Erweiterte Zieleinstellungen** an.
5. Falls das Kästchen **Version-Flexible Replication** noch nicht aktiviert ist, wird es jetzt aktiviert.
6. Zum Aktivieren der Backup-Option wird das Kästchen **With backup option** ausgewählt; anschließend wird auf **Apply** geklickt.
7. Auf **Anwenden** klicken.

   Sie gelangen zurück zur Seite „Volume / Health details“.

8. Oben auf der Detailseite **Volume / Health** befindet sich der Link zum Schutzkonfigurationsauftrag.

   Die Aufgaben und Details des Jobs finden Sie auf der Seite „Job details“.

9. Auf der Seite **Auftragsdetails** wird durch Klicken auf **Aktualisieren** die Aufgabenliste sowie die mit dem Schutzkonfigurationsauftrag verknüpften Aufgabendetails aktualisiert, und es lässt sich feststellen, wann der Auftrag abgeschlossen ist.
10. Nach Abschluss der Aufgaben des Jobs gelangen Sie über **Back** in Ihrem Browser zur Detailseite **Volume / Health** zurück.

Die neue Beziehung wird in der Topologieansicht der Seite „Volume / Gesundheitsdetails“ angezeigt.

Konfiguration der Zieleffizienzeinstellungen in Active IQ Unified Manager

Im Dialogfeld „Erweiterte Zieleinstellungen“ können Sie die Effizienzeinstellungen für ein Schutzziel konfigurieren, z. B. Deduplizierung, Komprimierung, automatisches Wachstum und Speicherplatzzusage. Sie verwenden diese Einstellungen, wenn Sie die Speicherplatznutzung auf einem Ziel oder sekundären Volume maximieren möchten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Standardmäßig entsprechen die Effizienzeinstellungen denen des Quell-Volumes, mit Ausnahme der Komprimierungseinstellungen in einer SnapVault Beziehung, die standardmäßig deaktiviert sind.

Schritte

1. Im Dialogfeld **Schutz konfigurieren** hängt die Auswahl der Registerkarte **SnapMirror** bzw. **SnapVault** vom Typ der zu konfigurierenden Beziehung ab.
2. Im Bereich **Zielinformationen** kann **Erweitert** ausgewählt werden.

   Das Dialogfeld „Erweiterte Zieleinstellungen“ wird geöffnet.
3. Die Effizienzeinstellungen für Deduplizierung, Komprimierung, automatisches Wachstum und Speicherplatzzusage können je nach Bedarf aktiviert oder deaktiviert werden.
4. Wenn Sie **Anwenden** auswählen, wird Ihre Auswahl gespeichert, und Sie kehren zum Dialogfeld **Schutz konfigurieren** zurück.

Erstellung von SnapMirror und SnapVault Zeitplänen in Active IQ Unified Manager

Sie können einfache oder erweiterte SnapMirror- und SnapVaultZeitpläne erstellen, um automatische Transfers zum Schutz von Daten auf einem Quell- oder Primär-Volume zu aktivieren, sodass die Transfers je nachdem, wie häufig sich die Daten auf Ihren Volumes ändern, häufiger oder seltener erfolgen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Der Bereich „Destination Information“ im Dialogfeld „Configure Protection“ muss bereits ausgefüllt sein.
- Voraussetzung für diese Aufgabe ist, dass Workflow Automation eingerichtet ist.

Schritte

1. Auf der Registerkarte **SnapMirror** oder **SnapVault** des Dialogfelds **Schutz konfigurieren** befindet sich im Bereich **Beziehungseinstellungen** der Link **Zeitplan erstellen**.

   Das Dialogfeld „Zeitplan erstellen“ wird angezeigt.
2. Im Feld **Terminplanname** können Sie den gewünschten Namen für den Terminplan eingeben.
3. Wählen Sie eine der folgenden Optionen aus:
   - **Standard**

Diese Option wird verwendet, wenn Sie einen einfachen Intervallplan erstellen möchten.

- **Fortschrittlich**

  Diese Option ist für das Erstellen eines Zeitplans im Cron-Stil vorgesehen.

4. Klicken Sie auf **Create**.

   Der neue Zeitplan wird in der Dropdown-Liste SnapMirror Zeitplan oder SnapVault Zeitplan angezeigt.

Die Erweiterung des Schutzes mithilfe von Kaskaden- oder Fanout-Beziehungen in Active IQ Unified Manager

Sie können den Schutz einer bestehenden Beziehung erweitern, indem Sie entweder einen Fanout vom Quellvolume oder eine Kaskade vom Zielvolume einer bestehenden Beziehung erstellen. Dies kann beispielsweise sinnvoll sein, wenn Sie Daten von einem Standort auf mehrere Standorte kopieren oder zusätzlichen Schutz durch die Erstellung weiterer Backups gewährleisten möchten.

Sie können den Schutz mithilfe einer Konsistenzgruppe auf Volumes ausweiten. Eine Konsistenzgruppe ist ein Container, der mehrere Volumes enthält, sodass Sie alle Volumes als eine Einheit managen können. Sie können die SnapMirror active sync Konsistenzgruppe und die synchrone Konsistenzgruppenbeziehung auf der Seite „Beziehungen“ von Unified Manager anzeigen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Schritte

1. Die Auswahl erfolgt über **Schutz** > **Beziehungen**. Alternativ können Sie die Beziehungen auf der Seite mit den Volumendetails einsehen.
2. Auf der Seite **Volume-Beziehungen** erfolgt die Auswahl der SnapMirror Beziehung, für die der Schutz erweitert werden soll.
3. In der Aktionsleiste erfolgt die Auswahl von **Schutz erweitern**.
4. Im Menü ist je nachdem, ob eine Fanout-Beziehung von der Quelle oder eine Kaskadenbeziehung vom Ziel erstellt werden soll, entweder **Von Quelle** oder **Von Ziel** auszuwählen.
5. Je nach Art der Schutzbeziehung, die Sie erstellen, erfolgt die Auswahl entweder über **Mit SnapMirror** oder **Mit SnapVault**.

   Das Dialogfeld **Schutz konfigurieren** wird angezeigt.

   Dies kann auf der Seite „unified relationship / Volume Relationship“ und „Volume / Health details“ erreicht werden.

6. Sie vervollständigen die Informationen wie im Dialogfeld **Schutz konfigurieren** angegeben.

Auf der Seite „Volume-Beziehungen“ in Active IQ Unified Manager können Schutzbeziehungen bearbeitet werden

Sie können bestehende Schutzbeziehungen bearbeiten, um die maximale Transferrate, die Datensicherungsstrategie oder den Schutzzeitplan zu ändern. Sie können beispielsweise eine Beziehung bearbeiten, um die für Übertragungen verwendete Bandbreite zu verringern oder die Häufigkeit geplanter Übertragungen zu erhöhen, weil sich die Daten häufig ändern.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die ausgewählten Volumes müssen Ziele von Datensicherungsbeziehungen sein. Beziehungen können nicht bearbeitet werden, wenn Quell-Volumes, Load-Sharing-Volumes oder Volumes ausgewählt sind, die nicht das Ziel einer SnapMirror oder SnapVault Beziehung sind.

Schritte

1. Auf der Seite **Volume Relationships** sind in der Volume-Liste ein oder mehrere Volumes in derselben SVM auszuwählen, deren Beziehungseinstellungen bearbeitet werden sollen; anschließend ist in der Symbolleiste **Edit** auszuwählen.

   Das Dialogfeld „Beziehung bearbeiten“ wird angezeigt.

2. Im Dialogfeld **Beziehung bearbeiten** lassen sich bei Bedarf die maximale Transferrate, die Datensicherungsstrategie oder der Sicherungszeitplan bearbeiten.
3. Auf **Anwenden** klicken.

   Die Änderungen gelten für die ausgewählten Beziehungen.

Auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager können Schutzbeziehungen bearbeitet werden

Sie können bestehende Sicherungsbeziehungen bearbeiten, um die aktuelle maximale Transferrate, Datensicherungsstrategie oder den aktuellen Sicherungszeitplan zu ändern. Eine Beziehung kann bearbeitet werden, um die für Übertragungen verwendete Bandbreite zu verringern oder die Häufigkeit geplanter Übertragungen zu erhöhen, weil sich die Daten häufig ändern.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation installiert und konfiguriert haben.

Die ausgewählten Volumes müssen Ziele von Datensicherungsbeziehungen sein. Beziehungen können nicht bearbeitet werden, wenn Quell-Volumes, Load-Sharing-Volumes oder Volumes ausgewählt sind, die nicht das Ziel einer SnapMirror oder SnapVault Beziehung sind.

Schritte

1. Auf der Registerkarte **Protection** der Detailseite **Volume / Health** in der Topologie die zu bearbeitende Schutzbeziehung lokalisieren und mit der rechten Maustaste anklicken.
2. Die Auswahl im Menü erfolgt über **Bearbeiten**.

Alternativ können Sie im Menü **Aktionen** die Option **Beziehung** > **Bearbeiten** auswählen, um die Beziehung zu bearbeiten, deren Details Sie gerade anzeigen.

Das Dialogfeld **Beziehung bearbeiten** wird angezeigt.

3. Im Dialogfeld „Beziehung bearbeiten“ lassen sich die maximale Transferrate, die Datensicherungsstrategie oder der Sicherungszeitplan nach Bedarf bearbeiten.
4. Auf **Anwenden** klicken.

Die Änderungen gelten für die ausgewählten Beziehungen.

Eine SnapMirror Richtlinie zur Maximierung der Übertragungseffizienz in Active IQ Unified Manager erstellen

Sie können eine SnapMirror Richtlinie erstellen, um die SnapMirror Übertragungspriorität für Schutzbeziehungen festzulegen. SnapMirror Richtlinien ermöglichen es Ihnen, die Übertragungseffizienz von der Quelle zum Ziel zu maximieren, indem Sie Prioritäten zuweisen, sodass Übertragungen mit niedrigerer Priorität nach Übertragungen mit normaler Priorität eingeplant werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.
- Diese Aufgabe setzt voraus, dass Sie den Bereich „Zielinformationen“ im Dialogfeld „Schutz konfigurieren“ bereits ausgefüllt haben.

Schritte

1. Im Dialogfeld **Configure Protection** lässt sich auf der Registerkarte **SnapMirror** im Bereich **Relationship Settings** der Link **Create Policy** auswählen.

   Das Dialogfeld zum Erstellen der SnapMirror Richtlinie wird angezeigt.

2. Im Feld **Richtlinienname** ist ein Name einzugeben, den Sie der Richtlinie geben möchten.
3. Im Feld **Übertragungspriorität** wird die Übertragungspriorität ausgewählt, die der Richtlinie zugewiesen werden soll.
4. Im Feld **Comment** können Sie optional einen Kommentar für die Richtlinie eingeben.
5. Klicken Sie auf **Create**.

   Die neue Richtlinie wird in der Dropdown-Liste SnapMirror Policy angezeigt.

Erstellung einer SnapVault Richtlinie zur Maximierung der Übertragungseffizienz in Active IQ Unified Manager

Sie können eine neue SnapVault Richtlinie erstellen, um die Priorität für eine SnapVault Übertragung festzulegen. Richtlinien werden verwendet, um die Effizienz von Transfers vom primären zum sekundären System in einer Datensicherungsbeziehung zu maximieren.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.
- Sie müssen den Bereich „Zielinformationen“ im Dialogfeld „Schutz konfigurieren“ bereits ausgefüllt haben.

Schritte

1. Auf der Registerkarte **SnapVault** des Dialogfelds **Configure Protection** befindet sich im Bereich **Relationship Settings** der Link **Create Policy**.

   Der SnapVault Tab wird angezeigt.

2. Im Feld **Richtlinienname** können Sie den Namen eingeben, den Sie der Richtlinie geben möchten.
3. Im Feld **Übertragungspriorität** ist die Übertragungspriorität auszuwählen, die der Richtlinie zugewiesen werden soll.
4. **Optional:** Im Feld **Kommentar** kann ein Kommentar für die Richtlinie eingegeben werden.
5. Im Bereich **Replikationsbezeichnung** können Sie bei Bedarf eine Replikationsbezeichnung hinzufügen oder bearbeiten.
6. Klicken Sie auf **Create**.

   Die neue Richtlinie wird in der Dropdown-Liste „Richtlinie erstellen“ angezeigt.

Abbrechen einer Übertragung auf der Seite „Volume Beziehungen“ in Active IQ Unified Manager

Sie können einen aktiven Datenschutztransfer abbrechen, wenn Sie eine laufende SnapMirror Replikation stoppen möchten. Sie können auch den Neustart-Checkpoint für Übertragungen nach dem Basistransfer löschen. Ein Transfer kann beispielsweise abgebrochen werden, wenn er mit einem anderen Vorgang, wie etwa dem Verschieben eines Volume, in Konflikt steht.

Sie können keine Volume-Beziehungen abbrechen, die durch die Consistency Group geschützt sind.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Die Abbruchoption ist in den folgenden Fällen nicht verfügbar:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: beispielsweise wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn eine clusterübergreifende Beziehung besteht und der Ziel-Cluster noch nicht erkannt wurde

Der Neustart-Checkpoint für einen Basistransfer kann nicht gelöscht werden.

Schritte

1. Zum Abbrechen von Übertragungen für eine oder mehrere Schutzbeziehungen können auf der Seite **Volume Relationships** ein oder mehrere Volumes ausgewählt und anschließend in der Symbolleiste

Abort angeklickt werden.

Das Dialogfeld „Übertragung abbrechen“ wird angezeigt.

2. Wenn der Neustart-Checkpoint für einen Transfer gelöscht werden soll, der kein Basistransfer ist, steht **Checkpoints löschen** zur Verfügung.
3. Klicken Sie auf **Weiter**.

   Das Dialogfeld „Abort Transfer“ wird geschlossen, und der Status des Abbruchjobs wird oben auf der Seite „Volume Relationships“ zusammen mit einem Link zu den Jobdetails angezeigt.

4. **Optional:** Über den Link **View details** gelangen Sie zur Detailseite **Job**, auf der zusätzliche Details und der Auftragsfortschritt angezeigt werden.

Abbrechen einer Übertragung auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager

Sie können einen aktiven Datentransfer abbrechen, wenn Sie eine laufende SnapMirror Replikation beenden möchten. Außerdem können Sie den Neustart Checkpoint für eine Übertragung löschen, wenn es sich nicht um einen Basistransfer handelt. Sie können eine Übertragung abbrechen, wenn sie mit einem anderen Vorgang, etwa dem Verschieben eines Volumes, in Konflikt steht.

Sie können keine Volume-Beziehungen abbrechen, die durch die Consistency Group geschützt sind.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Die Abbruchoption ist in den folgenden Fällen nicht verfügbar:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: beispielsweise wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn eine clusterübergreifende Beziehung besteht und der Ziel-Cluster noch nicht erkannt wurde

Der Neustart-Checkpoint für einen Basistransfer kann nicht gelöscht werden.

Schritte

1. Auf der Registerkarte **Schutz** der Detailseite **Volume / Integrität** wird in der Topologieansicht für den Datentransfer, der abgebrochen werden soll, die Beziehung mit der rechten Maustaste angeklickt und anschließend **Abbrechen** ausgewählt.

   Das Dialogfeld „Übertragung abbrechen“ wird angezeigt.

2. Wenn der Neustart-Checkpoint für einen Transfer gelöscht werden soll, der kein Basistransfer ist, steht **Checkpoints löschen** zur Verfügung.
3. Klicken Sie auf **Weiter**.

   Das Dialogfeld „Übertragung abbrechen“ wird geschlossen, und oben auf der Seite „Volume /

Integritätsdetails“ erscheint der Status des Abbruchvorgangs zusammen mit einem Link zu den Auftragsdetails.

4. **Optional:** Über den Link **View details** gelangen Sie zur Detailseite **Job**, auf der zusätzliche Details und der Auftragsfortschritt angezeigt werden.
5. Die Details der einzelnen Arbeitsaufgaben lassen sich durch Klicken auf die jeweilige Aufgabe anzeigen.
6. Über den Zurück-Pfeil in Ihrem Browser gelangen Sie zurück zur Detailseite **Volume / Health**.

   Der Abbruchvorgang ist beendet, wenn alle Job-Aufgaben erfolgreich abgeschlossen sind.

Eine Schutzbeziehung auf der Seite „Volume Beziehungen“ in Active IQ Unified Manager anhalten

Auf der Seite „Volume-Beziehungen“ können Sie eine Schutzbeziehung anhalten, um Datenübertragungen vorübergehend zu verhindern. Dies kann beispielsweise sinnvoll sein, wenn Sie eine Snapshot Kopie eines SnapMirror Ziel-Volumes erstellen möchten, das eine Datenbank enthält, und sicherstellen möchten, dass sein Inhalt während des Vorgangs zum Erstellen der Snapshot Kopie stabil bleibt.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Die Quiesce-Aktion wird in folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen; z. B. wenn Sie nur über Bedienerrechte verfügen
- Wenn die Volume-ID unbekannt ist, beispielsweise bei einer clusterübergreifenden Beziehung, wenn der Ziel-Cluster noch nicht erkannt wurde
- Wenn Sie Workflow Automation und Unified Manager noch nicht gekoppelt haben

Schritte

1. Übertragungen für eine oder mehrere Schutzbeziehungen lassen sich auf der Seite **Volume Relationships** anhalten, indem ein oder mehrere Volumes ausgewählt und in der Symbolleiste **Quiesce** angeklickt werden.

   Das Dialogfeld „Quiesce“ wird angezeigt.

2. Klicken Sie auf **Weiter**.

   Oben auf der Seite „Volume / Zustandsdetails“ erscheint der Status des Quiesce-Jobs zusammen mit einem Link zu den Jobdetails.

3. Über den Link **Details anzeigen** sind auf der **Job**-Detailseite zusätzliche Details und der Fortschritt des Jobs verfügbar.
4. **Optional:** Über den Pfeil **Back** in Ihrem Browser ist die Rückkehr zur Seite **Volume Relationships** möglich.

   Der Quiesce-Job ist abgeschlossen, wenn alle Aufgaben des Jobs erfolgreich abgeschlossen sind.

Eine Schutzbeziehung auf der Seite „Volume-/Gesundheitsdetails“ in Active IQ Unified Manager anhalten

Sie können eine Schutzbeziehung stillsetzen, um Datentransfers vorübergehend zu verhindern. Dies kann beispielsweise sinnvoll sein, wenn Sie eine Snapshot-Kopie eines SnapMirror Ziel-Volumes erstellen möchten, das eine Datenbank enthält, und sichergehen möchten, dass sein Inhalt während der Snapshot-Kopie stabil bleibt.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Die Quiesce-Aktion wird in folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, beispielsweise wenn Sie nur über Bedienerrechte verfügen
- Wenn die Volume-ID unbekannt ist, beispielsweise bei einer clusterübergreifenden Beziehung, wenn der Ziel-Cluster noch nicht ermittelt wurde
- Wenn Sie Workflow Automation und Unified Manager noch nicht gekoppelt haben

Schritte

1. Auf der Registerkarte **Schutz** der Detailseite **Volume / Integrität** lässt sich in der Topologieansicht die Beziehung für die Schutzbeziehung, die angehalten werden soll, per Rechtsklick auswählen.
2. Im Menü erfolgt die Auswahl von **Quiesce**.
3. Klicken Sie auf **Yes**, um fortzufahren.

   Oben auf der Seite „Volume / Zustandsdetails“ erscheint der Status des Quiesce-Jobs zusammen mit einem Link zu den Jobdetails.

4. Über den Link **Details anzeigen** sind auf der **Job**-Detailseite zusätzliche Details und der Fortschritt des Jobs verfügbar.
5. **Optional:** Über den Zurück-Pfeil im Browser ist die Rückkehr zur Detailseite **Volume / Health** möglich.

   Der Quiesce-Job ist abgeschlossen, wenn alle Aufgaben des Jobs erfolgreich abgeschlossen sind.

Eine SnapMirror Beziehung auf der Seite „Volume Beziehungen“ von Active IQ Unified Manager aufheben

Sie können eine Schutzbeziehung aufheben, um Datentransfers zwischen einem Quell-Volume und einem Ziel-Volume in einer SnapMirror Beziehung zu stoppen. Eine Beziehung kann beispielsweise für die Datenmigration, die Notfallwiederherstellung oder für Applikationstests aufgehoben werden. Das Ziel-Volume wird in ein lesen/schreiben-Volume geändert. Eine SnapVault Beziehung kann nicht aufgehoben werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Schritte

1. Auf der Seite **Volume-Beziehungen** sind ein oder mehrere Volumes mit Schutzbeziehungen auszuwählen, für die der Datentransfer gestoppt werden soll; anschließend ist in der Symbolleiste auf **Unterbrechen** zu klicken.

   Das Dialogfeld „Beziehung aufheben“ wird angezeigt.

2. Über **Weiter** lässt sich die Beziehung beenden.
3. Auf der Seite **Volume-Beziehungen** muss in der Spalte **Beziehungsstatus** ersichtlich sein, dass die Beziehung unterbrochen ist.

   Die Spalte „Beziehungsstatus“ ist standardmäßig ausgeblendet, sodass Sie sie möglicherweise in der Liste der ein-/ausblendbaren Spalten auswählen müssen .

Das Entfernen einer Schutzbeziehung von der Seite „Volume Relationships“ in Active IQ Unified Manager

Auf der Seite „Volume-Beziehungen“ können Sie eine Schutzbeziehung entfernen, um eine bestehende Beziehung zwischen der ausgewählten Quelle und dem Ziel dauerhaft zu löschen, beispielsweise wenn Sie eine Beziehung mit einem anderen Ziel erstellen möchten. Dieser Vorgang entfernt alle Metadaten und kann nicht rückgängig gemacht werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Schritte

1. Auf der Seite **Volume Relationships** können Sie ein oder mehrere Volumes mit Schutzbeziehungen auswählen, die entfernt werden sollen, und anschließend in der Symbolleiste auf **Remove** klicken.

   Das Dialogfeld „Beziehung entfernen“ wird angezeigt.

2. Mit **Weiter** lässt sich die Beziehung entfernen.

   Die Beziehung wird von der Seite „Volume Relationships“ entfernt.

Geplante Transfers für eine ruhende Beziehung können auf der Seite „Volumenbeziehungen“ in Active IQ Unified Manager fortgesetzt werden

Nachdem Sie eine Beziehung in den Ruhezustand versetzt haben, um geplante Übertragungen zu stoppen, können Sie mit **Resume** geplante Übertragungen wieder aktivieren, sodass die Daten auf dem Quell- oder Primär-Volume geschützt bleiben. Beim nächsten geplanten Übertragungsintervall werden die Übertragungen, sofern vorhanden, von einem Checkpoint aus fortgesetzt.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Sie können maximal 10 ruhende Beziehungen auswählen, für die Übertragungen wieder aufgenommen

werden sollen.

Schritte

1. Auf der Seite „Volume Beziehungen“ lassen sich ein oder mehrere Volumes mit angehaltenen Beziehungen auswählen; in der Symbolleiste kann anschließend auf „Fortsetzen“ geklickt werden.
2. Im Dialogfeld **Resume** wählen Sie **Continue**.

   Sie kehren zur Seite „Volume Relationships“ zurück.
3. Die zugehörigen Job-Aufgaben und ihr Fortschritt lassen sich über den Job-Link anzeigen, der oben auf der Seite **Volume Relationships** angezeigt wird.
4. Führen Sie einen der folgenden Schritte aus:
   - Wenn nur ein Auftrag angezeigt wird, können auf der Seite „Auftragsdetails“ durch Klicken auf **Aktualisieren** die Aufgabenliste und die mit dem Schutzkonfigurationsauftrag verknüpften Aufgabendetails aktualisiert sowie der Abschluss des Auftrags festgestellt werden.
   - Wenn mehr als ein Job angezeigt wird,
     i. Auf der Seite „Jobs“ lässt sich der Job auswählen, dessen Details angezeigt werden sollen.
     ii. Auf der Seite „Auftragsdetails“ dient **Aktualisieren** dazu, die Aufgabenliste und die zugehörigen Aufgabendetails des Schutzkonfigurationsauftrags zu aktualisieren und festzustellen, wann der Auftrag abgeschlossen ist. Nach Abschluss der Aufträge werden die Datenübertragungen im nächsten geplanten Übertragungsintervall fortgesetzt.

Fortsetzen von Übertragungen in einer angehaltenen Beziehung auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager

Nachdem Sie eine Beziehung in den Ruhezustand versetzt haben, um zu verhindern, dass geplante Übertragungen stattfinden, können Sie auf der Seite „Volume-/Integritätsdetails“ **Resume** verwenden, um geplante Übertragungen wieder zu aktivieren, sodass die Daten auf dem Quell- oder primären Volume geschützt sind. Die Übertragungen werden beim nächsten geplanten Übertragungsintervall von einem Checkpoint aus fortgesetzt, sofern ein solcher vorhanden ist.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Schritte

1. Auf der Registerkarte **Schutz** der Detailseite **Volume / Integrität** kann in der Topologieansicht mit der rechten Maustaste auf eine angehaltene Beziehung geklickt werden, die fortgesetzt werden soll.

   Alternativ kann im Menü **Aktionen** > **Beziehung** die Option **Fortsetzen** ausgewählt werden.
2. Im Dialogfeld **Resume** wählen Sie **Continue**.

   Sie gelangen zurück zur Seite „Volume / Health details“.
3. Die zugehörigen Job-Aufgaben und ihr Fortschritt lassen sich über den Job-Link oben auf der Detailseite **Volume / Health** anzeigen und nachverfolgen.

4. Auf der Seite **Auftragsdetails** aktualisiert **Aktualisieren** die Aufgabenliste und die mit dem Schutzkonfigurationsauftrag verknüpften Aufgabendetails; außerdem lässt sich damit feststellen, wann der Auftrag abgeschlossen ist.

   Nach Abschluss der Jobs werden die Datenübertragungen beim nächsten geplanten Übertragungsintervall wieder aufgenommen.

Schutzbeziehungen können auf der Seite „Volume Beziehungen“ in Active IQ Unified Manager initialisiert oder aktualisiert werden

Auf der Seite „Volume Relationships“ können Sie für eine neue Schutzbeziehung einen erstmaligen Basistransfer durchführen oder eine Beziehung aktualisieren, wenn sie bereits initialisiert ist und Sie eine manuelle, ungeplante inkrementelle Aktualisierung für eine sofortige Übertragung durchführen möchten.

Durch Konsistenzgruppen geschützte Volumes können nicht initialisiert oder aktualisiert werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Auf der Seite **Volume Relationships** können Sie mit der rechten Maustaste auf ein Volume klicken und ein oder mehrere Volumes mit Beziehungen auswählen, die aktualisiert oder initialisiert werden sollen; anschließend klicken Sie in der Symbolleiste auf **Initialize/Update**.

   Das Dialogfeld **Initialisieren/Aktualisieren** wird angezeigt.

2. Im Reiter **Übertragungsoptionen** erfolgt die Auswahl einer Übertragungspriorität und der maximalen Transferrate.
3. Nach einem Klick auf **Source Snapshot Copies** ist in der Spalte **Snapshot Copy** auf **Default** zu klicken.

   Das Dialogfeld „Quell-Snapshot-Kopie auswählen“ wird angezeigt.

4. Zum Angeben einer vorhandenen Snapshot-Kopie anstelle der Standard-Snapshot-Kopie ist **Vorhandene Snapshot Copy** anzuklicken und eine Snapshot-Kopie aus der Liste auszuwählen.
5. Anschließend **Absenden** auswählen.

   Daraufhin befinden Sie sich wieder im Dialogfeld **Initialisieren/Aktualisieren**.

6. Wenn Sie mehr als eine Quelle zum Initialisieren oder Aktualisieren ausgewählt haben, erfolgt für die nächste Quelle, für die Sie eine vorhandene Snapshot-Kopie angeben möchten, die Auswahl von **Default**.
7. Mit **Submit** wird der Initialisierungs- oder Aktualisierungsjob gestartet.

   Nach dem Start des Initialisierungs- oder Aktualisierungsauftrags gelangen Sie zurück zur Seite „Volume Relationships“, und oben auf der Seite wird ein Link zu den Aufträgen angezeigt.

8. **Optional:** In der Ansicht **Zustand: Alle Volumes** kann über **Aufträge anzeigen** der Status jedes Initialisierungs- oder Aktualisierungsauftrags verfolgt werden.

   Eine gefilterte Liste der Jobs wird angezeigt.

9. **Optional:** Die Details der einzelnen Aufträge lassen sich durch Klicken auf den jeweiligen Auftrag anzeigen.
10. **Optional:** Über den Pfeil **Back** in Ihrem Browser ist die Rückkehr zur Seite **Volume Relationships** möglich.

    Der Initialisierungs- oder Aktualisierungsvorgang ist beendet, wenn alle Aufgaben erfolgreich abgeschlossen sind.

Schutzbeziehungen können auf der Seite „Volume-/Integritätsdetails“ in Active IQ Unified Manager initialisiert oder aktualisiert werden

Sie können einen erstmaligen Basistransfer für eine neue Schutzbeziehung durchführen oder eine bereits initialisierte Beziehung aktualisieren, wenn Sie eine manuelle, ungeplante inkrementelle Aktualisierung durchführen möchten, um Daten sofort zu übertragen.

HINWEIS: Durch Consistency Groups geschützte Volumes können nicht initialisiert oder aktualisiert werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Auf der Registerkarte **Schutz** der Detailseite **Volume / Integrität** die Schutzbeziehung in der Topologie auswählen, die initialisiert oder aktualisiert werden soll, und dann mit der rechten Maustaste darauf klicken.
2. Im Menü ist **Initialize/Update** auszuwählen.

   Alternativ steht im Menü **Aktionen** die Option **Beziehung** > **Initialisieren/Aktualisieren** zum Initialisieren oder Aktualisieren der Beziehung zur Verfügung, deren Details derzeit angezeigt werden.

   Das Dialogfeld „Initialisieren/Aktualisieren“ wird angezeigt.
3. Im Reiter **Übertragungsoptionen** erfolgt die Auswahl einer Übertragungspriorität und der maximalen Transferrate.
4. Nach einem Klick auf **Source Snapshot Copies** ist in der Spalte **Snapshot Copy** auf **Default** zu klicken.

   Das Dialogfeld „Quell-Snapshot-Kopie auswählen“ wird angezeigt.
5. Zum Angeben einer vorhandenen Snapshot-Kopie anstelle der Standard-Snapshot-Kopie ist **Vorhandene Snapshot Copy** anzuklicken und eine Snapshot-Kopie aus der Liste auszuwählen.
6. Anschließend **Absenden** auswählen.

   Sie kehren zum Dialogfeld „Initialisieren/Aktualisieren“ zurück.
7. Wenn Sie mehr als eine Quelle zum Initialisieren oder Aktualisieren ausgewählt haben, ist für die nächste Quelle für lesen/schreiben, für die Sie eine vorhandene Snapshot Kopie angeben möchten, **Default** auszuwählen.

   Es kann keine andere Snapshot-Kopie für Datensicherungs-Volumes ausgewählt werden.
8. Mit **Submit** wird der Initialisierungs- oder Aktualisierungsjob gestartet.

Der Initialisierungs- oder Aktualisierungsauftrag startet, Sie kehren zur Seite mit den Volumen-/Zustandsdetails zurück, und oben auf der Seite erscheint ein Link zu Jobs.

9. **Optional:** Auf der Detailseite **Volume / Health** lässt sich über **View Jobs** der Status jedes Initialisierungs- oder Aktualisierungsauftrags verfolgen.

   Eine gefilterte Liste der Jobs wird angezeigt.

10. **Optional:** Die Details der einzelnen Aufträge lassen sich durch Klicken auf den jeweiligen Auftrag anzeigen.
11. **Optional:** Über den Zurück-Pfeil im Browser ist die Rückkehr zur Detailseite **Volume / Health** möglich.

    Der Initialisierungs- oder Aktualisierungsvorgang ist abgeschlossen, wenn alle Jobaufgaben erfolgreich abgeschlossen sind.

Neusynchronisierung von Schutzbeziehungen auf der Seite „Volume Beziehungen“ in Active IQ Unified Manager

Auf der Seite „Volume Relationships“ können Sie eine Beziehung neu synchronisieren, entweder um sich von einem Ereignis zu erholen, das Ihr Quellvolume deaktiviert hat, oder wenn Sie die aktuelle Quelle in ein anderes Volume ändern möchten.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.

Schritte

1. Auf der Seite **Volume Relationships** lassen sich ein oder mehrere Volumes mit angehaltenen Beziehungen auswählen; anschließend kann in der Symbolleiste auf **Resynchronize** geklickt werden.

   Das Dialogfeld „Resynchronisieren“ wird angezeigt.

2. Auf der Registerkarte **Resynchronisierungsoptionen** lassen sich eine Übertragungspriorität und die maximale Transferrate auswählen.
3. Nach einem Klick auf **Source Snapshot Copies** ist in der Spalte **Snapshot Copy** auf **Default** zu klicken.

   Das Dialogfeld „Quell-Snapshot-Kopie auswählen“ wird angezeigt.

4. Zum Angeben einer vorhandenen Snapshot-Kopie anstelle der Standard-Snapshot-Kopie ist **Vorhandene Snapshot Copy** anzuklicken und eine Snapshot-Kopie aus der Liste auszuwählen.
5. Anschließend **Absenden** auswählen.

   Sie kehren zum Dialogfeld „Resynchronisieren“ zurück.

6. Bei Auswahl von mehr als einer Quelle für die Resynchronisierung wird für die nächste Quelle, für die eine vorhandene Snapshot-Kopie angegeben werden soll, **Default** ausgewählt.
7. Mit **Submit** wird der Resynchronisierungsvorgang gestartet.

   Der Resynchronisierungsauftrag startet, danach gelangen Sie zurück zur Seite „Volume Relationships“, und oben auf der Seite erscheint ein Link zu Aufträgen.

8. **Optional:** Auf der Seite **Volume Relationships** lässt sich über **View Jobs** der Status jedes Resynchronisierungsauftrags verfolgen.

   Eine gefilterte Liste der Jobs wird angezeigt.

9. **Optional:** Über den Pfeil **Back** in Ihrem Browser ist die Rückkehr zur Seite **Volume Relationships** möglich.

   Der Resynchronisierungsvorgang ist abgeschlossen, wenn alle Jobaufgaben erfolgreich abgeschlossen sind.

Umgekehrte Schutzbeziehungen auf der Seite „Volume Beziehungen“ in Active IQ Unified Manager

Wenn ein Katastrophenfall das Quellvolume in Ihrer Schutzbeziehung außer Betrieb setzt, können Sie das Zielvolume für die Bereitstellung von Daten verwenden, indem Sie es während der Reparatur oder des Austauschs des Quellvolumes in ein Volume mit lesen/schreiben Zugriff konvertieren. Sobald das Quellvolume wieder für den Datenempfang verfügbar ist, kann mit dem Vorgang zur umgekehrten Resynchronisierung die Beziehung in umgekehrter Richtung eingerichtet werden, wobei die Daten auf dem Quellvolume mit den Daten auf dem Zielvolume mit lesen/schreiben Zugriff synchronisiert werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen Workflow Automation eingerichtet haben.
- Die Beziehung darf keine SnapVault Beziehung sein.
- Eine Schutzbeziehung muss bereits vorhanden sein.
- Die Schutzbeziehung muss getrennt werden.
- Sowohl Quelle als auch Ziel müssen online sein.
- Die Quelle darf nicht das Ziel eines anderen Datensicherungs-Volumes sein.
- Wenn Sie diese Aufgabe ausführen, werden auf der Quelle Daten gelöscht, die neuer sind als die Daten in der gemeinsamen Snapshot Kopie.
- Richtlinien und Zeitpläne, die für Beziehungen zur umgekehrten Resynchronisierung erstellt wurden, sind dieselben wie bei der ursprünglichen Schutzbeziehung.

  Falls keine Richtlinien und Zeitpläne existieren, werden sie erstellt.

Schritte

1. Auf der Seite **Volume-Beziehungen** können Sie ein oder mehrere Volumes mit Beziehungen auswählen, die umgekehrt werden sollen, und anschließend in der Symbolleiste auf **Resynchronisierung umkehren** klicken.

   Das Dialogfeld „Umgekehrte Resynchronisierung“ wird angezeigt.

2. Im Dialogfeld **Reverse Resync** ist zu überprüfen, ob die angezeigten Beziehungen diejenigen sind, für die die umgekehrte Resynchronisierung ausgeführt werden soll; anschließend ist auf **Submit** zu klicken.

   Der umgekehrte Resynchronisierungsvorgang startet, anschließend gelangen Sie zurück zur Seite

„Volume Relationships“, und oben auf der Seite wird ein Link zu Jobs angezeigt.

3. **Optional:** Auf der Seite **Volume Relationships** lässt sich über **View Jobs** der Status jedes Auftrags zur umgekehrten Resynchronisierung nachverfolgen.

   Eine gefilterte Liste der mit diesem Vorgang zusammenhängenden Jobs wird angezeigt.

4. **Optional:** Über den Pfeil **Back** in Ihrem Browser ist die Rückkehr zur Seite **Volume Relationships** möglich.

   Der umgekehrte Resynchronisierungsvorgang ist beendet, wenn alle Jobaufgaben erfolgreich abgeschlossen sind.

Die Wiederherstellung von Daten erfolgt mithilfe der Seiten „Volume“ und „Volume/Integritätsdetails“ in Active IQ Unified Manager

Überschriebene oder gelöschte Dateien, Verzeichnisse oder ein gesamtes Volume lassen sich mithilfe der Wiederherstellungsfunktion auf den Seiten „Volume“ und „Volume/Integritätsdetails“ aus einer Snapshot Kopie wiederherstellen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Folgende Punkte sind zu beachten:

- Sie können ein Verzeichnis oder ein Volume in keiner der folgenden Szenarien aus einem Snapshot wiederherstellen:
  - Die Option **Yes, preserve all snapshot copies** ist ausgewählt.
  - Sie verwenden ein LDAP-Konto zur Überwachung des Clusters.
  - Sie sind als Domänenbenutzer angemeldet.
  - Ihr Konto ist für die SAML-Authentifizierung konfiguriert.
  - Sie verwenden das NDMP-Protokoll.

    Weitere Einzelheiten finden Sie im Knowledge Base Artikel "So konfigurieren Sie die NDMP Authentifizierung im 'SVM-scope'-Modus".
- Sie können NTFS-Dateistreams nicht wiederherstellen.
- Die Wiederherstellungsoption ist nicht verfügbar, wenn:
  - Die Volume-ID ist unbekannt, zum Beispiel wenn Sie über eine Intercluster-Beziehung verfügen und der Ziel-Cluster noch nicht entdeckt wurde.
  - Das Volume ist für die synchrone SnapMirror Replikation konfiguriert.

Schritte

1. Der Pfad im linken Navigationsbereich lautet **Storage > Volumes**.
2. Nach Auswahl des Volumes erfolgt ein Klick auf die Schaltfläche **Wiederherstellen**. Alternativ führt ein Klick auf das Volume zu **Volume / Zustandsdetails > Aktionen > Wiederherstellen**. Das Dialogfeld „Wiederherstellen“ wird angezeigt. Informationen zu dieser Seite sind unter "Wiederherstellungsdialogfeld" verfügbar.

3. Das Volume und die Snapshot-Kopie, aus denen Daten wiederhergestellt werden sollen, können ausgewählt werden, wenn sie von der Standardeinstellung abweichen.
4. Die Auswahl umfasst die Elemente, die wiederhergestellt werden sollen, z. B. die Quell-LUN.

   Sie können das gesamte Volume wiederherstellen, oder Sie können die Ordner und Dateien angeben, die Sie wiederherstellen möchten.

5. Der Speicherort, an dem die ausgewählten Elemente wiederhergestellt werden sollen, ist auszuwählen: entweder **Ursprünglicher Speicherort** oder **Alternativer vorhandener Speicherort**.
6. Wenn Sie einen alternativen, bereits vorhandenen Standort auswählen, ist eine der folgenden Aktionen erforderlich:
   - Im Textfeld „Wiederherstellungspfad“ geben Sie den Pfad des Speicherorts ein, an dem Sie die Daten wiederherstellen möchten, und klicken dann auf **Verzeichnis auswählen**.
   - Über **Durchsuchen** lässt sich das Dialogfeld „Verzeichnisse durchsuchen“ öffnen; anschließend sind die folgenden Schritte auszuführen:
     i. Wählen Sie den Ziel-Cluster, die Storage VM (SVM) und das Volume aus, auf dem die Wiederherstellung erfolgen soll.
     ii. In der Tabelle Name erfolgt die Auswahl eines Verzeichnisnamens, der wiederhergestellt werden muss.
     iii. Es ist auf **Verzeichnis auswählen** zu klicken.
7. Klicken Sie auf **Wiederherstellen**.

   Der Wiederherstellungsprozess beginnt. Im Backend wird ein Auftrag erstellt, der den Wiederherstellungsprozess abschließt.

8. Wenn Sie den Auftragsfortschritt anzeigen möchten, wechseln Sie im linken Navigationsbereich zu **Schutz > Aufträge**, um den Status des Wiederherstellungsauftrags in der Auftragsliste anzuzeigen.

> Wenn ein Wiederherstellungsvorgang zwischen Cloud Volumes ONTAP HA Clustern mit einem NDMP-Fehler fehlschlägt, kann es erforderlich sein, im Ziel-Cluster eine explizite AWS Route hinzuzufügen, damit das Ziel mit der Cluster-Management-LIF des Quellsystems kommunizieren kann. Dieser Konfigurationsschritt wird über die NetApp Console ausgeführt.

Informationen zu Ressourcenpools in Active IQ Unified Manager

Ressourcenpools sind Gruppen von Aggregaten, die von einem Storage-Administrator mit Unified Manager erstellt werden, um Partnerapplikationen für das Backup-Management Provisionierung bereitzustellen.

Sie können Ihre Ressourcen anhand von Attributen wie Performance, Kosten, physischem Standort oder Verfügbarkeit bündeln. Durch die Gruppierung verwandter Ressourcen in einem Pool können Sie den Pool für Überwachung und Provisionierung als eine einzelne Einheit behandeln. Dies vereinfacht die Verwaltung dieser Ressourcen und ermöglicht eine flexiblere und effizientere Nutzung des Storage.

Während der Provisionierung des sekundären Storage ermittelt Unified Manager anhand der folgenden Kriterien das am besten geeignete Aggregat im Ressourcenpool für den Schutz:

- Das Aggregat ist ein Datenaggregat (kein Root-Aggregat) und es ist ONLINE.

- Das Aggregat befindet sich auf einem Ziel-Cluster-Knoten, dessen ONTAP Version der Hauptversion des Quell-Clusters entspricht oder höher ist.
- Das Aggregat verfügt über den größten verfügbaren Speicherplatz aller Aggregate im Ressourcenpool.
- Nach der Provisionierung des Ziel-Volumes liegt der Aggregatspeicherplatz innerhalb des für das Aggregat definierten Schwellenwerts für nahezu volle Auslastung und nahezu Überbelegung (globaler oder lokaler Schwellenwert, je nachdem, welcher anwendbar ist).
- Die Anzahl der FlexVol Volumes auf dem Zielknoten darf das Plattformlimit nicht überschreiten.

In Active IQ Unified Manager können Ressourcenpools erstellt werden.

Im Dialogfeld „Ressourcenpool erstellen“ können Sie Aggregate zu Provisionierungszwecken gruppieren.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

Ressourcenpools können Aggregate aus verschiedenen Clustern enthalten, aber dasselbe Aggregat kann nicht zu verschiedenen Ressourcenpools gehören.

1. Im linken Navigationsbereich erfolgt die Auswahl von **Protection** > **Resource Pools**.
2. Auf der Seite **Ressourcenpools** erfolgt ein Klick auf **Erstellen**.
3. Im Dialogfeld **Ressourcenpool erstellen** können Sie gemäß den Anweisungen einen Namen und eine Beschreibung angeben sowie Aggregate als Mitglieder zu dem Ressourcenpool hinzufügen, den Sie erstellen möchten.

Ressourcenpools in Active IQ Unified Manager bearbeiten

Sie können einen bestehenden Ressourcenpool bearbeiten, wenn Sie den Namen und die Beschreibung des Ressourcenpools ändern möchten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die Schaltfläche „Bearbeiten“ ist nur aktiviert, wenn ein Ressourcenpool ausgewählt ist. Sind mehrere Ressourcenpools ausgewählt, ist die Schaltfläche „Bearbeiten“ deaktiviert.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Protection** > **Resource Pools**.
2. Sie wählen einen Ressourcenpool aus der Liste aus.
3. Klicken Sie auf **Bearbeiten**.

   Das Fenster „Ressourcenpool bearbeiten“ wird angezeigt.

4. Name und Beschreibung des Ressourcenpools lassen sich bei Bedarf bearbeiten.
5. Auf **Speichern** klicken.

   In der Ressourcenpoolliste erscheinen der neue Name und die neue Beschreibung.

Anzeigen des Ressourcenpool-Inventars in Active IQ Unified Manager

Auf der Seite „Ressourcenpools“ können Sie den Bestand der Ressourcenpools anzeigen und die verbleibende Kapazität für jeden Ressourcenpool überwachen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritt

1. Im linken Navigationsbereich erfolgt die Auswahl von **Protection** > **Resource Pools**.

   Das Inventar des Ressourcenpools wird angezeigt.

Hinzufügen von Ressourcenpoolmitgliedern in Active IQ Unified Manager

Ein Ressourcenpool besteht aus einer Anzahl von Mitgliedsaggregaten. Vorhandenen Ressourcenpools können Aggregate hinzugefügt werden, um den für die Provisionierung sekundärer Volumes verfügbaren Speicherplatz zu vergrößern.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können einem Ressourcenpool maximal 200 Aggregate gleichzeitig hinzufügen. Die im Dialogfeld „Aggregate“ angezeigten Aggregate gehören keinem anderen Ressourcenpool an.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Protection** > **Resource Pools**.
2. In der Liste **Resource Pools** wird ein Ressourcenpool ausgewählt.

   Die Mitglieder des Ressourcenpools sind im Bereich unterhalb der Ressourcenpoolliste aufgeführt.

3. Im Mitgliederbereich des Ressourcenpools erfolgt ein Klick auf **Hinzufügen**.

   Das Dialogfeld „Aggregate“ wird angezeigt.

4. Ein oder mehrere Aggregate auswählen.
5. Klicken Sie auf **Add**.

   Nach dem Schließen des Dialogfelds werden die Aggregate in der Mitgliederliste für den ausgewählten Ressourcenpool angezeigt.

Aggregate aus Ressourcenpools in Active IQ Unified Manager entfernen

Sie können Aggregate aus einem bestehenden Ressourcenpool entfernen, beispielsweise wenn Sie ein Aggregat für einen anderen Zweck verwenden möchten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die Mitglieder eines Ressourcenpools werden nur angezeigt, wenn ein Ressourcenpool ausgewählt ist.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Protection** > **Resource Pools**.
2. Sie wählen den Ressourcenpool aus, aus dem Sie Mitgliedsaggregate entfernen möchten.

   Die Liste der Mitgliedsaggregate wird im Bereich „Mitglieder“ angezeigt.
3. Ein oder mehrere Aggregate auswählen.

   Die Schaltfläche **Entfernen** ist aktiviert.
4. **Entfernen** auswählen.

   Ein Warndialogfeld wird angezeigt.
5. Klicken Sie auf **Yes**, um fortzufahren.

   Die ausgewählten Aggregate werden aus dem Bereich „Mitglieder“ entfernt.

Löschen von Ressourcenpools in Active IQ Unified Manager

Sie können Ressourcenpools löschen, wenn sie nicht mehr benötigt werden. Beispielsweise können Sie die Mitgliedsaggregate eines Ressourcenpools auf mehrere andere Ressourcenpools verteilen, wodurch der ursprüngliche Ressourcenpool überflüssig wird.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die Schaltfläche **Löschen** ist nur aktiviert, wenn mindestens ein Ressourcenpool ausgewählt ist.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Protection** > **Resource Pools**.
2. Wählen Sie den Ressourcenpool aus, der gelöscht werden soll.
3. Klicken Sie auf **Delete**.

   Der Ressourcenpool wird aus der Liste der Ressourcenpools entfernt, und seine Aggregate werden aus der Mitgliederliste entfernt.

Storage VM Disaster Recovery Schutzbeziehungen überwachen

Informationen zu Disaster-Recovery-Beziehungen von Storage VMs in Active IQ Unified Manager

Active IQ Unified Manager unterstützt die Überwachung von Storage VM Disaster Recovery Beziehungen, die Disaster Recovery auf der Granularität einer Storage VM Ebene bereitstellen. Storage VM Disaster Recovery ermöglicht die Wiederherstellung der in den zugehörigen Volumes der Storage VM vorhandenen Daten sowie die Wiederherstellung der Storage VM Konfiguration.

Eine DR-Beziehung für eine Storage VM wird von der Quell-Storage VM zur Ziel-Storage VM erstellt, um eine asynchrone Notfallwiederherstellung bereitzustellen. Abhängig vom Cluster-Setup können Sie auswählen, ob

die gesamte oder nur ein Teil der Storage VM Konfiguration (mit Ausnahme der Netzwerk- und Protokollkonfiguration) zusammen mit den Datenvolumes repliziert werden soll.

Nachdem die Beziehung für die Notfallwiederherstellung der Storage VM konfiguriert wurde, wird die Ziel-Storage VM gestartet, wenn die Quell-Storage VM aufgrund eines Hardwarefehlers oder einer Umweltkatastrophe nicht mehr verfügbar ist, sodass mit möglichst geringer Unterbrechung auf die Daten zugegriffen werden kann. Sobald die Quell-Storage VM wieder verfügbar ist, wird sie mit der Ziel-Storage VM resynchronisiert; anschließend wird die Quelle neu gestartet, um die Daten bereitzustellen. Für die Konfiguration und das Managen der Beziehung für die Notfallwiederherstellung der Storage VM können SnapMirror Befehle verwendet werden.

Die Überwachung von Storage VMs erfolgt über die Seite „Beziehungen“ in Active IQ Unified Manager

Sie können Ihre Disaster-Recovery-Beziehungen für Storage VMs auf der Seite „Beziehungen“ im Abschnitt „SCHUTZ“ des INVENTARS überwachen. Standardmäßig werden auf der Seite „Beziehungen“ nur die Beziehungen der obersten Ebene aufgeführt, da der Filter für die zugehörigen Beziehungen angewendet wird.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie verwenden Filter, um die Disaster-Recovery-Beziehungen der Storage VM anzuzeigen.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **SCHUTZ** > **Beziehungen**.

   Die Seite zeigt alle Arten von Beziehungen an: Volume-, Konsistenzgruppen- und Storage VM Beziehungen.

2. Mit **Filter** sowie **Relationship Object Type** und **Storage VM** lassen sich nur Disaster-Recovery-Beziehungen von Storage VMs anzeigen.
3. **Filter anwenden** auswählen.

   Zum Anzeigen aller Schutzbeziehungen sollte der Filter für die Beziehungen zwischen den Bestandteilen gelöscht werden.

   Auf der Seite werden nur die Disaster-Recovery-Beziehungen der Storage-VMs angezeigt.

Anzeigen von Schutzbeziehungen auf der Seite „Speicher-VMs“ in Active IQ Unified Manager

Auf der Seite „Storage VMs“ kann der Status der Disaster-Recovery-Beziehungen vorhandener Storage VMs angezeigt werden.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können auch Details zu den Schutzbeziehungen einsehen, einschließlich Übertragungs- und Verzögerungsstatus sowie Quell- und Zieldetails. Sie können Berichte planen oder vorhandene Berichte im gewünschten Format herunterladen. Über die Schaltfläche **Ein-/Ausblenden** können Sie die benötigten Spalten zu den Berichten hinzufügen, da diese standardmäßig nicht angezeigt werden.

Schritte

1. Im linken Navigationsbereich auf **STORAGE** > **Storage VMs** klicken.
2. Die Auswahl erfolgt im Menü **ANSICHT** über **Beziehung** > **Alle Beziehungen**.

   Die Ansicht „Beziehungen: Alle Beziehungen“ zeigt alle konfigurierten Storage VMs an.

Speicher-VMs basierend auf dem Schutzstatus in Active IQ Unified Manager anzeigen

Auf der Seite „Storage VMs“ des Inventars können Sie alle Storage VMs in Active IQ Unified Manager anzeigen und die Storage VMs anhand ihres Schutzstatus filtern.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Der Ansicht „Storage VMs“ wurde eine neue Spalte „Schutzrolle“ hinzugefügt, die Informationen dazu enthält, ob die Storage VM geschützt oder ungeschützt ist.

Wenn in Active IQ Unified Manager kein Quell-Cluster hinzugefügt wurde, sind in den Rastern alle Informationen zu diesem Cluster nicht verfügbar.

Schritte

1. Im linken Navigationsbereich auf **STORAGE** > **Storage VMs** klicken.
2. Im Menü **VIEW** ist **Health** > **All Storage VMs** auszuwählen.

   Integrität: Alle Storage VMs wird angezeigt.

3. Mit **Filter** lässt sich eine der folgenden Storage VMs anzeigen.

Zum Anzeigen	Filterwert
Geschützte Storage VMs	Die **Schutzrolle** ist **geschützt**
Ungeschützte Storage VMs	Die **Schutzrolle** ist **ungeschützt**

Es ist nicht möglich, die geschützten und ungeschützten Storage VMs gleichzeitig anzuzeigen. Zum erneuten Anwenden einer neuen Filteroption muss der vorhandene Filter gelöscht werden.

4. **Filter anwenden** auswählen.

   Die Ansicht „Nicht gespeichert“ zeigt alle Storage VMs an, die basierend auf Ihren Filterauswahlen durch Storage VM Disaster Recovery entweder geschützt oder ungeschützt sind.

Verwalten von Speicher-VM-Zuordnungen in Active IQ Unified Manager

Storage virtual machine (storage VM)-Zuordnungen sind Zuordnungen von einer Storage VM als Quelle zu einer Storage VM als Ziel, die von Partneranwendungen für die Ressourcenauswahl und die Provisionierung sekundärer Volumes verwendet werden.

Zuordnungen werden zwischen einer Quell-Storage-VM und einer Ziel-Storage-VM erstellt, unabhängig davon, ob die Ziel-Storage-VM ein sekundäres oder ein tertiäres Ziel ist. Sie können eine sekundäre Ziel-Storage-VM nicht als Quelle verwenden, um eine Zuordnung mit einer tertiären Ziel-Storage-VM zu erstellen.

Als Anwendungsadministrator oder Storage-Administrator können Sie die Storage VM-Zuordnungen in Ihrer Umgebung auf der Seite **Schutz** > **Storage VM-Zuordnungen** anzeigen.

SVMs können auf drei Arten verknüpft werden:

- **Beliebige Storage VM zuordnen**: Sie können eine Zuordnung zwischen einer beliebigen primären Quell-Storage-VM und einer oder mehreren Ziel-SVMs erstellen. Das bedeutet, dass alle vorhandenen SVMs, die derzeit geschützt werden müssen, sowie alle SVMs, die künftig erstellt werden, den angegebenen Ziel-SVMs zugeordnet sind. Beispielsweise kann es sinnvoll sein, Anwendungen aus mehreren unterschiedlichen Quellen an verschiedenen Standorten auf einer oder mehreren Ziel-SVMs an einem Standort zu sichern.
- **Zuordnung einer bestimmten Storage VM**: Sie können eine Zuordnung zwischen einer bestimmten Quell Storage VM und einer oder mehreren bestimmten Ziel SVMs erstellen. Wenn Sie beispielsweise Storage Services für viele Kunden bereitstellen, deren Daten voneinander getrennt sein müssen, können Sie diese Option wählen, um eine bestimmte Quell Storage VM einer bestimmten Ziel Storage VM zuzuordnen, die nur diesem Kunden zugewiesen ist.
- **Verknüpfung mit einer externen Storage VM**: Sie können eine Verknüpfung zwischen einer Quell-Storage VM und einem externen flexiblen Volume einer Ziel-Storage VM erstellen.

Erstellen von Storage VM-Zuordnungen

Der Assistent zum Erstellen von Storage VM Zuordnungen ermöglicht es Partneranwendungen für den Datenschutz, eine Quell-Storage-VM einer Ziel-Storage-VM für die Verwendung mit SnapMirror und SnapVault Beziehungen zuzuordnen. Partneranwendungen verwenden diese Zuordnungen bei der erstmaligen Provisionierung von Ziel-Volumes, um zu bestimmen, welche Ressourcen auszuwählen sind.dd

Bevor Sie beginnen

- Die Storage VM, die Sie zuordnen möchten, muss bereits vorhanden sein.
- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Für jede Quell-Storage-VM und jeden Beziehungstyp ist auf jedem Ziel-Cluster nur eine Ziel-Storage-VM auswählbar.

Das Ändern von Zuordnungen mithilfe der Funktionen „Löschen“ und „Erstellen“ wirkt sich nur auf zukünftige Provisionierungsvorgänge aus. Vorhandene Ziel-Volumes werden nicht verschoben.

Schritte

1. Im linken Navigationsbereich wählen Sie **Protection** > **Storage VM Associations** aus.
2. Auf der Seite **Speicher-VM-Zuordnungen** ist **Erstellen** auszuwählen.

   Der Assistent **Create Storage Virtual Machine Associations** wird gestartet.

3. Eine der folgenden Quellen ist auszuwählen:
   - **Beliebig**

     Diese Option eignet sich, wenn Sie eine Zuordnung zwischen einer beliebigen primären Storage VM als Quelle und einer oder mehreren Ziel Storage VMs erstellen möchten. Dies bedeutet, dass alle vorhandenen Storage VMs, die derzeit Schutz erfordern, sowie alle Storage VMs, die künftig erstellt werden, der angegebenen Ziel Storage VM zugeordnet werden. Beispielsweise kann es sinnvoll sein, Anwendungen aus mehreren unterschiedlichen Quellen an verschiedenen Standorten in einer oder mehreren Ziel Storage VMs an einem Standort zu sichern.

- **Einzel**

  Diese Option wird verwendet, wenn eine bestimmte Quell-Storage-VM ausgewählt werden soll, die einer oder mehreren Ziel-Storage-VMs zugeordnet ist. Wenn beispielsweise Storage Services für viele Kunden bereitgestellt werden, deren Daten voneinander getrennt sein müssen, ist diese Option zu verwenden, um eine bestimmte Quell-Storage-VM einer bestimmten Ziel-Storage-VM zuzuordnen, die nur diesem Kunden zugewiesen ist.

- **Keine (Extern)**

  Diese Option kommt infrage, wenn Sie eine Zuordnung zwischen einer Quell-Storage-VM und einem externen flexiblen Volume einer Ziel-Storage-VM erstellen möchten.

4. Auszuwählen ist einer oder sind beide Schutzbeziehungstypen, die erstellt werden sollen:
   - **SnapMirror**
   - **SnapVault**
5. Klicken Sie auf **Weiter**.
6. Ein oder mehrere Storage VM-Datensicherungsziele auswählen.
7. Klicken Sie auf **Finish**.

Storage VM Zuordnungen löschen

Sie können Storage VM Zuordnungen für Partneranwendungen löschen, um die sekundäre Provisionierungsbeziehung zwischen der Quell Storage VM und der Ziel Storage VM zu entfernen; dies kann beispielsweise sinnvoll sein, wenn die Ziel Storage VM voll ist und Sie neue Storage VM Schutzzuordnungen erstellen möchten.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die Schaltfläche **Löschen** ist deaktiviert, bis mindestens eine Storage VM Zuordnung ausgewählt ist. Änderungen an Zuordnungen mithilfe der Funktionen „Löschen“ und „Erstellen“ wirken sich nur auf zukünftige Provisionierungsvorgänge aus; vorhandene Ziel-Volumes werden nicht verschoben.

Schritte

1. Im linken Navigationsbereich wählen Sie **Protection** > **Storage VM Associations** aus.
2. Mindestens eine Storage VM Zuordnung muss ausgewählt sein.

   Die Schaltfläche **Löschen** ist aktiviert.

3. **Löschen** auswählen.

   Ein Warndialogfeld wird angezeigt.

4. Klicken Sie auf **Yes**, um fortzufahren.

   Die ausgewählte Storage VM Zuordnung wird aus der Liste entfernt.

Anforderungen an SVMs und Ressourcenpools zur Unterstützung von Speicherdiensten in Active IQ Unified Manager

Sie können die Konformität in Partneranwendungen besser gewährleisten, wenn Sie einige für Storage Services spezifische Anforderungen an SVM-Zuordnungen und Ressourcenpools beachten: zum Beispiel, wenn Sie SVMs zuordnen und Ressourcenpools in Unified Manager erstellen, um eine Sicherungstopologie in einem von einer Partneranwendung bereitgestellten Storage Service zu unterstützen.

Einige Applikationen arbeiten mit dem Unified Manager Server zusammen, um Services bereitzustellen, die den SnapMirror oder SnapVault Backup-Schutz zwischen Quell-Volumes und Schutz-Volumes an sekundären oder tertiären Standorten automatisch konfigurieren und ausführen. Zur Unterstützung dieser Storage-Services zum Schutz müssen Sie Unified Manager verwenden, um die erforderlichen SVM-Zuordnungen und Ressourcenpools zu konfigurieren.

Zur Unterstützung des Single-Hop- oder Kaskadenschutzes von Storage Services, einschließlich der Replikation von einer SnapMirror Quelle oder einem primären SnapVault Volume zu entweder SnapMirror Zielen oder zu SnapVault Backup-Volumes, die sich an sekundären oder tertiären Standorten befinden, sind die folgenden Anforderungen zu beachten:

- SVM-Assoziationen müssen zwischen der SVM konfiguriert werden, die die SnapMirror Quelle oder das SnapVault Primär-Volume enthält, und jeder SVM, auf der sich entweder ein sekundäres Volume oder ein tertiäres Volume befindet.
  - Um beispielsweise eine Datensicherungstopologie zu unterstützen, bei der sich das Quellvolume Vol_A auf SVM_1 befindet, das sekundäre SnapMirror Zielvolume Vol_B auf SVM_2 und das tertiäre SnapVault Sicherungsvolume Vol_ C auf SVM_3, müssen Sie die Unified Manager Web-Benutzeroberfläche verwenden, um eine SnapMirror Beziehung zwischen SVM_1 und SVM_2 sowie eine SnapVault Sicherungsbeziehung zwischen SVM_1 und SVM_3 zu konfigurieren.

    In diesem Beispiel ist eine SnapMirror Zuordnung oder SnapVault Backup-Zuordnung zwischen SVM_2 und SVM_3 nicht erforderlich und wird nicht verwendet.

  - Um eine Schutztopologie zu unterstützen, bei der sich sowohl das Quellvolume Vol_A als auch das SnapMirror Zielvolume Vol_B auf SVM_1 befinden, müssen Sie eine SnapMirror Zuordnung zwischen SVM_1 und SVM_1 konfigurieren.
- Die Ressourcenpools müssen die den zugehörigen SVMs zur Verfügung stehenden Cluster-Aggregatressourcen enthalten.

  Die Konfiguration der Ressourcenpools erfolgt über die Unified Manager Web UI; anschließend erfolgt in der Partner-Applikation die Zuweisung der sekundären und tertiären Zielknoten des Storage Service.

Informationen zu Jobs in Active IQ Unified Manager

Ein Job ist eine Reihe von Aufgaben, die Sie mit Unified Manager überwachen können. Die Ansicht von Jobs und den dazugehörigen Aufgaben ermöglicht es Ihnen festzustellen, ob diese erfolgreich abgeschlossen wurden.

Jobs werden initiiert, wenn Sie SnapMirror- und SnapVault-Beziehungen erstellen, wenn Sie eine Beziehungsoperation durchführen (Aufheben, Bearbeiten, Anhalten, Entfernen, Fortsetzen, Resynchronisieren und umgekehrte Resynchronisierung), wenn Sie Aufgaben zur Datenwiederherstellung durchführen, wenn Sie sich bei einem Cluster anmelden usw.

Wenn Sie einen Job initiieren, können Sie auf der Seite „Jobs“ und auf der Seite „Job details“ den Job und den Fortschritt der zugehörigen Aufgaben des Jobs überwachen.

Überwachung von Aufträgen in Active IQ Unified Manager

Auf der Seite „Aufträge“ lassen sich der Auftragsstatus überwachen und Auftragseigenschaften wie Speicherdiensttyp, Status, Übermittlungszeitpunkt und Abschlusszeitpunkt anzeigen, um festzustellen, ob ein Auftrag erfolgreich abgeschlossen wurde.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich erfolgt der Aufruf von **Schutz** > **Aufträge**.

   Die Seite „Jobs“ wird angezeigt.

2. In der Spalte **Status** ist der Status der aktuell laufenden Aufträge ersichtlich.
3. Durch Klicken auf einen Jobnamen werden Details zu diesem Job angezeigt.

   Die Seite „Job details“ wird angezeigt.

Auftragsdetails in Active IQ Unified Manager

Nachdem Sie einen Auftrag gestartet haben, können Sie dessen Fortschritt auf der Seite mit den Auftragsdetails verfolgen und die zugehörigen Aufgaben auf mögliche Fehler überwachen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich erfolgt der Aufruf von **Schutz** > **Aufträge**.
2. Auf der Seite „Jobs“ öffnet ein Klick auf einen Jobnamen in der Spalte „Name“ die Liste der dem Job zugeordneten Aufgaben.
3. Bei Auswahl einer Aufgabe erscheinen rechts neben der Aufgabenliste zusätzliche Informationen im Bereich **Aufgabendetails** und im Bereich **Aufgabenmeldungen**.

Abbrechen von Jobs in Active IQ Unified Manager

Auf der Seite „Aufträge“ lässt sich ein Auftrag abbrechen, wenn sein Abschluss zu lange dauert, zu viele Fehler auftreten oder er nicht mehr benötigt wird. Ein Auftrag lässt sich nur abbrechen, wenn sein Status und Typ dies zulassen. Jeder laufende Auftrag lässt sich abbrechen.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich erfolgt der Aufruf von **Schutz** > **Aufträge**.
2. Aus der Liste der Aufträge kann ein Auftrag ausgewählt und anschließend auf **Abbrechen** geklickt werden.
3. Zum Abbrechen des ausgewählten Auftrags ist in der Bestätigungsabfrage **Ja** auszuwählen.

Wiederholen eines fehlgeschlagenen Schutzauftrags in Active IQ Unified Manager

Nachdem Sie Maßnahmen zur Behebung eines fehlgeschlagenen Schutzauftrags ergriffen haben, können Sie den Auftrag mit **Retry** erneut ausführen. Das Wiederholen eines Auftrags erstellt einen neuen Auftrag mit der ursprünglichen Auftrags-ID.

Bevor Sie beginnen

Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Sie können jeweils nur einen fehlgeschlagenen Auftrag wiederholen. Wenn Sie mehrere Aufträge auswählen, wird die Schaltfläche „Wiederholen“ deaktiviert. Nur Aufträge vom Typ „Schutzkonfiguration“ und „Schutzbeziehungsoperation“ können wiederholt werden.

Schritte

1. Im linken Navigationsbereich erfolgt der Aufruf von **Schutz** > **Aufträge**.
2. In der Liste der Aufträge ist ein einzelner fehlgeschlagener Auftrag vom Typ „Protection Configuration“ oder „Protection Relationship Operation“ auszuwählen.

   Die Schaltfläche **Wiederholen** ist aktiviert.

3. Auf **Retry** klicken.

   Der Auftrag startet neu.

Beschreibung der Fenster und Dialogfelder für Schutzbeziehungen

Informationen zur Seite „Ressourcenpools“ in Active IQ Unified Manager

Auf der Seite „Ressourcenpools“ werden bestehende Ressourcenpools und deren Mitglieder angezeigt, und sie ermöglicht das Erstellen, Überwachen und Managen von Ressourcenpools für die Provisionierung.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Erstellen**

  Startet das Dialogfeld „Ressourcenpool erstellen“, das zum Erstellen von Ressourcenpools verwendet werden kann.

- **Bearbeiten**

  Hier können Sie den Namen und die Beschreibung der von Ihnen erstellten Ressourcenpools bearbeiten.

- **Löschen**

Ermöglicht das Löschen eines oder mehrerer Ressourcenpools.

Liste der Ressourcenpools

Die Liste der Ressourcenpools zeigt (in Tabellenform) die Eigenschaften der vorhandenen Ressourcenpools an.

- **Ressourcenpool**

  Zeigt den Namen des Ressourcenpools an.

- **Beschreibung**

  Beschreibt den Ressourcenpool.

- **SnapLock Typ**

  Zeigt den SnapLock Typ an, der von den Aggregaten im Ressourcenpool verwendet wird. Gültige Werte für den SnapLock Typ sind Compliance, Enterprise und Non-SnapLock. Ein Ressourcenpool kann nur Aggregate eines SnapLock Typs enthalten.

- **Gesamtkapazität**

  Zeigt die Gesamtkapazität (in MB, GB usw.) des Ressourcenpools an.

- **Genutzte Kapazität**

  Zeigt die Menge an Speicherplatz an, die im Ressourcenpool verwendet wird (in MB, GB usw.).

- **Verfügbare Kapazität**

  Zeigt den im Ressourcenpool verfügbaren Speicherplatz (in MB, GB usw.) an.

- **Verwendet %**

  Zeigt den Prozentsatz des im Ressourcenpool belegten Speicherplatzes an.

Befehlsschaltflächen für die Mitgliederliste

Mit den Befehlsschaltflächen der Mitgliederliste können Sie die folgenden Aufgaben ausführen:

- **Hinzufügen**

  Ermöglicht das Hinzufügen von Mitgliedern zum Ressourcenpool.

- **Löschen**

  Hiermit können Sie ein oder mehrere Mitglieder aus dem Ressourcenpool löschen.

Mitgliederliste

Die Mitgliederliste zeigt (in Tabellenform) die Mitglieder des Ressourcenpools und deren Eigenschaften an, wenn ein Ressourcenpool ausgewählt ist.

- **Status**

Zeigt den aktuellen Status des Mitgliedsaggregats an. Der Status kann Kritisch (), Fehler (), Warnung () oder Normal () sein.

- **Aggregatname**

  Zeigt den Namen des Mitgliedsaggregats an.

- **Zustand**

  Zeigt den aktuellen Zustand des Aggregats an, der einen der folgenden Werte annehmen kann:

  - Offline

    Lese- und Schreibzugriff ist nicht gestattet.

  - Online

    Lese- und Schreibzugriff auf die Volumes, die auf diesem Aggregat gehostet werden, ist zulässig.

  - Eingeschränkt

    Begrenzte Operationen (wie z. B. Paritätsrekonstruktion) sind zulässig, der Datenzugriff jedoch nicht.

  - Erstellen

    Das Aggregat wird erstellt.

  - Zerstören

    Das Aggregat wird zerstört.

  - Fehlgeschlagen

    Das Aggregat kann nicht online geschaltet werden.

  - Gefroren

    Das Aggregat verarbeitet (vorübergehend) keine Anfragen.

  - Inkonsistent

    Das Aggregat wurde als beschädigt markiert; Sie sollten sich an den technischen Support wenden.

  - Eisen eingeschränkt

    Diagnosetools können nicht auf dem Aggregat ausgeführt werden.

  - Montage

    Das Aggregat wird derzeit eingehängt.

  - Teilweise

    Für das Aggregat wurde mindestens eine Festplatte gefunden, es fehlen jedoch zwei oder mehr Festplatten.

- Anhalten

  Das Aggregat wird in den Ruhezustand versetzt.

- Ruhend

  Das Aggregat ist angehalten.

- Zurückgesetzt

  Die Rücksetzung eines Aggregats ist abgeschlossen.

- Nicht eingehängt

  Das Aggregat wurde ausgehängt.

- Aushängen

  Das Aggregat wird offline genommen.

- Unbekannt

  Das Aggregat wurde gefunden, die Aggregatinformationen wurden jedoch noch nicht vom Unified Manager Server abgerufen.

Diese Spalte ist standardmäßig ausgeblendet.

- **Cluster**

  Zeigt den Namen des Clusters an, zu dem das Aggregat gehört.

- **Knoten**

  Zeigt den Namen des Knotens an, auf dem sich das Aggregat befindet.

- **Gesamtkapazität**

  Zeigt die Gesamtkapazität (in MB, GB usw.) des Aggregats an.

- **Genutzte Kapazität**

  Zeigt die im Aggregat belegte Speicherplatzmenge (in MB, GB usw.) an.

- **Verfügbare Kapazität**

  Zeigt die Menge des Speicherplatzes an, die im Aggregat verfügbar ist (in MB, GB usw.).

- **Verwendet %**

  Zeigt den Prozentsatz des im Aggregat verwendeten Speicherplatzes an.

- **Datenträgertyp**

  Zeigt den RAID-Konfigurationstyp an, der einer der folgenden sein kann:

  - RAID0: Alle RAID-Gruppen sind vom Typ RAID0.

- RAID4: Alle RAID-Gruppen sind vom Typ RAID4.
- RAID-DP: Alle RAID-Gruppen sind vom Typ RAID-DP.
- RAID-TEC: Alle RAID-Gruppen sind vom Typ RAID-TEC.
- Gemischtes RAID: Das Aggregat enthält RAID-Gruppen verschiedener RAID-Typen (RAID0, RAID4, RAID-DP und RAID-TEC). Diese Spalte ist standardmäßig ausgeblendet.

Das Dialogfeld „Ressourcenpool erstellen“ in Active IQ Unified Manager kann verwendet werden

Im Dialogfeld „Ressourcenpool erstellen“ können Sie einen neuen Ressourcenpool benennen und beschreiben sowie Aggregate zu diesem Ressourcenpool hinzufügen und Aggregate aus diesem Ressourcenpool löschen.

Name des Ressourcenpools

Mithilfe der Textfelder können Sie die folgenden Informationen hinzufügen, um einen Ressourcenpool zu erstellen:

Ermöglicht die Angabe des Namens eines Ressourcenpools.

Beschreibung

Ermöglicht die Beschreibung eines Ressourcenpools.

Mitglieder

Anzeige der Mitglieder des Ressourcenpools. Sie können auch Mitglieder hinzufügen und löschen.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Hinzufügen**

  Öffnet das Dialogfeld „Aggregate“, sodass Sie Aggregate aus einem bestimmten Cluster zum Ressourcenpool hinzufügen können. Sie können Aggregate aus verschiedenen Clustern hinzufügen, jedoch können dieselben Aggregate nicht zu mehr als einem Ressourcenpool hinzugefügt werden.

- **Entfernen**

  Ermöglicht das Entfernen ausgewählter Aggregate aus dem Ressourcenpool.

- **Erstellen**

  Erstellt den Ressourcenpool. Diese Schaltfläche ist erst aktiviert, wenn in die Felder „Name des Ressourcenpools“ oder „Beschreibung“ Informationen eingegeben wurden.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld „Ressourcenpool erstellen“.

Im Active IQ Unified Manager steht das Dialogfeld „Ressourcenpool bearbeiten“ zur Verfügung

Im Dialogfeld „Ressourcenpool bearbeiten“ können Sie den Namen und die

Beschreibung eines vorhandenen Ressourcenpools ändern. Wenn beispielsweise der ursprüngliche Name und die Beschreibung ungenau oder fehlerhaft sind, können Sie sie präzisieren.

Textfelder

Mithilfe der Textfelder können Sie die folgenden Informationen für den ausgewählten Ressourcenpool ändern:

- **Name des Ressourcenpools**

  Ermöglicht die Eingabe eines neuen Namens.

- **Beschreibung**

  Ermöglicht Ihnen die Eingabe einer neuen Beschreibung.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Speichern**

  Speichert die Änderungen am Namen und der Beschreibung des Ressourcenpools.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld „Ressourcenpool bearbeiten“.

Im Active IQ Unified Manager steht das Dialogfeld „Aggregate“ zur Verfügung

Im Dialogfeld „Aggregate“ können Sie die Aggregate auswählen, die Sie Ihrem Ressourcenpool hinzufügen möchten.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Hinzufügen**

  Fügt die ausgewählten Aggregate dem Ressourcenpool hinzu. Die Schaltfläche „Hinzufügen“ ist erst aktiviert, wenn mindestens ein Aggregat ausgewählt ist.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld „Aggregate“.

Aggregatliste

Die Liste der Aggregate zeigt (in Tabellenform) die Namen und Eigenschaften der überwachten Aggregate an.

- **Status**

  Zeigt den aktuellen Status eines Volumes an. Der Status kann Kritisch (), Fehler (), Warnung () oder Normal () sein.

Wenn Sie den Mauszeiger über den Status bewegen, erhalten Sie weitere Informationen zu dem Ereignis bzw. den Ereignissen, die für das Volume generiert wurden.

- **Aggregatname**

  Zeigt den Namen des Aggregats an.

- **Zustand**

  Zeigt den aktuellen Zustand des Aggregats an, der einen der folgenden Werte annehmen kann:

  - Offline

    Lese- und Schreibzugriff ist nicht gestattet.

  - Eingeschränkt

    Begrenzte Operationen (wie z. B. Paritätsrekonstruktion) sind zulässig, der Datenzugriff jedoch nicht.

  - Online

    Lese- und Schreibzugriff auf die Volumes, die auf diesem Aggregat gehostet werden, ist zulässig.

  - Erstellen

    Das Aggregat wird erstellt.

  - Zerstören

    Das Aggregat wird zerstört.

  - Fehlgeschlagen

    Das Aggregat kann nicht online geschaltet werden.

  - Gefroren

    Das Aggregat verarbeitet (vorübergehend) keine Anfragen.

  - Inkonsistent

    Das Aggregat wurde als beschädigt markiert; Sie sollten sich an den technischen Support wenden.

  - Eisen eingeschränkt

    Diagnosetools können nicht auf dem Aggregat ausgeführt werden.

  - Montage

    Das Aggregat wird derzeit eingehängt.

  - Teilweise

    Für das Aggregat wurde mindestens eine Festplatte gefunden, es fehlen jedoch zwei oder mehr Festplatten.

- Anhalten

  Das Aggregat wird in den Ruhezustand versetzt.

- Ruhend

  Das Aggregat ist angehalten.

- Zurückgesetzt

  Die Rücksetzung eines Aggregats ist abgeschlossen.

- Nicht eingehängt

  Das Aggregat ist offline.

- Aushängen

  Das Aggregat wird offline genommen.

- Unbekannt

  Das Aggregat wurde gefunden, die Aggregatinformationen wurden jedoch noch nicht vom Unified Manager Server abgerufen.

- **Cluster**

  Zeigt den Namen des Clusters an, auf dem sich das Aggregat befindet.

- **Knoten**

  Zeigt den Namen des Storage Controllers an, der das Aggregat enthält.

- **Gesamtkapazität**

  Zeigt die Gesamtdatengröße des Aggregats (in MB, GB usw.) an. Diese Spalte ist standardmäßig ausgeblendet.

- **Zugesicherte Kapazität**

  Zeigt den gesamten zugesicherten Speicherplatz (in MB, GB usw.) an, der für alle Volumes im Aggregat reserviert ist. Diese Spalte ist standardmäßig ausgeblendet.

- **Genutzte Kapazität**

  Zeigt die im Aggregat belegte Speicherplatzmenge (in MB, GB usw.) an.

- **Verfügbare Kapazität**

  Zeigt die Menge an Speicherplatz (in MB, GB usw.) an, die im Aggregat für Daten verfügbar ist. Diese Spalte ist standardmäßig ausgeblendet.

- **Verfügbar %**

  Zeigt den prozentualen Speicherplatz an, der für Daten im Aggregat verfügbar ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendet %**

  Zeigt den Prozentsatz des Speicherplatzes an, der von Daten im Aggregat verwendet wird.

- **RAID-Typ**

  Zeigt den RAID-Typ des ausgewählten Volumes an. Der RAID-Typ kann RAID0, RAID4, RAID-DP, RAID-TEC oder Mixed RAID sein.

Informationen zur Jobseite in Active IQ Unified Manager

Auf der Seite „Aufträge“ sind der aktuelle Status und weitere Informationen zu allen derzeit laufenden sowie abgeschlossenen Aufträgen zum Schutz von Partner-Applikationen verfügbar. Mithilfe dieser Informationen lässt sich feststellen, welche Aufträge noch ausgeführt werden und ob ein Auftrag erfolgreich war oder fehlgeschlagen ist.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Abbrechen**

  Bricht den ausgewählten Auftrag ab. Diese Option ist nur verfügbar, wenn der ausgewählte Auftrag ausgeführt wird.

- **Wiederholen**

  Ein fehlgeschlagener Auftrag vom Typ „Protection Configuration“ oder „Protection Relationship Operation“ wird neu gestartet. Es kann jeweils nur ein fehlgeschlagener Auftrag erneut ausgeführt werden. Wenn mehr als ein fehlgeschlagener Auftrag ausgewählt ist, ist die Schaltfläche **Retry** deaktiviert. Fehlgeschlagene Storage-Serviceaufträge können nicht erneut ausgeführt werden.

- **Aktualisieren**

  Aktualisiert die Liste der Aufträge und die zugehörigen Informationen.

Stellenliste

Die Jobliste zeigt in tabellarischer Form eine Liste der Jobs an, die gerade ausgeführt werden. Standardmäßig werden in der Liste nur die Jobs angezeigt, die innerhalb der letzten Woche erstellt wurden. Mithilfe von Spaltensortierung und Filterung kann angepasst werden, welche Jobs angezeigt werden.

- **Status**

  Zeigt den aktuellen Status eines Auftrags an. Der Status kann Fehler (❗) oder Normal (✅) sein.

- **Job-ID**

  Zeigt die Kennnummer des Auftrags an. Diese Spalte ist standardmäßig ausgeblendet.

  Die Job-Identifikationsnummer ist eindeutig und wird vom Server beim Start des Jobs vergeben. Sie können nach einem bestimmten Job suchen, indem Sie die Job-Identifikationsnummer in das vom Spaltenfilter bereitgestellte Textfeld eingeben.

- **Name**

  Zeigt den Namen des Jobs an.

- **Typ**

  Zeigt den Jobtyp an. Die Jobtypen sind wie folgt:

  - **Clustererfassung**

    Ein Workflow Automation Auftrag führt eine erneute Erkennung eines Clusters durch.

  - **Schutzkonfiguration**

    Ein Schutzauftrag initiiert Workflow Automation Workflows, wie z. B. Cron-Zeitpläne, SnapMirror Richtlinienerstellung usw.

  - **Vorgang der Schutzbeziehung**

    Ein Schutzjob führt SnapMirror Vorgänge aus.

  - **Schutz-Workflow-Kette**

    Ein Workflow Automation Job führt mehrere Workflows aus.

  - **Wiederherstellen**

    Ein Wiederherstellungsauftrag läuft.

  - **Aufräumarbeiten**

    Die Aufgabe besteht darin, Artefakte von Storage-Service-Mitgliedern zu bereinigen, die für Wiederherstellungszwecke nicht mehr benötigt werden.

  - **Konform**

    Die Aufgabe besteht darin, die Konfiguration der Storage Service-Mitglieder zu überprüfen, um sicherzustellen, dass sie den Vorgaben entsprechen.

  - **Zerstören**

    Der Job zerstört einen Storage-Service.

  - **Importieren**

    Die Aufgabe besteht darin, nicht verwaltete Storage-Objekte in einen bestehenden Storage-Service zu importieren.

  - **Ändern**

    Die Aufgabe besteht darin, Attribute eines bestehenden Storage-Service zu ändern.

  - **Abonnement**

    Die Aufgabe besteht darin, Mitglieder für einen Storage-Service anzumelden.

- **Abbestellen**

  Die Aufgabe besteht darin, Mitglieder von einem Storage-Service abzumelden.

- **Aktualisieren**

  Ein Schutzaktualisierungsauftrag läuft.

- **WFA Konfiguration**

  Ein Auftrag von Workflow Automation überträgt Cluster-Anmeldeinformationen und synchronisiert Datenbank-Caches.

- **Zustand**

  Zeigt den Ausführungsstatus des Jobs an. Folgende Statusoptionen stehen zur Verfügung:

  - **Abgebrochen**

    Der Auftrag wurde abgebrochen.

  - **Abbruch**

    Der Auftrag wird gerade abgebrochen.

  - **Abgeschlossen**

    Der Job ist abgeschlossen.

  - **Läuft**

    Der Auftrag läuft.

- **Einreichungszeitpunkt**

  Zeigt den Zeitpunkt an, zu dem der Job übermittelt wurde.

- **Dauer**

  Zeigt die für die Ausführung des Auftrags benötigte Zeit an. Diese Spalte wird standardmäßig angezeigt.

- **Abschlusszeit**

  Zeigt den Zeitpunkt des Auftragsabschlusses an. Diese Spalte ist standardmäßig ausgeblendet.

Informationen zur Seite mit den Auftragsdetails in Active IQ Unified Manager

Auf der Seite „Auftragsdetails“ lassen sich Status und weitere Informationen zu bestimmten Aufgaben von Datensicherungsaufträgen anzeigen, die ausgeführt werden, in der Warteschlange stehen oder abgeschlossen sind. Anhand dieser Informationen lassen sich der Fortschritt von Datensicherungsaufträgen überwachen und Fehler bei Aufträgen beheben.

Stellenbeschreibung

Die Auftragsübersicht enthält folgende Informationen:

- Job-ID
- Typ
- Status
- Übermittlungszeitpunkt
- Abschlusszeit
- Dauer

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Aktualisieren**

  Aktualisiert die Aufgabenliste und die Eigenschaften, die mit jeder Aufgabe verknüpft sind.

- **Jobs anzeigen**

  Sie gelangen zurück zur Seite „Jobs“.

Aufgabenliste

Die Liste der Job-Aufgaben zeigt in einer Tabelle alle Aufgaben an, die einem bestimmten Job zugeordnet sind, sowie die Eigenschaften der einzelnen Aufgaben.

- **Startzeit**

  Zeigt Datum und Uhrzeit des Aufgabenstarts an. Standardmäßig werden die neuesten Aufgaben oben in der Spalte und ältere Aufgaben unten angezeigt.

- **Typ**

  Zeigt die Art der Aufgabe an.

- **Zustand**

  Der Status einer bestimmten Aufgabe:

  - **Abgeschlossen**

    Die Aufgabe ist abgeschlossen.

  - **In der Warteschlange**

    Der Task wird in Kürze ausgeführt.

  - **Läuft**

    Die Aufgabe wird ausgeführt.

  - **Warten**

Ein Auftrag wurde übermittelt, und einige zugehörige Aufgaben warten noch auf ihre Einreihung in die Warteschlange und Ausführung.

- **Status**

  Zeigt den Aufgabenstatus an:

  - **Fehler (❗)**

    Die Aufgabe ist fehlgeschlagen.

  - **Normal (✅)**

    Die Aufgabe wurde erfolgreich abgeschlossen.

  - **Übersprungen (↪)**

    Eine Aufgabe ist fehlgeschlagen, wodurch nachfolgende Aufgaben übersprungen wurden.

- **Dauer**

  Zeigt die seit Beginn der Aufgabe verstrichene Zeit an.

- **Abschlusszeit**

  Zeigt den Zeitpunkt des Abschlusses der Aufgabe an. Diese Spalte ist standardmäßig ausgeblendet.

- **Aufgaben-ID**

  Zeigt die GUID an, die eine einzelne Aufgabe eines Auftrags identifiziert. Die Spalte kann sortiert und gefiltert werden. Standardmäßig ist diese Spalte ausgeblendet.

- **Abhängigkeitsreihenfolge**

  Zeigt eine ganze Zahl an, die die Reihenfolge der Aufgaben in einem Diagramm darstellt, wobei der ersten Aufgabe der Wert Null zugewiesen wird. Standardmäßig ist diese Spalte ausgeblendet.

- **Bereich Aufgabendetails**

  Zeigt zusätzliche Informationen zu jeder Aufgabe eines Jobs an, einschließlich des Aufgabennamens, der Aufgabenbeschreibung und, falls die Aufgabe fehlgeschlagen ist, des Grundes für den Fehler.

- **Aufgabennachrichtenbereich**

  Zeigt Meldungen speziell für die ausgewählte Aufgabe an. Diese Meldungen können den Grund für den Fehler und Lösungsvorschläge enthalten. Nicht für alle Aufgaben werden Meldungen angezeigt.

Im Active IQ Unified Manager steht das Dialogfeld „Erweiterte Sekundäreinstellungen“ zur Verfügung

Im Dialogfeld „Erweiterte sekundäre Einstellungen“ können Sie versionsflexible Replikation, Mehrfachkopie-Backups und speicherbezogene Einstellungen auf einem sekundären Volume aktivieren. Das Dialogfeld „Erweiterte sekundäre Einstellungen“ kann beispielsweise verwendet werden, wenn die aktuellen Einstellungen aktiviert, deaktiviert oder geändert werden sollen.

Speicherbezogene Einstellungen maximieren die Menge der gespeicherten Daten, darunter Deduplizierung, Datenkomprimierung, automatisches Wachstum und Speicherplatzzusage.

Das Dialogfeld enthält folgende Felder:

- **Aktivierung der versionsflexiblen Replikation**

  Ermöglicht die versionsflexible Replikation mit SnapMirror. Die versionsflexible Replikation ermöglicht den SnapMirror Schutz eines Quell-Volumes, selbst wenn auf dem Ziel-Volume eine ältere ONTAP Version als auf dem Quell-Volume ausgeführt wird.

  - Backup aktivieren

    Wenn die versionsflexible Replikation aktiviert ist, werden auch mehrere Snapshot Kopien der SnapMirror Quelldaten an das SnapMirror Ziel übertragen und dort aufbewahrt.

- **Deduplizierung aktivieren**

  Aktiviert die Deduplizierung auf dem sekundären Volume in einer SnapVault Beziehung, sodass doppelte Datenblöcke eliminiert werden und Speicherplatz eingespart wird. Die Deduplizierung kann sinnvoll sein, wenn die Speicherplatzeinsparung mindestens 10 Prozent beträgt und die Daten nicht schnell überschrieben werden. Die Deduplizierung wird häufig für virtualisierte Umgebungen, Dateifreigaben und Sicherungsdaten verwendet. Diese Einstellung ist standardmäßig deaktiviert. Wenn diese Einstellung aktiviert ist, wird dieser Vorgang nach jeder Übertragung initiiert.

  - Komprimierung aktivieren

    Aktiviert die transparente Datenkomprimierung. Die Komprimierung kann verwendet werden, wenn die Speicherplatzersparnis mindestens 10 Prozent beträgt, der potenzielle Mehraufwand akzeptabel ist und ausreichend Systemressourcen zur Verfügung stehen, damit die Komprimierung außerhalb der Spitzenzeiten abgeschlossen werden kann. In einer SnapVault Beziehung ist diese Einstellung standardmäßig deaktiviert. Die Komprimierung ist nur verfügbar, wenn die Deduplizierung ausgewählt ist.

  - Inline komprimieren

    Ermöglicht sofortige Speicherplatzeinsparungen durch Datenkomprimierung vor dem Schreiben der Daten auf die Festplatte. Inline-Komprimierung kann verwendet werden, wenn Ihr System während der Spitzenzeiten nicht mehr als 50 % ausgelastet ist und wenn das System neue Schreibvorgänge sowie zusätzliche CPU-Leistung während der Spitzenzeiten verarbeiten kann. Diese Einstellung ist nur verfügbar, wenn “Enable Compression” ausgewählt ist.

- **Autogrow aktivieren**

  Ermöglicht die automatische Vergrößerung des Ziel-Volume, wenn der Prozentsatz des freien Speicherplatzes unter den angegebenen Schwellenwert fällt, sofern auf dem zugehörigen Aggregat Speicherplatz verfügbar ist.

- **Maximale Größe**

  Legt den maximalen Prozentsatz fest, um den ein Volume wachsen kann. Der Standardwert liegt 20 Prozent über der Größe des Quellvolumes. Ein Volume wächst nicht automatisch, wenn seine aktuelle Größe den maximalen Prozentsatz für automatisches Wachstum erreicht oder überschreitet. Dieses Feld ist nur aktiviert, wenn die Einstellung für automatisches Wachstum aktiviert ist.

- **Inkrementgröße**

  Gibt die prozentuale Schrittweite an, um die das Volume automatisch anwächst, bevor der maximale Prozentsatz des Quell-Volumes erreicht wird.

- **Speicherplatzzusage**

  Stellt sicher, dass auf dem sekundären Volume genügend Speicherplatz zugewiesen wird, damit Datenübertragungen stets erfolgreich sind. Die Einstellung für die Speicherplatzzusage kann eine der folgenden sein:

  ◦ Datei
  ◦ Volumen
  ◦ Keine + Beispielsweise haben Sie möglicherweise ein 200-GB-Volume, das Dateien mit insgesamt 50 GB enthält; diese Dateien umfassen jedoch nur 10 GB an Daten. Die Volume-Garantie reserviert 200 GB für das Zielvolume, unabhängig vom Inhalt auf der Quelle. Die Dateigarantie reserviert 50 GB, um sicherzustellen, dass ausreichend Speicherplatz für Dateien auf der Quelle vorhanden ist; wenn in diesem Szenario „Keine“ ausgewählt ist, reserviert das Zielvolume nur 10 GB für den tatsächlich von Dateidaten auf der Quelle genutzten Speicherplatz.

  Die Speicherplatzzusage ist standardmäßig auf Volume eingestellt.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Anwenden**

  Speichert die ausgewählten Effizienzeinstellungen und wendet sie an, wenn Sie im Dialogfeld „Schutz konfigurieren“ auf **Anwenden** klicken.

- **Stornieren**

  Verwirft Ihre Auswahl und schließt das Dialogfeld „Advanced Destination Settings“.

Im Active IQ Unified Manager kann das Dialogfeld „Erweiterte Zieleinstellungen“ verwendet werden.

Im Dialogfeld „Erweiterte Zieleinstellungen“ können Sie die Speicherplatzzusage für ein Zielvolume aktivieren. Dies ist beispielsweise sinnvoll, wenn die Speicherplatzzusage auf dem Quellvolume deaktiviert ist, Sie sie aber auf dem Zielvolume aktivieren möchten. Die Einstellungen für Deduplizierung, Komprimierung und automatisches Wachstum in einer SnapMirror Beziehung werden vom Quellvolume übernommen und können nicht geändert werden.

Platzgarantie

Stellt sicher, dass auf dem Ziel-Volume ausreichend Speicherplatz reserviert wird, damit Datenübertragungen stets erfolgreich sind. Die Einstellung für die Speicherplatzzusage kann eine der folgenden sein:

- Datei
- Volumen
- Keine

Beispielsweise könnte ein 200-GB-Volume Dateien mit einer Gesamtgröße von 50 GB enthalten; diese Dateien enthalten jedoch nur 10 GB an Daten. Die Volume-Garantie reserviert 200 GB für das Zielvolume, unabhängig vom Inhalt auf dem Quellvolume. Die Dateigarantie reserviert 50 GB, um sicherzustellen, dass auf dem Zielvolume genügend Speicherplatz für die Quelldateien vorhanden ist; die Auswahl von **None** bedeutet in diesem Fall, dass auf dem Zielvolume nur 10 GB für den tatsächlich von den Dateidaten auf dem Quellvolume belegten Speicherplatz reserviert werden.

Die Speicherplatzzusage ist standardmäßig auf Volume eingestellt.

Das Dialogfeld „Wiederherstellen“ in Active IQ Unified Manager wird verwendet

Im Dialogfeld „Restore“ können Sie Daten aus einer bestimmten Snapshot Kopie auf ein Volume wiederherstellen.

Wiederherstellen von

Im Bereich „Wiederherstellen von“ können Sie festlegen, woher die Daten wiederhergestellt werden sollen.

- **Volumen**

  Gibt das Volume an, von dem Sie Daten wiederherstellen möchten. Standardmäßig ist das Volume ausgewählt, auf dem Sie die Wiederherstellungsaktion initiiert haben. Sie können ein anderes Volume aus der Dropdown-Liste auswählen, die alle Volumes mit Schutzbeziehungen zu dem Volume enthält, auf dem Sie die Wiederherstellungsaktion initiiert haben.

- **Snapshot Kopie**

  Legt fest, welche Snapshot-Kopie Sie zur Wiederherstellung von Daten verwenden möchten. Standardmäßig ist die neueste Snapshot-Kopie ausgewählt. Sie können auch eine andere Snapshot-Kopie aus der Dropdown-Liste auswählen. Die Liste der Snapshot-Kopien ändert sich je nach ausgewähltem Volume.

- **Maximal 995 Dateien und Verzeichnisse auflisten**

  Standardmäßig werden maximal 995 Objekte in der Liste angezeigt. Sie können dieses Kontrollkästchen deaktivieren, wenn Sie alle Objekte im ausgewählten Volume anzeigen möchten. Dieser Vorgang kann einige Zeit dauern, wenn die Anzahl der Elemente sehr groß ist.

Auswahl der wiederherzustellenden Elemente

Im Bereich „Zu wiederherstellende Elemente auswählen“ können Sie entweder das gesamte Volume oder bestimmte Dateien und Ordner auswählen, die Sie wiederherstellen möchten. Sie können maximal 10 Dateien, Ordner oder eine Kombination aus beidem auswählen. Sobald die maximale Anzahl an Elementen ausgewählt ist, sind die Kontrollkästchen für die Elementauswahl deaktiviert.

- **Pfadfeld**

  Hier wird der Pfad zu den wiederherzustellenden Daten angezeigt. Sie können entweder zu dem gewünschten Ordner und den Dateien navigieren oder den Pfad eingeben. Dieses Feld ist leer, bis Sie einen Pfad auswählen oder eingeben. Nach der Pfadauswahl gelangen Sie durch Klicken auf  in der Verzeichnisstruktur eine Ebene nach oben.

- **Ordner- und Dateiliste**

Zeigt den Inhalt des eingegebenen Pfades an. Standardmäßig wird zunächst der Stammordner angezeigt. Durch Klicken auf einen Ordnernamen wird der Inhalt des Ordners angezeigt.

Sie können die wiederherzustellenden Elemente wie folgt auswählen:

- Wenn Sie den Pfad mit einem bestimmten Dateinamen im Feld „Pfad“ eingeben, erscheint die angegebene Datei in „Ordner und Dateien“.
- Wenn Sie einen Pfad eingeben, ohne eine bestimmte Datei anzugeben, erscheint der Inhalt des Ordners in der Liste „Ordner und Dateien“, und Sie können bis zu 10 Dateien, Ordner oder eine Kombination aus beidem zur Wiederherstellung auswählen.

  Wenn ein Ordner mehr als 995 Elemente enthält, wird eine Meldung angezeigt, die darauf hinweist, dass zu viele Elemente für die Anzeige vorhanden sind, und wenn Sie den Vorgang fortsetzen, werden alle Elemente im angegebenen Ordner wiederhergestellt. Sie können das Kontrollkästchen “Maximal 995 Dateien und Verzeichnisse auflisten” deaktivieren, wenn Sie alle Objekte innerhalb des ausgewählten Volume anzeigen möchten.

NTFS-Dateistreams lassen sich nicht wiederherstellen.

Wiederherstellen in

Im Bereich „Wiederherstellen unter“ können Sie festlegen, wo die Daten wiederhergestellt werden sollen.

- **Ursprünglicher Speicherort in Volume_Name**

  Stellt die ausgewählten Daten in dem Verzeichnis auf der Quelle wieder her, aus dem die Daten ursprünglich gesichert wurden.

- **Alternativer Standort**

  Stellt die ausgewählten Daten an einem neuen Speicherort wieder her:

  - Wiederherstellungspfad

    Gibt einen alternativen Pfad zum Wiederherstellen der ausgewählten Daten an. Der Pfad muss bereits existieren. Über die Schaltfläche **Durchsuchen** kann zu dem Speicherort navigiert werden, an dem die Daten wiederhergestellt werden sollen, oder der Pfad kann manuell im Format `cluster://svm/volume/path` eingegeben werden.

  - Verzeichnishierarchie beibehalten

    Wenn diese Option aktiviert ist, wird die Struktur der ursprünglichen Datei oder des ursprünglichen Verzeichnisses beibehalten. Wenn beispielsweise die Quelle /A/B/C/myFile.txt und das Ziel /X/Y/Z ist, stellt Unified Manager die Daten mithilfe der folgenden Verzeichnisstruktur auf dem Ziel wieder her: /X/Y/Z/A/B/C/myFile.txt.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Stornieren**

  Verwirft Ihre Auswahl und schließt das Dialogfeld „Wiederherstellen“.

- **Wiederherstellen**

  Übernimmt Ihre Auswahl und startet den Wiederherstellungsprozess.

Im Active IQ Unified Manager steht das Dialogfeld „Verzeichnisse durchsuchen“ zur Verfügung

Sie können das Dialogfeld „Verzeichnisse durchsuchen“ verwenden, wenn Sie Daten in einem Verzeichnis auf einem Cluster und einer SVM wiederherstellen möchten, die sich von der ursprünglichen Quelle unterscheiden. Der ursprüngliche Quell-Cluster und das Quell-Volume sind standardmäßig ausgewählt.

Im Dialogfeld „Verzeichnisse durchsuchen“ können Sie den Cluster, die SVM, das Volume und den Verzeichnispfad auswählen, in dem Sie die Daten wiederherstellen möchten.

- **Cluster**

  Listet die verfügbaren Clusterziele auf, in die Sie Daten wiederherstellen können. Standardmäßig ist der Cluster des ursprünglichen Quell-Volumes ausgewählt.

- **SVM-Auswahlliste**

  Listet die für den ausgewählten Cluster verfügbaren SVMs auf. Standardmäßig ist die SVM des ursprünglichen Quellvolumes ausgewählt.

- **Volumen**

  Listet alle lesen/schreiben Volumes in einer ausgewählten SVM auf. Sie können die Volumes nach Name und verfügbarem Speicherplatz filtern. Das Volume mit dem meisten verfügbaren Speicherplatz steht zuerst, gefolgt von den übrigen in absteigender Reihenfolge. Standardmäßig ist das ursprüngliche Quellvolume ausgewählt.

- **Textfeld für den Dateipfad**

  Ermöglicht die Eingabe des Dateipfads, in den die Daten wiederhergestellt werden sollen. Der eingegebene Pfad muss bereits existieren.

- **Name**

  Zeigt die Namen der verfügbaren Ordner für das ausgewählte Volume an. Durch Klicken auf einen Ordner in der Namensliste werden die Unterordner angezeigt, sofern welche vorhanden sind. In den Ordnern enthaltene Dateien werden nicht angezeigt. Durch Klicken auf  nach der Auswahl eines Ordners gelangen Sie in der Verzeichnisstruktur eine Ebene nach oben.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Verzeichnis auswählen**

  Wendet Ihre Auswahl an und schließt das Dialogfeld „Verzeichnisse durchsuchen“. Wenn kein Verzeichnis ausgewählt ist, ist diese Schaltfläche deaktiviert.

- **Stornieren**

Verwirft Ihre Auswahl und schließt das Dialogfeld „Verzeichnisse durchsuchen“.

Im Active IQ Unified Manager steht das Dialogfeld „Schutz konfigurieren“ zur Verfügung

Im Dialogfeld „Schutz konfigurieren“ können Sie SnapMirror- und SnapVault-Beziehungen für alle Volumes mit Lese-/Schreibzugriff sowie Datenschutz-Volumes auf Clustern erstellen, um sicherzustellen, dass die Daten auf einem Quellvolume oder primären Volume repliziert werden.

Registerkarte „Quelle“

- **Topologieansicht**

  Zeigt eine visuelle Darstellung der Beziehung, die Sie erstellen. Die Quelle in der Topologie ist standardmäßig hervorgehoben.

- **Quellinformationen**

  Zeigt Details zu den ausgewählten Quellvolumes an, einschließlich der folgenden Informationen:

  - Name des Quell-Clusters
  - Name der Quell-SVM
  - Kumulative Gesamtgröße des Volumens

    Zeigt die Gesamtgröße aller ausgewählten Quell-Volumes an.

  - Kumulierte verwendete Volume-Größe

    Zeigt die kumulative verwendete Größe aller ausgewählten Quell-Volumes an.

  - Quellvolumen

    Die folgende Tabelle enthält diese Informationen:

    - Quellvolumen

      Zeigt die Namen der ausgewählten Quell-Volumes an.

    - Typ

      Zeigt den Volumentyp an.

    - SnapLock Typ

      Zeigt den SnapLock Typ des Volume an. Die Optionen sind Compliance, Enterprise und Non-SnapLock.

    - Snapshot Kopie

      Zeigt die Snapshot-Kopie an, die für den Basistransfer verwendet wird. Wenn das Quell-Volume lesen/schreiben ist, bedeutet der Wert „Default“ in der Spalte „Snapshot-Kopie“, dass standardmäßig eine neue Snapshot-Kopie erstellt und für den Basistransfer verwendet wird. Wenn das Quell-Volume ein Datensicherungs-Volume ist, bedeutet der Wert „Default“ in der Spalte „Snapshot-Kopie“, dass keine neue Snapshot-Kopie erstellt wird und alle vorhandenen Snapshot-

Kopien an das Ziel übertragen werden. Beim Klicken auf den Wert der Snapshot-Kopie wird eine Liste von Snapshot-Kopien angezeigt, aus der eine vorhandene Snapshot-Kopie für den Basistransfer ausgewählt werden kann. Wenn der Quelltyp Datensicherung ist, kann keine andere Standard-Snapshot-Kopie ausgewählt werden.

SnapMirror Registerkarte

Ermöglicht die Angabe eines Ziel-Clusters, einer Storage Virtual Machine (SVM) und eines Aggregats für eine Schutzbeziehung sowie einer Namenskonvention für Ziele beim Erstellen einer SnapMirror Beziehung. Sie können außerdem eine SnapMirror Richtlinie und einen Zeitplan festlegen.

- **Topologieansicht**

  Zeigt eine visuelle Darstellung der Beziehung an, die Sie erstellen. Die SnapMirror Zielressource in der Topologie ist standardmäßig hervorgehoben.

- **Zielinformationen**

  Ermöglicht die Auswahl der Zielressourcen für eine Schutzbeziehung:

  - Erweiterter Link

    Öffnet das Dialogfeld „Erweiterte Zieleinstellungen“, wenn Sie eine SnapMirror Beziehung erstellen.

  - Cluster

    Listet die Cluster auf, die als Schutzzielhosts verfügbar sind. Dieses Feld ist erforderlich.

  - Storage Virtual Machine (SVM)

    Listet die auf dem ausgewählten Cluster verfügbaren SVMs auf. Ein Cluster muss ausgewählt werden, bevor die SVM-Liste angezeigt wird. Dieses Feld ist erforderlich.

  - Aggregat

    Listet die für die ausgewählte SVM verfügbaren Aggregate auf. Vor der Anzeige der Aggregatliste muss ein Cluster ausgewählt werden. Dieses Feld ist erforderlich. Die Aggregatliste enthält folgende Informationen:

    - Rang

      Wenn mehrere Aggregate alle Anforderungen für ein Ziel erfüllen, gibt der Rang gemäß den folgenden Bedingungen die Priorität an, in der das Aggregat aufgeführt ist:

      A. Zur Trennung der Fehlerdomänen ist ein Aggregat auf einem anderen Knoten als dem Knoten des Quell-Volumes vorzuziehen.
      B. Ein Aggregat auf einem Knoten mit weniger Volumes ist zu bevorzugen, um den Lastausgleich zwischen den Knoten in einem Cluster zu ermöglichen.
      C. Ein Aggregat, das mehr freien Platz als andere Aggregate hat, wird bevorzugt, um einen Kapazitätsausgleich zu ermöglichen. Ein Rang von 1 bedeutet, dass das Aggregat gemäß den drei Kriterien am meisten bevorzugt wird.

    - Aggregatname

      Name des Aggregats

- Verfügbare Kapazität
- Verfügbarer Speicherplatz auf dem Aggregat für Daten
- Ressourcenpool

  Name des Ressourcenpools, zu dem das Aggregat gehört

◦ Namenskonvention

Legt die standardmäßige Namenskonvention fest, die auf das Zielvolume angewendet wird. Sie können die bereitgestellte Namenskonvention übernehmen oder eine benutzerdefinierte erstellen. Die Namenskonvention kann die folgenden Attribute enthalten: %C, %M, %V und %N, wobei %C der Clustername, %M der SVM-Name, %V das Quellvolume und %N der Topologie-Ziel-Node-Name ist.

Das Feld für die Namenskonvention wird rot hervorgehoben, wenn Ihre Eingabe ungültig ist. Durch Klicken auf den Link „`Preview Name`“ wird eine Vorschau der von Ihnen eingegebenen Namenskonvention angezeigt, und der Vorschautext wird beim Eingeben einer Namenskonvention in das Textfeld dynamisch aktualisiert. Beim Erstellen der Beziehung wird dem Zielnamen ein Suffix zwischen 001 und 999 angehängt, das das im Vorschautext angezeigte nnn ersetzt, wobei zuerst 001, dann 002 usw. zugewiesen wird.

- **Beziehungseinstellungen**

Ermöglicht Ihnen, die maximale Transferrate, die SnapMirror Richtlinie und den Zeitplan festzulegen, die für die Schutzbeziehung verwendet werden:

◦ Maximale Transferrate

Gibt die maximale Transferrate an, mit der Daten zwischen Clustern über das Netzwerk übertragen werden. Falls keine maximale Transferrate verwendet wird, ist der Basistransfer zwischen Beziehungen unbegrenzt.

◦ SnapMirror Richtlinie

Legt die ONTAP SnapMirror Richtlinie für die Beziehung fest. Der Standardwert ist DPDefault.

◦ Richtlinie erstellen

Öffnet das Dialogfeld „SnapMirror Richtlinie erstellen“, in dem Sie eine neue SnapMirror Richtlinie erstellen und verwenden können.

◦ SnapMirror Zeitplan

Gibt die ONTAP SnapMirror Richtlinie für die Beziehung an. Verfügbare Zeitpläne sind None, 5min, 8hour, daily, hourly und weekly. Der Standardwert ist None, was angibt, dass der Beziehung kein Zeitplan zugeordnet ist. Beziehungen ohne Zeitpläne haben keine Lag-Statuswerte, es sei denn, sie gehören zu einem Storage-Service.

◦ Zeitplan erstellen

Öffnet das Dialogfeld „Zeitplan erstellen“, mit dem ein neuer SnapMirror Zeitplan erstellt werden kann.

SnapVault Registerkarte

Damit können Sie ein sekundäres Cluster, eine SVM und ein Aggregat für eine Schutzbeziehung sowie eine Namenskonvention für sekundäre Volumes beim Erstellen einer SnapVault Beziehung angeben. Außerdem

können Sie eine SnapVault Richtlinie und einen Zeitplan angeben.

- **Topologieansicht**

  Zeigt eine visuelle Darstellung der erstellten Beziehung. Die SnapVault sekundäre Ressource in der Topologie ist standardmäßig hervorgehoben.

- **Sekundärinformationen**

  Ermöglicht die Auswahl der sekundären Ressourcen für eine Schutzbeziehung:

  - Erweiterter Link

    Öffnet das Dialogfeld „Erweiterte Sekundäreinstellungen“.

  - Cluster

    Listet die Cluster auf, die als sekundäre Schutzhosts verfügbar sind. Dieses Feld ist erforderlich.

  - Storage Virtual Machine (SVM)

    Listet die auf dem ausgewählten Cluster verfügbaren SVMs auf. Ein Cluster muss ausgewählt werden, bevor die SVM-Liste angezeigt wird. Dieses Feld ist erforderlich.

  - Aggregat

    Listet die für die ausgewählte SVM verfügbaren Aggregate auf. Vor der Anzeige der Aggregatliste muss ein Cluster ausgewählt werden. Dieses Feld ist erforderlich. Die Aggregatliste enthält folgende Informationen:

    - Rang

      Wenn mehrere Aggregate alle Anforderungen für ein Ziel erfüllen, gibt der Rang gemäß den folgenden Bedingungen die Priorität an, in der das Aggregat aufgeführt ist:

      A. Für die Trennung der Fehlerdomänen ist ein Aggregat vorzuziehen, das sich auf einem anderen Node als dem Node des primären Volume befindet.
      B. Ein Aggregat auf einem Knoten mit weniger Volumes ist zu bevorzugen, um den Lastausgleich zwischen den Knoten in einem Cluster zu ermöglichen.
      C. Ein Aggregat, das mehr freien Platz als andere Aggregate hat, wird bevorzugt, um einen Kapazitätsausgleich zu ermöglichen. Ein Rang von 1 bedeutet, dass das Aggregat gemäß den drei Kriterien am meisten bevorzugt wird.

    - Aggregatname

      Name des Aggregats

    - Verfügbare Kapazität
    - Verfügbarer Speicherplatz auf dem Aggregat für Daten
    - Ressourcenpool

      Name des Ressourcenpools, zu dem das Aggregat gehört

  - Namenskonvention

Gibt die Standard-Namenskonvention an, die auf das sekundäre Volume angewendet wird. Sie können die bereitgestellte Namenskonvention übernehmen oder eine benutzerdefinierte erstellen. Die Namenskonvention kann die folgenden Attribute enthalten: %C, %M, %V und %N, wobei %C der Clustername, %M der SVM-Name, %V das Quell-Volume und %N der Node-Name des sekundären Topologieknotens ist.

Das Feld „Namenskonvention“ wird rot hervorgehoben, wenn Ihr Eintrag ungültig ist. Beim Klicken auf den Link „`Preview Name`“ wird eine Vorschau der eingegebenen Namenskonvention angezeigt, und der Vorschautext wird beim Eingeben einer Namenskonvention in das Textfeld dynamisch aktualisiert. Wenn ein ungültiger Wert eingegeben wird, werden die ungültigen Informationen im Vorschaubereich als rote Fragezeichen angezeigt. Beim Erstellen der Beziehung wird an den sekundären Namen ein Suffix zwischen 001 und 999 angehängt, das die im Vorschautext angezeigte Zeichenfolge „nnn“ ersetzt, wobei zuerst 001, dann 002 usw. zugewiesen wird.

- **Beziehungseinstellungen**

  Damit können Sie die maximale Transferrate, die SnapVault Richtlinie und den SnapVault Zeitplan festlegen, die bzw. den die Schutzbeziehung verwendet:

  - Maximale Transferrate

    Gibt die maximale Transferrate an, mit der Daten zwischen Clustern über das Netzwerk übertragen werden. Falls keine maximale Transferrate verwendet wird, ist der Basistransfer zwischen Beziehungen unbegrenzt.

  - SnapVault Richtlinie

    Legt die ONTAP SnapVault Richtlinie für die Beziehung fest. Der Standardwert ist XDPDefault.

  - Richtlinie erstellen

    Öffnet das Dialogfeld „SnapVault Richtlinie erstellen“, mit dem Sie eine neue SnapVault Richtlinie erstellen und verwenden können.

  - SnapVault Zeitplan

    Gibt den ONTAP SnapVault Zeitplan für die Beziehung an. Verfügbare Zeitpläne sind None, 5min, 8hour, daily, hourly und weekly. Der Standardwert ist None, was angibt, dass der Beziehung kein Zeitplan zugeordnet ist. Beziehungen ohne Zeitpläne haben keine Lag-Statuswerte, es sei denn, sie gehören zu einem Storage-Service.

  - Zeitplan erstellen

    Öffnet das Dialogfeld „Zeitplan erstellen“, mit dem Sie einen SnapVault Zeitplan erstellen können.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Stornieren**

  Verwirft Ihre Auswahl und schließt das Dialogfeld „Schutz konfigurieren“.

- **Anwenden**

  Wendet Ihre Auswahl an und startet den Schutzprozess.

Im Dialogfeld „Zeitplan erstellen“ in Active IQ Unified Manager

Das Dialogfeld „Zeitplan erstellen“ ermöglicht das Erstellen eines einfachen oder erweiterten Schutzzeitplans für Übertragungen von SnapMirror und SnapVault Beziehungen. Es kann beispielsweise ein neuer Zeitplan erstellt werden, um die Häufigkeit der Datenübertragungen aufgrund häufiger Datenaktualisierungen zu erhöhen, oder ein weniger häufiger Zeitplan, wenn sich Daten nur selten ändern.

Zeitpläne können für SnapMirror Synchronous Beziehungen nicht konfiguriert werden.

- **Ziel-Cluster**

  Der Name des Clusters, den Sie auf der Registerkarte SnapVault oder SnapMirror im Dialogfeld „Schutz konfigurieren“ ausgewählt haben.

- **Name des Zeitplans**

  Der von Ihnen angegebene Name für den Zeitplan. Zeitplannamen dürfen aus den Zeichen A bis Z, a bis z, 0 bis 9 sowie den folgenden Sonderzeichen bestehen: ! @ # $ % ^ & * ( ) _ -. Zeitplannamen dürfen die folgenden Zeichen nicht enthalten: < >.

- **Basic oder Advanced**

  Der gewünschte Zeitplanmodus.

  Der Basismodus umfasst folgende Elemente:

  - Wiederholen

    Wie häufig eine geplante Übertragung stattfindet. Zur Auswahl stehen stündlich, täglich und wöchentlich.

  - Tag

    Wenn die Option „Wöchentliche Wiederholung“ ausgewählt ist, wird der Wochentag angezeigt, an dem die Übertragung erfolgt.

  - Zeit

    Wenn „Täglich“ oder „Wöchentlich“ ausgewählt ist, wird die Tageszeit angezeigt, zu der die Übertragung erfolgt.

    Der erweiterte Modus umfasst folgende Elemente:

  - Monate

    Eine durch Kommas getrennte numerische Liste, die die Monate des Jahres darstellt. Gültige Werte sind 0 bis 11, wobei 0 für Januar steht usw. Dieses Element ist optional. Wenn das Feld leer bleibt, bedeutet dies, dass die Übertragungen jeden Monat erfolgen.

  - Tage

    Eine durch Kommas getrennte numerische Liste, die den Tag des Monats angibt. Gültige Werte sind 1 bis 31. Dieses Element ist optional. Wenn das Feld leer bleibt, bedeutet dies, dass an jedem Tag des Monats eine Übertragung stattfindet.

- Wochentage

  Eine durch Kommas getrennte numerische Liste, die die Wochentage darstellt. Gültige Werte sind 0 bis 6, wobei 0 für Sonntag steht usw. Dieses Element ist optional. Wenn das Feld leer bleibt, erfolgt eine Übertragung an jedem Wochentag. Wenn ein Wochentag, aber kein Monatstag angegeben ist, erfolgt eine Übertragung nur am angegebenen Wochentag und nicht jeden Tag.

- Stunden

  Eine durch Kommas getrennte numerische Liste, die die Anzahl der Stunden eines Tages angibt. Gültige Werte sind 0 bis 23, wobei 0 für Mitternacht steht. Dieses Element ist optional.

- Minuten

  Eine durch Kommas getrennte numerische Liste, die die Minuten einer Stunde darstellt. Gültige Werte sind 0 bis 59. Dieses Element ist erforderlich.

Im Active IQ Unified Manager steht das Dialogfeld „SnapMirror Richtlinie erstellen“ zur Verfügung

Im Dialogfeld „SnapMirror Richtlinie erstellen“ können Sie eine Richtlinie erstellen, um die Priorität für SnapMirror Transfers festzulegen. Mithilfe von Richtlinien maximieren Sie die Effizienz von Übertragungen von der Quelle zum Ziel.

- **Ziel-Cluster**

  Der Name des Clusters, das Sie auf der Registerkarte SnapMirror im Dialogfeld „Schutz konfigurieren“ ausgewählt haben.

- **Ziel-SVM**

  Der Name der SVM, die Sie auf der SnapMirror Registerkarte des Dialogfelds „Schutz konfigurieren“ ausgewählt haben.

- **Richtlinienname**

  Der Name für die neue Richtlinie. Richtliniennamen können aus den Zeichen A bis Z, a bis z, 0 bis 9, Punkt (.), Bindestrich (-) und Unterstrich (_) bestehen.

- **Transferpriorität**

  Die Priorität, mit der ein Transfer für asynchrone Vorgänge ausgeführt wird. Es kann entweder „Normal“ oder „Niedrig“ ausgewählt werden. Transferbeziehungen mit Richtlinien, die eine normale Transferpriorität festlegen, werden vor solchen mit Richtlinien ausgeführt, die eine niedrige Transferpriorität festlegen.

- **Kommentar**

  Ein optionales Feld, in dem Sie Kommentare zur Richtlinie hinzufügen können.

- **Transferneustart**

  Gibt an, welche Neustartaktion erfolgt, wenn eine Übertragung durch einen Abbruchvorgang oder einen Fehler, z. B. einen Netzwerkausfall, unterbrochen wird. Sie können eine der folgenden Optionen auswählen:

  - Stets

Gibt an, dass vor dem Neustart eines Transfers eine neue Snapshot Kopie erstellt wird und der Transfer dann, falls vorhanden, von einem Checkpoint aus neu gestartet wird, gefolgt von einem inkrementellen Transfer von der neu erstellten Snapshot Kopie.

◦ Niemals

Legt fest, dass unterbrochene Übertragungen niemals neu gestartet werden.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Stornieren**

  Verwirft die Auswahl und schließt das Dialogfeld „Schutz konfigurieren“.

- **Anwenden**

  Übernimmt Ihre Auswahl und startet den Schutzprozess.

Das Dialogfeld „Richtlinie erstellen“ für SnapVault in Active IQ Unified Manager

Das Dialogfeld „SnapVault Richtlinie erstellen“ ermöglicht das Erstellen einer Richtlinie zum Festlegen der Priorität für SnapVault Übertragungen. Mithilfe von Richtlinien lässt sich die Effizienz von Übertragungen vom primären zum sekundären Volume maximieren.

- **Ziel-Cluster**

  Der Name des Clusters, den Sie auf der SnapVault Registerkarte des Dialogfelds „Schutz konfigurieren“ ausgewählt haben.

- **Ziel-SVM**

  Der Name der SVM, die Sie auf der SnapVault Registerkarte des Dialogfelds „Schutz konfigurieren“ ausgewählt haben.

- **Richtlinienname**

  Der Name für die neue Richtlinie. Richtliniennamen können aus den Zeichen A bis Z, a bis z, 0 bis 9, Punkt (.), Bindestrich (-) und Unterstrich (_) bestehen.

- **Transferpriorität**

  Die Priorität, mit der die Übertragung ausgeführt wird. Es kann entweder Normal oder Low ausgewählt werden. Übertragungsbeziehungen mit Richtlinien, die eine normale Übertragungspriorität festlegen, werden vor solchen mit Richtlinien ausgeführt, die eine niedrige Übertragungspriorität festlegen. Die Standardeinstellung ist Normal.

- **Kommentar**

  Ein optionales Feld, in dem Sie einen Kommentar von bis zu 255 Zeichen zur SnapVault Richtlinie hinzufügen können.

- **Zugriffszeit ignorieren**

Legt fest, ob inkrementelle Übertragungen für Dateien ignoriert werden, bei denen sich nur die Zugriffszeit geändert hat.

- **Replikationsetikett**

  Die Tabelle listet die Regeln auf, die den von ONTAP ausgewählten Snapshot Kopien mit einer bestimmten Replikationsbezeichnung in einer Richtlinie zugeordnet sind. Folgende Informationen und Aktionen sind ebenfalls verfügbar:

  - Befehlsschaltflächen

    Mithilfe der Befehlsschaltflächen können Sie folgende Aktionen ausführen:

    - Hinzufügen

      Ermöglicht das Erstellen einer Snapshot Kopie Bezeichnung und einer Aufbewahrungsanzahl.

    - Anzahl der Aufbewahrungen bearbeiten

      Ermöglicht das Ändern der Aufbewahrungsanzahl für eine vorhandene Snapshot-Kopierbezeichnung. Die Aufbewahrungsanzahl muss eine Zahl zwischen 1 und 251 sein. Die Summe aller Aufbewahrungsanzahlen für alle Regeln darf 251 nicht überschreiten.

    - Löschen

      Ermöglicht das Löschen einer vorhandenen Bezeichnung für eine Snapshot Kopie.

  - Snapshot Kopie-Label

    Zeigt die Bezeichnung der Snapshot-Kopie an. Wenn Sie ein oder mehrere Volumes mit derselben lokalen Snapshot-Kopierrichtlinie auswählen, wird für jede Bezeichnung in der Richtlinie ein Eintrag angezeigt. Wenn Sie mehrere Volumes mit zwei oder mehr lokalen Snapshot-Kopierrichtlinien auswählen, zeigt die Tabelle alle Bezeichnungen aus allen Richtlinien an.

  - Zeitplan

    Zeigt den Zeitplan an, der jeder Snapshot-Kopiebezeichnung zugeordnet ist. Wenn einer Bezeichnung mehr als ein Zeitplan zugeordnet ist, werden die Zeitpläne für diese Bezeichnung in einer durch Kommas getrennten Liste angezeigt. Wenn mehrere Volumes mit derselben Bezeichnung, aber unterschiedlichen Zeitplänen ausgewählt werden, wird „Verschiedene“ angezeigt, um darauf hinzuweisen, dass den ausgewählten Volumes mehr als ein Zeitplan zugeordnet ist.

  - Anzahl der Aufbewahrungen am Ziel

    Zeigt die Anzahl der Snapshot Kopien mit der angegebenen Bezeichnung an, die auf dem SnapVault Sekundärsystem aufbewahrt werden. Bei Bezeichnungen mit mehreren Zeitplänen wird die Summe der Aufbewahrungsanzahlen aller Bezeichnungs- und Zeitplanpaare angezeigt. Wenn mehrere Volumes mit zwei oder mehr lokalen Snapshot Kopierichtlinien ausgewählt sind, ist die Aufbewahrungsanzahl leer.

Bearbeiten einer Schutzbeziehung in Active IQ Unified Manager

Sie können eine bestehende Schutzbeziehung bearbeiten, um die maximale Transferrate, die Datensicherungsstrategie oder den Sicherungszeitplan zu ändern.

Zielinformationen

- **Ziel-Cluster**

  Der Name des ausgewählten Ziel-Clusters.

- **Ziel-SVM**

  Der Name der ausgewählten SVM

- **Beziehungseinstellungen**

  Ermöglicht Ihnen, die maximale Transferrate, die SnapMirror Richtlinie und den Zeitplan festzulegen, die für die Schutzbeziehung verwendet werden:

  - Maximale Transferrate

    Gibt die maximale Rate an, mit der Basisdaten zwischen Clustern über das Netzwerk übertragen werden. Wenn diese Option ausgewählt ist, wird die Netzwerkbandbreite auf den von Ihnen angegebenen Wert begrenzt. Sie können einen numerischen Wert eingeben und dann entweder Kilobyte pro Sekunde (KB/s), Megabyte pro Sekunde (MB/s), Gigabyte pro Sekunde (GB/s) oder Terabyte pro Sekunde (TB/s) auswählen. Die von Ihnen angegebene maximale Transferrate muss größer als 1 KB/s und kleiner als 4 TB/s sein. Wenn keine maximale Transferrate verwendet wird, ist der Basistransfer zwischen den Beziehungen unbegrenzt. Wenn der primäre Cluster und der sekundäre Cluster identisch sind, ist diese Einstellung deaktiviert.

  - SnapMirror Richtlinie

    Legt die ONTAP SnapMirror Richtlinie für die Beziehung fest. Der Standardwert ist DPDefault.

  - Richtlinie erstellen

    Öffnet das Dialogfeld „SnapMirror Richtlinie erstellen“, in dem Sie eine neue SnapMirror Richtlinie erstellen und verwenden können.

  - SnapMirror Zeitplan

    Gibt die ONTAP SnapMirror Richtlinie für die Beziehung an. Verfügbare Zeitpläne sind None, 5min, 8hour, daily, hourly und weekly. Der Standardwert ist None, was angibt, dass der Beziehung kein Zeitplan zugeordnet ist. Beziehungen ohne Zeitpläne haben keine Lag-Statuswerte, es sei denn, sie gehören zu einem Storage-Service.

  - Zeitplan erstellen

    Öffnet das Dialogfeld „Zeitplan erstellen“, mit dem ein neuer SnapMirror Zeitplan erstellt werden kann.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Stornieren**

  Verwirft die Auswahl und schließt das Dialogfeld „Schutz konfigurieren“.

- **Einreichen**

Übernimmt Ihre Auswahl und schließt das Dialogfeld „Beziehung bearbeiten“.

Im Active IQ Unified Manager steht das Dialogfeld „Initialisieren/Aktualisieren“ zur Verfügung

Im Dialogfeld „Initialisieren/Aktualisieren“ können Sie entweder einen erstmaligen Basistransfer für eine neue Schutzbeziehung durchführen oder eine bereits initialisierte Beziehung aktualisieren, wenn Sie eine manuelle, ungeplante, inkrementelle Aktualisierung durchführen möchten.

Registerkarte „Übertragungsoptionen“

Auf der Registerkarte „Transfer Options“ können Sie die Initialisierungspriorität eines Transfers und die während Transfers verwendete Bandbreite ändern.

- **Transferpriorität**

  Die Priorität, mit der der Transfer ausgeführt wird. Es kann entweder „Normal“ oder „Niedrig“ ausgewählt werden. Beziehungen mit Datensicherungsstrategien, die eine normale Transferpriorität festlegen, werden vor solchen ausgeführt, die eine niedrige Transferpriorität festlegen. „Normal“ ist standardmäßig ausgewählt.

- **Maximale Transferrate**

  Legt die maximale Transferrate fest, mit der Daten zwischen Clustern über das Netzwerk übertragen werden. Wenn Sie keine maximale Transferrate verwenden, ist der Basistransfer zwischen Beziehungen unbegrenzt. Wenn Sie mehr als eine Beziehung mit unterschiedlichen maximalen Transferraten auswählen, können Sie eine der folgenden Einstellungen für die maximale Transferrate festlegen:

  - Verwendet werden die Werte, die beim Einrichten oder Bearbeiten der einzelnen Beziehungen angegeben wurden.

    Wenn diese Option ausgewählt ist, verwenden Initialisierungs- und Aktualisierungsvorgänge die maximale Transferrate, die zum Zeitpunkt der Erstellung oder Bearbeitung der jeweiligen Beziehung festgelegt wurde. Dieses Feld ist nur verfügbar, wenn mehrere Beziehungen mit unterschiedlichen Transferraten initialisiert oder aktualisiert werden.

  - Unbegrenzt

    Zeigt an, dass für Übertragungen zwischen Beziehungen keine Bandbreitenbeschränkung besteht. Dieses Feld ist nur verfügbar, wenn mehrere Beziehungen mit unterschiedlichen Transferraten initialisiert oder aktualisiert werden.

  - Bandbreite begrenzen auf

    Wenn diese Option ausgewählt ist, wird die Netzwerkbandbreite auf den von Ihnen angegebenen Wert begrenzt. Sie können einen numerischen Wert eingeben und dann entweder Kilobyte pro Sekunde (KB/s), Megabyte pro Sekunde (MB/s), Gigabyte pro Sekunde (GB/s) oder Terabyte pro Sekunde (TB/s) auswählen. Die von Ihnen angegebene maximale Transferrate muss größer als 1 KB/s und kleiner als 4 TB/s sein.

Registerkarte „Quell-Snapshot Kopien“

Die Registerkarte „Quell-Snapshot-Kopien“ zeigt die folgenden Informationen zur Quell-Snapshot-Kopie an, die für den Basistransfer verwendet wird:

- **Quell-Volume**

  Zeigt die Namen der entsprechenden Quellvolumes an.

- **Ziel-Volume**

  Zeigt die Namen der ausgewählten Ziel-Volumes an.

- **Quellentyp**

  Zeigt den Volume-Typ an. Der Typ kann entweder Read/write oder Data Protection sein.

- **Snapshot-Kopie**

  Zeigt die Snapshot-Kopie an, die für den Datentransfer verwendet wird. Wenn Sie auf den Wert der Snapshot-Kopie klicken, wird das Dialogfeld „Select Source Snapshot Copy“ angezeigt, in dem Sie abhängig vom Typ der Datensicherungsbeziehung und vom ausgeführten Vorgang eine bestimmte Snapshot-Kopie für Ihren Datentransfer auswählen können. Die Option zum Angeben einer anderen Snapshot-Kopie ist für Quellen des Datensicherungstyps nicht verfügbar.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Stornieren**

  Verwirft Ihre Auswahl und schließt das Dialogfeld „Initialisieren/Aktualisieren“.

- **Einreichen**

  Speichert Ihre Auswahl und startet den Initialisierungs- oder Aktualisierungsvorgang.

Im Active IQ Unified Manager steht das Dialogfeld „Resynchronisieren“ zur Verfügung

Mit dem Dialogfeld „Resynchronisieren“ lassen sich Daten in einer SnapMirror oder SnapVault Beziehung resynchronisieren, die zuvor unterbrochen wurde und deren Ziel anschließend in ein lesen/schreiben-Volume umgewandelt wurde. Eine Resynchronisierung kann auch erforderlich sein, wenn eine erforderliche gemeinsame Snapshot-Kopie auf dem Quellvolume gelöscht wird und dadurch SnapMirror oder SnapVault Aktualisierungen fehlschlagen.

Registerkarte „Resynchronisierungsoptionen“

Über die Registerkarte „Resynchronisierungsoptionen“ können Sie die Übertragungspriorität und die maximale Transferrate für die Schutzbeziehung festlegen, die Sie resynchronisieren.

- **Transferpriorität**

  Die Priorität, mit der der Transfer ausgeführt wird. Sie können entweder „Normal“ oder „Niedrig“ auswählen. Beziehungen mit Richtlinien, die eine normale Transferpriorität festlegen, werden vor solchen mit Richtlinien ausgeführt, die eine niedrige Transferpriorität festlegen.

- **Maximale Transferrate**

Legt die maximale Rate fest, mit der Daten über das Netzwerk zwischen Clustern übertragen werden. Wenn diese Option ausgewählt ist, wird die Netzwerkbandbreite auf den von Ihnen angegebenen Wert begrenzt. Sie können einen numerischen Wert eingeben und anschließend Kilobyte pro Sekunde (KB/s), Megabyte pro Sekunde (MB/s), Gigabyte pro Sekunde (GB/s) oder TB/s auswählen. Wenn Sie keine maximale Transferrate verwenden, ist der Basistransfer zwischen Beziehungen unbegrenzt.

Registerkarte „Quell-Snapshot Kopien“

Die Registerkarte „Quell-Snapshot-Kopien“ zeigt die folgenden Informationen zur Quell-Snapshot-Kopie an, die für den Basistransfer verwendet wird:

- **Quell-Volume**

  Zeigt die Namen der entsprechenden Quellvolumes an.

- **Ziel-Volume**

  Zeigt die Namen der ausgewählten Ziel-Volumes an.

- **Quellentyp**

  Zeigt den Volume-Typ an: entweder lesen/schreiben oder Datenschutz.

- **Snapshot-Kopie**

  Zeigt die Snapshot-Kopie an, die für den Datentransfer verwendet wird. Wenn Sie auf den Wert der Snapshot-Kopie klicken, wird das Dialogfeld „Quell-Snapshot-Kopie auswählen“ angezeigt, in dem Sie abhängig von der Art der Schutzbeziehung und dem Vorgang, den Sie ausführen, eine bestimmte Snapshot-Kopie für Ihren Transfer auswählen können.

Befehlsschaltflächen

- **Einreichen**

  Startet den Resynchronisierungsvorgang und schließt das Dialogfeld „Resynchronisieren“.

- **Stornieren**

  Verwirft Ihre Auswahl und schließt das Dialogfeld „Resynchronisieren“.

Im Active IQ Unified Manager kann das Dialogfeld „Quell-Snapshot-Kopie auswählen“ verwendet werden

Im Dialogfeld „Quell-Snapshot-Kopie auswählen“ erfolgt die Auswahl einer bestimmten Snapshot-Kopie für den Datentransfer zwischen Schutzbeziehungen, oder es wird das Standardverhalten verwendet, das davon abhängt, ob eine Beziehung initialisiert, aktualisiert oder resynchronisiert wird und ob es sich bei der Beziehung um SnapMirror oder SnapVault handelt.

Standard

Zum Festlegen des Standardverhaltens für die Bestimmung der Snapshot-Kopie, die für Initialisierungs-, Aktualisierungs- und Resynchronisierungsübertragungen für SnapVault und SnapMirror Beziehungen verwendet wird.

Wenn Sie einen SnapVault Transfer durchführen, ist das Standardverhalten für jeden Vorgang wie folgt:

Betrieb	Standardverhalten von SnapVault, wenn die Quelle auf lesen/schreiben gesetzt ist	Standardverhalten von SnapVault, wenn die Quelle Data Protection (DP) ist
Initialisieren	Erstellt eine neue Snapshot-Kopie und überträgt diese.	Überträgt die zuletzt exportierte Snapshot Kopie.
Aktualisieren	Übertragen werden nur gekennzeichnete Snapshot-Kopien, wie in der Richtlinie angegeben.	Überträgt die zuletzt exportierte Snapshot Kopie.
Resynchronisieren	Überträgt alle gekennzeichneten Snapshot Kopien, die nach der neuesten gemeinsamen Snapshot Kopie erstellt wurden.	Überträgt die neueste gekennzeichnete Snapshot Kopie.

Wenn Sie einen SnapMirror Transfer durchführen, ist das Standardverhalten für jeden Vorgang wie folgt:

Betrieb	Standardmäßiges SnapMirror Verhalten	Standardverhalten von SnapMirror, wenn die Beziehung der zweite Hop in einer Kaskade von SnapMirror zu SnapMirror ist
Initialisieren	Erstellung einer neuen Snapshot-Kopie und Übertragung dieser sowie aller Snapshot-Kopien, die vor der neuen Snapshot-Kopie erstellt wurden.	Überträgt alle Snapshot Kopien aus der Quelle.
Aktualisieren	Erstellung einer neuen Snapshot-Kopie und Übertragung dieser sowie aller Snapshot-Kopien, die vor der neuen Snapshot-Kopie erstellt wurden.	Überträgt alle Snapshot Kopien.
Resynchronisieren	Erstellt eine neue Snapshot Kopie und überträgt anschließend alle Snapshot Kopien von der Quelle.	Überträgt alle Snapshot-Kopien vom sekundären Volume auf das tertiäre Volume und löscht alle Daten, die nach der Erstellung der neuesten gemeinsamen Snapshot-Kopie hinzugefügt wurden.

Vorhandene Snapshot Copy

Ermöglicht die Auswahl einer vorhandenen Snapshot Kopie aus der Liste, sofern die Auswahl einer Snapshot Kopie für diesen Vorgang zulässig ist.

- **Snapshot-Kopie**

  Zeigt die vorhandenen Snapshot-Kopien an, aus denen Sie eine für die Übertragung auswählen können.

- **Erstellungsdatum**

  Zeigt das Datum und die Uhrzeit an, zu der die Snapshot-Kopie erstellt wurde. Die Snapshot-Kopien sind von der neuesten zur ältesten aufgelistet, wobei die neueste ganz oben in der Liste steht.

Wenn Sie einen SnapVault Transfer durchführen und eine vorhandene Snapshot Kopie auswählen möchten, um sie von einer Quelle an ein Ziel zu übertragen, ist das Verhalten für die einzelnen Vorgänge wie folgt:

Betrieb	SnapVault Verhalten beim Angeben einer Snapshot Kopie	SnapVault Verhalten beim Angeben einer Snapshot Kopie in einer Kaskade
Initialisieren	Überträgt die angegebene Snapshot Kopie.	Die Auswahl von Quell Snapshot Kopien wird für Datensicherungsvolumes nicht unterstützt.
Aktualisieren	Überträgt die angegebene Snapshot Kopie.	Die Auswahl von Quell Snapshot Kopien wird für Datensicherungsvolumes nicht unterstützt.
Resynchronisieren	Überträgt die ausgewählte Snapshot Kopie.	Die Auswahl von Quell Snapshot Kopien wird für Datensicherungsvolumes nicht unterstützt.

Wenn Sie eine SnapMirror Übertragung durchführen und eine vorhandene Snapshot-Kopie zur Übertragung von einer Quelle zu einem Ziel auswählen möchten, verhält sich das Verhalten für jeden Vorgang wie folgt:

Betrieb	SnapMirror Verhalten beim Angeben einer Snapshot-Kopie	SnapMirror Verhalten beim Angeben einer Snapshot-Kopie in einer Kaskade
Initialisieren	Überträgt alle Snapshot-Kopien auf dem Quellsystem bis zur angegebenen Snapshot-Kopie.	Die Auswahl von Quell Snapshot Kopien wird für Datensicherungsvolumes nicht unterstützt.
Aktualisieren	Überträgt alle Snapshot-Kopien auf dem Quellsystem bis zur angegebenen Snapshot-Kopie.	Die Auswahl von Quell Snapshot Kopien wird für Datensicherungsvolumes nicht unterstützt.
Resynchronisieren	Überträgt alle Snapshot Kopien von der Quelle bis zur ausgewählten Snapshot Kopie und löscht anschließend alle Daten, die nach der Erstellung der neuesten gemeinsamen Snapshot Kopie hinzugefügt wurden.	Die Auswahl von Quell Snapshot Kopien wird für Datensicherungsvolumes nicht unterstützt.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aufgaben ausführen:

- **Einreichen**

  Übermittelt Ihre Auswahl und schließt das Dialogfeld „Quell-Snapshot-Kopie auswählen“.

- **Stornieren**

Verwirft Ihre Auswahl und schließt das Dialogfeld „Quell-Snapshot-Kopie auswählen“.

Umgekehrte Resynchronisierung in Active IQ Unified Manager

Wenn eine Schutzbeziehung unterbrochen ist, weil das Quellvolume deaktiviert ist und das Zielvolume in ein lesen/schreiben Volume umgewandelt wird, ermöglicht die umgekehrte Resynchronisierung die Umkehrung der Beziehungsrichtung, sodass das Zielvolume zur neuen Quelle und die Quelle zum neuen Zielvolume wird.

Wenn ein Katastrophenfall das Quellvolume in Ihrer Schutzbeziehung deaktiviert, können Sie das Zielvolume zur Datenbereitstellung verwenden, indem Sie es in lesen/schreiben konvertieren, während Sie das Quellvolume reparieren oder ersetzen, das Quellvolume aktualisieren und die Beziehung wiederherstellen. Bei einer umgekehrten Resynchronisierung werden die Daten auf dem Quellvolume gelöscht, die neuer sind als die Daten in der gemeinsamen Snapshot-Kopie.

Vor der umgekehrten Resynchronisierung

Zeigt die Quelle und das Ziel einer Beziehung vor einer umgekehrten Resynchronisierung an.

- **Quell-Volume**

  Der Name und der Speicherort des Quell-Volumes vor einem umgekehrten Resynchronisierungsvorgang.

- **Ziel-Volume**

  Der Name und der Speicherort des Ziel-Volumes vor einem umgekehrten Resynchronisierungsvorgang.

Nach der umgekehrten Resynchronisierung

Zeigt an, was nach einem Reserve-Resynchronisierungsvorgang die Quelle und das Ziel einer Beziehung sind.

- **Quell-Volume**

  Der Name und Speicherort des Quell-Volumes nach einem umgekehrten Resynchronisierungsvorgang.

- **Ziel-Volume**

  Der Name und der Speicherort des Ziel-Volumes nach einer umgekehrten Resynchronisierung.

Befehlsschaltflächen

Mithilfe der Befehlsschaltflächen können Sie folgende Aktionen ausführen:

- **Einreichen**

  Beginnt den umgekehrten Resynchronisierungsprozess.

- **Stornieren**

  Schließt das Dialogfeld „Umgekehrte Resynchronisierung“, ohne eine umgekehrte Resynchronisierungsoperation auszulösen.

Anzeige der Beziehungen: Alle Beziehungen in Active IQ Unified Manager

Die Ansicht „Beziehung: Alle Beziehungen“ zeigt Informationen über Schutzbeziehungen im Storage-System.

Standardmäßig enthält der Bericht, der beim Aufrufen der Seite „Relationships“ angezeigt wird, die Schutzbeziehungen der obersten Ebene für Volumes und Storage VMs. Mit den Steuerelementen am oberen Rand der Seite lassen sich eine bestimmte Ansicht auswählen, Suchen zum Auffinden bestimmter Objekte ausführen, Filter zum Eingrenzen der Liste der angezeigten Daten erstellen und anwenden, Spalten auf der Seite hinzufügen, entfernen oder neu anordnen und die Daten auf der Seite in eine Datei im Format .csv, .pdf oder .xlsx exportieren. Nach dem Anpassen der Seite lassen sich die Ergebnisse als benutzerdefinierte Ansicht speichern, und es lässt sich ein Bericht über diese Daten planen, der regelmäßig erstellt und per E-Mail versendet wird. Standardmäßig enthält der angezeigte Bericht beim Auswählen des Menüs **Relationships** Schutzbeziehungen für Volumes und Storage VMs in Ihrem Datacenter. Mit der Option **Filter** lassen sich nur ausgewählte Storage-Systeme anzeigen, also beispielsweise nur Volumes oder nur Storage VMs. Derselbe Bericht wird auf der Seite Storage angezeigt und nur für die ausgewählte Storage-Entität. Wenn Beziehungen von Volumes oder Storage VMs angezeigt werden sollen, kann entweder die Seite **Storage** > **Volumes** > **Relationship: All Relationships** oder **Protection** > **Relationships** > **Relationship: All Relationships** aufgerufen werden. Anschließend lässt sich die Option **Relationship Object Type** in **Filter** verwenden, um nur Daten zu Volumes oder Storage VMs zu filtern.

Auf der Seite „Beziehungen“, auf der alle Schutzbeziehungen aufgelistet sind, befindet sich für den Ziel-Cluster der Link **Im System Manager anzeigen**, über den dieselben Objekte im ONTAP System Manager angezeigt werden können.

- **Status**

  Zeigt den aktuellen Status der Schutzbeziehung an.

  Der Status kann Fehler (), Warnung () oder OK () sein.

- **Quell-Storage-VM**

  Zeigt den Namen der Quell-SVM an. Weitere Details zur Quell-SVM können durch Klicken auf den SVM-Namen angezeigt werden.

  Wenn eine SVM im Cluster vorhanden ist, aber noch nicht dem Unified Manager Inventar hinzugefügt wurde oder wenn die SVM nach der letzten Aktualisierung des Clusters erstellt wurde, ist dieses Feld leer. Es ist sicherzustellen, dass die SVM vorhanden ist, oder eine erneute Clustererkennung ist durchzuführen, um die Ressourcenliste zu aktualisieren.

- **Quelle**

  Je nach Ihrer Auswahl wird entweder das geschützte Quellvolume oder die geschützte source storage VM angezeigt. Weitere Details zum Quellvolume oder zur storage VM können durch Klicken auf den Namen des Volumes oder der storage VM angezeigt werden.

  Wird diese Meldung `Resource-key not discovered` angezeigt, kann dies darauf hindeuten, dass das Volume zwar im Cluster vorhanden ist, aber noch nicht dem Unified Manager Inventar hinzugefügt wurde, oder dass es nach der letzten Aktualisierung des Clusters erstellt wurde. Dabei muss sichergestellt sein, dass das Volume vorhanden ist, oder auf dem Cluster muss eine erneute Erkennung durchgeführt werden, um die Ressourcenliste zu aktualisieren.

- **Ziel-Storage VM**

Zeigt den Namen der Ziel-SVM an. Durch Klicken auf den SVM-Namen können Sie weitere Details zur Ziel-SVM anzeigen.

- **Ziel**

  Zeigt den Namen des Zielvolumes oder der Storage VM basierend auf Ihrer Auswahl an. Weitere Details zum Zielvolume oder zur Storage VM lassen sich durch Klicken auf den jeweiligen Objektnamen anzeigen.

- **Beziehungsobjekttyp**

  Zeigt den Typ des in der Beziehung verwendeten Objekts an, z. B. Storage VM, Volume oder Consistency Group. Bei Objekten in einer Konsistenzbeziehung werden die Beziehungsquelle und -ziele sowie die Consistency Group angezeigt. Ein Klick darauf führt zur LUN-Seite, auf der die Beziehung angezeigt wird.

- **Richtlinie**

  Zeigt den Namen der Datensicherungsstrategie für die SnapMirror Beziehung an. Ein Klick auf den Namen der Datensicherungsstrategie zeigt die zugehörigen Details an, darunter die folgenden Informationen:

  - Übertragungspriorität

    Legt die Priorität fest, mit der eine Übertragung für asynchrone Vorgänge ausgeführt wird. Die Übertragungspriorität ist „Normal“ oder „Niedrig“. Übertragungen mit normaler Priorität werden vor Übertragungen mit niedriger Priorität geplant. Der Standardwert ist „Normal“.

  - Zugriffszeit ignorieren

    Gilt nur für SnapVault Beziehungen. Diese Einstellung legt fest, ob inkrementelle Übertragungen Dateien ignorieren, deren Zugriffszeit sich lediglich geändert hat. Die Werte sind entweder True oder False. Der Standardwert ist False.

  - Wenn eine Beziehung nicht synchron ist

    Legt die Aktion fest, die ONTAP ausführt, wenn eine synchrone Beziehung nicht synchronisiert werden kann. StrictSync Beziehungen schränken den Zugriff auf das primäre Volume ein, wenn die Synchronisierung mit dem sekundären Volume fehlschlägt. Sync Beziehungen schränken den Zugriff auf das primäre Volume nicht ein, wenn die Synchronisierung mit dem sekundären Volume fehlschlägt.

  - Versuchslimit

    Legt die maximale Anzahl von Versuchen fest, die für jede manuelle oder geplante Übertragung einer SnapMirror Beziehung unternommen werden. Der Standardwert ist 8.

  - Kommentare

    Bietet ein Textfeld für Kommentare, die speziell für die ausgewählte Richtlinie gelten.

  - SnapMirror Etikett

    Gibt die SnapMirror Bezeichnung für den ersten Zeitplan an, der der Snapshot-Kopierrichtlinie zugeordnet ist. Die SnapMirror Bezeichnung wird vom SnapVault Subsystem verwendet, wenn Sie Snapshot-Kopien zu einem SnapVault Ziel sichern.

  - Aufbewahrungseinstellung

    Legt fest, wie lange Backups aufbewahrt werden, basierend auf der Zeit oder der Anzahl der Backups.

- Tatsächliche Snapshot Copies

  Gibt die Anzahl der Snapshot Kopien auf diesem Volume an, die mit der angegebenen Bezeichnung übereinstimmen.

- Snapshot Kopien beibehalten

  Gibt die Anzahl der SnapVault Snapshot-Kopien an, die nicht automatisch gelöscht werden, selbst wenn das für die Richtlinie festgelegte Limit erreicht ist. Die Werte sind entweder True oder False. Der Standardwert ist False.

- Warnschwelle für die Aufbewahrung

  Legt die Snapshot Kopie-Grenze fest, bei der eine Warnung gesendet wird, die anzeigt, dass die maximale Aufbewahrungsgrenze nahezu erreicht ist.

- **Verzögerungsdauer**

  Zeigt die Zeitspanne an, um die die Daten auf dem Spiegel gegenüber der Quelle hinterherhinken.

  Die Verzögerungsdauer sollte bei StrictSync Beziehungen nahe bei oder gleich 0 Sekunden liegen.

- **Lag-Status**

  Zeigt den Verzögerungsstatus für verwaltete Beziehungen und für nicht verwaltete Beziehungen an, denen ein Zeitplan zugeordnet ist. Der Verzögerungsstatus kann Folgendes sein:

  - Fehler

    Die Verzögerungsdauer ist größer oder gleich dem Schwellenwert für den Verzögerungsfehler.

  - Warnung

    Die Verzögerungsdauer ist größer als oder gleich dem Schwellenwert für die Verzögerungswarnung.

  - OK

    Die Verzögerungsdauer liegt im normalen Bereich.

  - Nicht zutreffend

    Der Verzögerungsstatus ist für synchrone Beziehungen nicht anwendbar, da kein Zeitplan konfiguriert werden kann.

- **Letzte erfolgreiche Aktualisierung**

  Zeigt den Zeitpunkt der letzten erfolgreichen SnapMirror- oder SnapVault-Operation an.

  Das letzte erfolgreiche Update ist für synchrone Beziehungen nicht anwendbar.

- **Konstituentenbeziehungen**

  Zeigt an, ob im ausgewählten Objekt Volumina vorhanden sind.

- **Beziehungsart**

Zeigt den Beziehungstyp an, der zum Replizieren eines Volumes verwendet wird. Zu den Beziehungstypen gehören:

- Asynchroner Spiegel
- Asynchroner Vault
- Asynchrones MirrorVault
- StrictSync
- Synchronisieren

- **Übertragungsstatus**

Zeigt den Übertragungsstatus für die Schutzbeziehung an. Der Übertragungsstatus kann einer der folgenden sein:

- Abbruch

  SnapMirror Übertragungen sind aktiviert; es wird jedoch derzeit ein Vorgang zum Abbruch einer Übertragung ausgeführt, der möglicherweise die Entfernung des Checkpoints umfasst.

- Überprüfung

  Das Ziel-Volume wird derzeit diagnostisch überprüft, und es findet kein Datentransfer statt.

- Finalisierung

  SnapMirror Übertragungen sind aktiviert. Das Volume befindet sich aktuell in der Nachübertragungsphase für inkrementelle SnapVault Übertragungen.

- Leerlauf

  Transfers sind aktiviert, und es wird kein Transfer ausgeführt.

- In-Sync

  Die Daten in den beiden Volumes in der synchronen Beziehung sind synchronisiert.

- Nicht synchronisiert

  Die Daten im Ziel-Volume sind nicht mit dem Quell-Volume synchronisiert.

- Vorbereitung

  SnapMirror Übertragungen sind aktiviert. Das Volume befindet sich aktuell in der Vorübertragungsphase für inkrementelle SnapVault Übertragungen.

- In der Warteschlange

  SnapMirror Transfers sind aktiviert. Derzeit sind keine Transfers in Bearbeitung.

- Ruhend

  SnapMirror Transfers sind deaktiviert. Es ist kein Transfer im Gange.

- Anhalten

Eine SnapMirror Übertragung ist im Gange. Zusätzliche Übertragungen sind deaktiviert.

- Übertragung

  SnapMirror Datentransfers sind aktiviert, und ein Transfer wird ausgeführt.

- Übergang

  Der asynchrone Datentransfer vom Quell- zum Ziel-Volume ist abgeschlossen, und der Übergang zum synchronen Betrieb hat begonnen.

- Warten

  Ein SnapMirror Transfer wurde eingeleitet, aber einige zugehörige Aufgaben warten darauf, in die Warteschlange eingereiht zu werden.

- **Dauer des letzten Transfers**

  Zeigt die Zeit an, die für den Abschluss des letzten Datentransfers benötigt wurde.

  Die Übertragungsdauer gilt nicht für StrictSync Beziehungen, da die Übertragung gleichzeitig erfolgen sollte.

- **Größe der letzten Übertragung**

  Zeigt die Größe des letzten Datentransfers in Byte an.

  Die Übertragungsgröße ist für StrictSync Beziehungen nicht zutreffend.

- **Mediatoren**

  Anzeige des Mediatorstatus.

  - Nicht zutreffend

    Wenn der Cluster SnapMirror active sync nicht unterstützt.

  - Nicht konfiguriert

    Falls dies nicht konfiguriert ist oder zwar konfiguriert ist, aber nur der Ziel-Cluster und nicht der Quell-Cluster in Unified Manager hinzugefügt wurde.

  - Mediator IP-Adresse

    Wenn dies konfiguriert ist und sowohl Quell- als auch Ziel-Cluster in Unified Manager hinzugefügt wurden.

- **Zustand**

  Zeigt den Status der SnapMirror oder SnapVault Beziehung an. Der Status kann Uninitialized, SnapMirrored oder Broken-Off sein. Wenn ein Quellvolume ausgewählt ist, ist der Beziehungsstatus nicht anwendbar und wird nicht angezeigt.

- **Beziehungsintegrität**

  Zeigt den Integritätsstatus der Beziehung des Clusters an.

- **Grund für den fehlerhaften Zustand**

  Der Grund, warum sich die Beziehung in einem fehlerhaften Zustand befindet.

- **Transferpriorität**

  Zeigt die Priorität an, mit der ein Transfer ausgeführt wird. Die Transferpriorität ist „Normal“ oder „Niedrig“. Transfers mit normaler Priorität werden vor Transfers mit niedriger Priorität geplant.

  Die Übertragungspriorität ist für synchrone Beziehungen nicht anwendbar, da alle Übertragungen mit derselben Priorität behandelt werden.

- **Zeitplan**

  Zeigt den Namen des der Beziehung zugeordneten Schutzzeitplans an.

  Der Zeitplan gilt nicht für synchrone Beziehungen.

- **Versionsflexible Replikation**

  Es wird entweder „Ja“, „Ja mit Backup-Option“ oder „Keine“ angezeigt.

- **Quell-Cluster**

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Quell-Clusters für die SnapMirror Beziehung an.

- **FQDN des Quell-Clusters**

  Zeigt den Namen des Quell-Clusters für die SnapMirror Beziehung an.

- **Quell-Node**

  Zeigt den Namen des Links für den Quell-Node-Namen der SnapMirror Beziehung eines Volumes an und zeigt den Link zur Node-Anzahl der SnapMirror Beziehung an, wenn das Objekt eine Storage VM oder eine Konsistenzgruppe ist.

In der benutzerdefinierten Ansicht können Sie beim Klicken auf den Link für den Node-Name den Schutz für Storage Objekte anzeigen und erweitern, zu denen die Volumes dieser Konsistenzgruppen in einer SnapMirror Active Sync Beziehung gehören.

Wenn Sie auf den Link „Knotenanzahl“ klicken, gelangen Sie zur Knotenseite mit den zugehörigen Knoten dieser Beziehung. Ist die Knotenanzahl 0, wird kein Wert angezeigt, da keine Knoten mit dieser Beziehung verknüpft sind.

- **Ziel-Node**

  Zeigt den Link des Ziel-Node-Namens für die SnapMirror Beziehung eines Volumes an und zeigt den Link zur Node-Anzahl der SnapMirror Beziehung an, wenn das Objekt eine Storage VM oder eine Konsistenzgruppe ist.

  Wenn Sie auf den Link „Knotenanzahl“ klicken, gelangen Sie zur Knotenseite mit den zugehörigen Knoten dieser Beziehung. Ist die Knotenanzahl 0, wird kein Wert angezeigt, da keine Knoten mit dieser Beziehung verknüpft sind.

- **Ziel-Cluster**

Zeigt den Namen des Ziel-Clusters für die SnapMirror Beziehung an.

- **Ziel-Cluster-FQDN**

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Ziel-Clusters für die SnapMirror Beziehung an.

- **Geschützt durch**

  Zeigt die verschiedenen Beziehungen an. In dieser Spalte können Sie die Volume- und Konsistenzgruppenbeziehungen für Cluster und die Reihenfolge der Storage Virtual Machines anzeigen, einschließlich:

  - SnapMirror
  - Storage VM DR
  - SnapMirror, Storage-VM-DR
  - Konsistenzgruppe
  - SnapMirror, Konsistenzgruppe.

Verwandte Informationen

- Informationen zur Ansicht **Beziehung: MetroCluster** finden Sie unter "Überwachung von MetroCluster Konfigurationen".
- Informationen zur Ansicht **Beziehung: Transferstatus des letzten Monats** sind unter "Beziehung: Ansicht des Übertragungsstatus des letzten Monats" verfügbar.
- Informationen zur Ansicht **Beziehung: Alle Beziehungen** sind unter "Beziehung: Ansicht der Datentransferrate des letzten Monats" verfügbar.

Anzeige der Ansicht „Transferstatus des letzten Monats“ in Active IQ Unified Manager

Die Ansicht „Beziehung: Übertragungsstatus des letzten 1 Monats“ ermöglicht die Analyse der Übertragungstrends über einen bestimmten Zeitraum für Volumes und Storage VMs in asynchronen Beziehungen. Auf dieser Seite wird außerdem angezeigt, ob die Übertragung erfolgreich war oder fehlgeschlagen ist.

Die Steuerelemente am oberen Rand der Seite ermöglichen die Suche nach bestimmten Objekten, das Erstellen und Anwenden von Filtern zur Eingrenzung der Liste der angezeigten Daten, das Hinzufügen, Entfernen und Neuanordnen von Spalten auf der Seite sowie den Export der Daten auf der Seite in eine `.csv`, `.pdf` oder `.xlsx` Datei. Nachdem Sie die Seite angepasst haben, können Sie die Ergebnisse als benutzerdefinierte Ansicht speichern und die regelmäßige Erstellung und den E-Mail-Versand eines Berichts über diese Daten planen. Mit der Option **Filter** lassen sich nur ausgewählte Storage-Systeme anzeigen, beispielsweise nur Volumes oder nur Storage VMs. Derselbe Bericht wird auf der Seite **Storage** und nur für die ausgewählte Storage-Entität angezeigt. Wenn Sie beispielsweise Volume-Beziehungen anzeigen möchten, können Sie für die Storage VMs entweder über das Menü **Storage** > **Storage VMs** > **Relationship: Last 1 Month Transfer Status** oder über das Menü **Protection** > **Relationships** > **Relationship: Last 1 Month Transfer Status** auf den Bericht zugreifen und mit dem **Filter** nur Daten für Volumes anzeigen.

- **Quell-Volume**

  Zeigt den Namen des Quell-Volumes an.

- **Ziel-Volume**

Zeigt den Namen des Ziel-Volumes an.

- **Vorgangstyp**

  Zeigt die Art der Volumenübertragung an.

- **Operationsergebnis**

  Zeigt an, ob die Volumenübertragung erfolgreich war.

- **Übertragungsbeginn**

  Zeigt die Startzeit der Volume-Übertragung an.

- **Endzeit der Übertragung**

  Zeigt die Endzeit der Volume-Übertragung an.

- **Übertragungsdauer**

  Zeigt die für die Volumenübertragung benötigte Zeit (in Stunden) an.

- **Transfergröße**

  Zeigt die Größe (in MB) des übertragenen Volumes an.

- **Quell-SVM**

  Zeigt den Namen der Storage Virtual Machine (SVM) an.

- **Quell-Cluster**

  Zeigt den Namen des Quell-Clusters an.

- **Ziel-SVM**

  Zeigt den Namen der Ziel-SVM an.

- **Ziel-Cluster**

  Zeigt den Namen des Ziel-Clusters an.

Verwandte Informationen

- Informationen zur Ansicht **Beziehung: Alle Beziehungen** sind unter "Beziehung: Ansicht Alle Beziehungen" verfügbar.
- Informationen zur Ansicht **Beziehung:MetroCluster** finden Sie unter "Überwachung von MetroCluster Konfigurationen".
- Informationen zur Ansicht **Beziehung: Alle Beziehungen** sind unter "Beziehung: Ansicht der Datentransferrate des letzten Monats" verfügbar.

Die Ansicht „Übertragungsrate des letzten Monats“ der Beziehung in Active IQ Unified Manager

Die Ansicht „Beziehung: Übertragungsrate des letzten Monats“ ermöglicht die Analyse des Datenvolumens, das für Volumes in asynchronen Beziehungen täglich übertragen

wird. Diese Seite bietet außerdem Details zu den täglichen Datentransfers und zur benötigten Zeit für den Abschluss des Übertragungsvorgangs für Volumes und Storage VMs.

Die Steuerelemente am oberen Rand der Seite ermöglichen Ihnen die Suche nach bestimmten Objekten, das Erstellen und Anwenden von Filtern zur Eingrenzung der Liste der angezeigten Daten, das Hinzufügen, Entfernen und Neuanordnen von Spalten auf der Seite sowie den Export der Daten auf der Seite in eine .csv-, .pdf- oder .xlsx-Datei. Nach der Anpassung der Seite können Sie die Ergebnisse als benutzerdefinierte Ansicht speichern und anschließend die regelmäßige Generierung und den E-Mail-Versand eines Berichts zu diesen Daten planen. Wenn Sie beispielsweise Volume-Beziehungen anzeigen möchten, können Sie entweder das Menü **Storage** > **Volumes** > **Relationship: Last 1 Month Transfer Rate** oder das Menü **Protection** > **Relationships** > **Relationships:Last 1 Month Transfer Rate** aufrufen und den **Filter** verwenden, um nur Daten für Volumes anzuzeigen.

- **Gesamtübertragungsgröße**

  Zeigt die Gesamtgröße der Volume-Übertragung in Gigabyte an.

- **Tag**

  Zeigt den Tag an, an dem die Volumenübertragung eingeleitet wurde.

- **Endzeit**

  Zeigt die Endzeit der Volume-Übertragung mit Datum an.

Verwandte Informationen

- Informationen zur Ansicht **Beziehung:MetroCluster** finden Sie unter "Überwachung von MetroCluster Konfigurationen".
- Informationen zur Ansicht **Beziehung: Transferstatus des letzten Monats** sind unter "Beziehung: Ansicht des Übertragungsstatus des letzten Monats" verfügbar.
- Informationen zur Ansicht **Beziehung: Alle Beziehungen** sind unter "Beziehung: Ansicht der Datentransferrate des letzten Monats" verfügbar.

Benutzerdefinierte Berichte generieren

Unified Manager Berichterstellung

Informationen zur Berichtsfunktion von Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) ermöglicht das Anzeigen, Anpassen, Herunterladen und Planen von Berichten für Ihre ONTAP Storage-Systeme. Die Berichte können Details zur Kapazität, zum Systemstatus, zur Performance, zur Sicherheit und zu den Schutzbeziehungen des Storage-Systems bereitstellen.

Die in Active IQ Unified Manager 9.6 eingeführte neue Berichts- und Planungsfunktionalität von Unified Manager ersetzt die vorherige Berichts-Engine, die in Unified Manager Version 9.5 eingestellt wurde.

Die Berichtsfunktion bietet verschiedene Ansichten Ihres Netzwerks und liefert wertvolle Erkenntnisse zu Kapazität, Systemstatus, Performance, Sicherheit und Schutzdaten. Sie können Ihre Ansichten individuell anpassen, indem Sie Spalten ein- und ausblenden, neu anordnen, Daten filtern und sortieren sowie die Ergebnisse durchsuchen. Benutzerdefinierte Ansichten lassen sich speichern und wiederverwenden, als Berichte herunterladen und als wiederkehrende Berichte per E-Mail verteilen.

Sie können Ansichten im Microsoft® Excel-Format herunterladen und anpassen. Sie können erweiterte Excel-Funktionen wie komplexe Sortierungen, mehrstufige Filter, Pivot-Tabellen und Diagramme verwenden. Wenn Sie mit dem resultierenden Excel-Bericht zufrieden sind, können Sie die Excel-Datei hochladen, damit sie bei jeder geplanten und freigegebenen Berichtserstellung verwendet wird.

Zusätzlich zur Erstellung von Berichten über die Benutzeroberfläche können Sie Daten zu Systemstatus, Sicherheit und Performance mit diesen weiteren Methoden aus Unified Manager extrahieren:

- Verwendung von Open Database Connectivity (ODBC) und ODBC-Tools für den direkten Zugriff auf die Datenbank zur Ermittlung von Clusterinformationen
- Ausführen von Unified Manager REST APIs, um die Informationen abzurufen, die Sie überprüfen möchten

In dieser Version von Active IQ Unified manager wurden folgende Verbesserungen an den Berichten vorgenommen:

- Eine E-Mail für einen Bericht wird gemäß dem konfigurierten Zeitplan gesendet. Auch wenn Sie einen Bericht bei Bedarf erstellen, erhalten Sie eine E-Mail.
- Der Dateiname des Berichts und die Metadaten des Berichts enthalten den Hostnamen, von dem der Bericht generiert wurde. Selbst wenn jemand den Dateinamen ändert, lässt sich dank dieser Verbesserung weiterhin der Hostname identifizieren, von dem der Bericht generiert wurde.

Zugriffspunkte zum Generieren von Berichten

Es gibt drei Möglichkeiten, auf die Berichtsfunktionen in Active IQ Unified Manager zuzugreifen.

Im Unified Manager können Sie Informationen über Ihre Cluster sammeln, um Berichte über die Benutzeroberfläche, MySQL-Datenbankabfragen und REST-APIs zu erstellen.

Diese Abschnitte beschreiben das Berichtswesen und die Terminplanung von Unified Manager über die

Benutzeroberfläche.

Es gibt drei Möglichkeiten, auf die Berichtsfunktionen von Unified Manager zuzugreifen:

- Direktes Extrahieren von Daten aus den Inventarseiten in der Benutzeroberfläche.
- Der Zugriff auf alle verfügbaren Objekte erfolgt über Open Database Connectivity (ODBC) und ODBC-Tools.
- Ausführen von Unified Manager REST APIs, um die Informationen zurückzugeben, die Sie überprüfen möchten.

Diese Abschnitte beschreiben das Berichtswesen und die Terminplanung von Unified Manager über die Benutzeroberfläche.

Zugriff auf Datenbanken für benutzerdefinierte Berichte in Active IQ Unified Manager

Unified Manager verwendet eine MySQL Datenbank, um Daten aus den Clustern zu speichern, die überwacht werden. Die Daten werden in verschiedenen Schemas der MySQL Datenbank gespeichert.

Alle Tabellendaten aus den folgenden Datenbanken sind verfügbar:

Datenbank	Beschreibung
netapp_model	Daten über die Objekte auf ONTAP Controllern.
netapp_model_view	Daten über die Objekte auf ONTAP Controllern, die für Berichtstools geeignet sind.
netapp_performance	Clusterspezifische Performance-Zähler.
ocum	Applikationsdaten und Informationen von Unified Manager zur Unterstützung der UI-Filterung, Sortierung und der Berechnung einiger abgeleiteter Felder.
ocum_report	Daten für Inventarkonfiguration und kapazitätsbezogene Informationen.
ocum_report_birt	Ansichten für Inventarkonfigurations- und kapazitätsbezogene Daten, geeignet zur Nutzung durch Berichtstools.
opm	Informationen zu Performance Konfigurationseinstellungen und Schwellenwerten.
scalemonitor	Daten zu Systemstatus- und Performanceproblemen der Unified Manager Applikation.
vmware_model	VMware-Objektdaten für Datastores, die auf NetApp Storage gehostet werden.
vmware_model_view	Ansichten für VMware-Objektdaten für auf NetApp Storage gehostete Datastores, geeignet für die Verwendung mit Berichtstools.
vmware_performance	VMware Performance-Counter-Daten für Datastores auf NetApp Storage.

Ein Reporting-Benutzer, also ein Datenbankbenutzer mit der Rolle Report Schema, kann auf die Daten in diesen Tabellen zugreifen. Dieser Benutzer hat direkt in der Unified Manager Datenbank schreibgeschützten Zugriff auf Reporting- und andere Datenbankansichten. Es ist zu beachten, dass dieser Benutzer keine Berechtigung für den Zugriff auf Tabellen mit Benutzerdaten oder Cluster-Anmeldeinformationen hat.

Active IQ Unified Manager REST APIs für die Berichterstellung verwenden

Mithilfe von REST APIs können Sie Ihre Cluster managen, indem Sie die von Unified Manager erfassten Informationen zu Systemstatus, Kapazität, Performance und Sicherheit einsehen.

REST APIs sind über die Swagger-Webseite verfügbar. Über die Swagger-Webseite können die Unified Manager REST API-Dokumentation angezeigt und API-Aufrufe manuell ausgeführt werden. Der Zugriff über die Unified Manager Web-UI erfolgt in der Menüleiste über die Schaltfläche **Help** und die anschließende Auswahl von **API Documentation**. Informationen zu Unified Manager REST APIs finden sich in "Erste Schritte mit Active IQ Unified Manager REST APIs".

Sie benötigen die Rolle „Operator“, „Storage Administrator“ oder „Application Administrator“, um auf die REST APIs zugreifen zu können.

Berichte in Active IQ Unified Manager verstehen

Berichte zeigen detaillierte Informationen zu Storage-, Netzwerk-, Quality of Service- und Schutzbeziehungen an und helfen Ihnen dabei, potenzielle Probleme zu erkennen und zu lösen, bevor sie auftreten.

Wenn Sie eine Ansicht anpassen, können Sie diese unter einem eindeutigen Namen zur späteren Verwendung speichern. Auf Grundlage dieser Ansicht kann außerdem ein Bericht geplant werden, der regelmäßig ausgeführt und mit anderen geteilt werden kann. Sie können die Ansicht auch in Excel herunterladen, um sie mithilfe erweiterter Excel-Funktionen anzupassen, und diese Datei anschließend wieder in Unified Manager hochladen. Wenn Sie mit dieser Ansicht einen Bericht planen, wird die hochgeladene Excel-Datei verwendet, um aussagekräftige Berichte zu erstellen, die geteilt werden können.

Auf der Seite „Berichtspläne“ ist das Managen aller geplanten Berichte möglich.

> Zum Managen von Berichten ist die Rolle „Application Administrator“ oder „Storage Administrator“ erforderlich.

Sie können Berichte als CSV-, Excel- oder PDF-Dateien herunterladen.

Die Beziehung zwischen Ansicht und Bericht in Active IQ Unified Manager

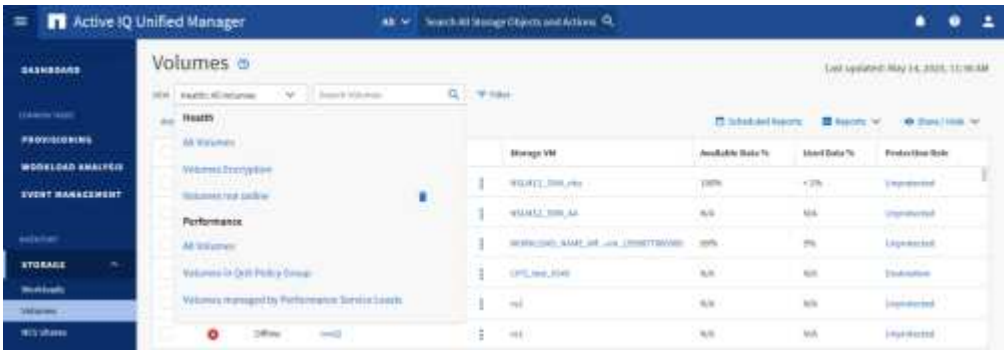
Ansichten und Inventarseiten werden zu Berichten, wenn Sie sie herunterladen oder planen.

Sie können Ansichten und Inventarseiten anpassen und zur Wiederverwendung speichern. Fast alles, was Sie in Unified Manager anzeigen können, lässt sich speichern, wiederverwenden, anpassen, planen und als Bericht freigeben.

Im Dropdown-Menü „Ansicht“ sind Elemente mit einem Löschsymbol vorhandene benutzerdefinierte Ansichten, die Sie oder ein anderer Benutzer erstellt haben. Elemente ohne Symbol sind Standardansichten, die mit Unified Manager bereitgestellt werden. Standardansichten können nicht geändert oder gelöscht

werden.

- Wenn Sie eine benutzerdefinierte Ansicht aus der Liste löschen, werden auch alle Excel-Dateien oder geplanten Berichte gelöscht, die diese Ansicht verwenden.
- Wenn Sie eine benutzerdefinierte Ansicht ändern, werden Berichte, die diese Ansicht verwenden, die Änderung bei der nächsten Erstellung und dem nächsten Versand per E-Mail gemäß dem Berichtszeitplan widerspiegeln. Beim Ändern von Ansichten ist sicherzustellen, dass Ihre Änderungen mit allen zugehörigen Excel-Anpassungen für die Berichte kompatibel sind. Bei Bedarf können Sie die Excel-Datei aktualisieren, indem Sie sie herunterladen, die erforderlichen Änderungen vornehmen und sie als neue Excel-Anpassung für die Ansicht hochladen.



Nur Benutzer mit der Rolle „Applikationsadministrator“ oder „Storage-Administrator“ können das Löschsymbol sehen, eine Ansicht ändern oder löschen oder einen geplanten Bericht ändern oder löschen.

Informationen zu den verschiedenen Berichtstypen in Active IQ Unified Manager

Diese Tabelle bietet eine umfassende Liste der Ansichten und Inventarseiten, die als Berichte verfügbar sind und die Sie anpassen, herunterladen und planen können.

Active IQ Unified Manager Berichte

Typ	Storage- oder Netzwerkobjekt
Kapazität	Cluster Aggregate Volumes Qtrees

Typ	Storage- oder Netzwerkobjekt
Systemzustand	Cluster Nodes Aggregate Storage VMs Volumes SMB/CIFS Freigaben NFS Shares
Performance	Cluster Nodes Aggregate Storage VMs Volumes LUNs NVMe Namespaces Netzwerkschnittstellen (LIFs) Ports
Servicequalität	Traditionelle QoS-Richtliniengruppen Adaptive QoS Richtliniengruppen Richtliniengruppen für Performance Service Level
Volumenschutzbeziehungen (verfügbar auf der Seite „Volumes“)	Alle Beziehungen Transferstatus des letzten Monats Transferrate des letzten Monats
Sicherheit	Storage VMs Cluster

Berichtsbeschränkungen in Active IQ Unified Manager verstehen

Es gibt einige Einschränkungen bei der neuen Berichtsfunktionalität von Active IQ Unified Manager, deren Sie sich bewusst sein sollten.

Vorhandene Berichte aus früheren Versionen von Unified Manager

Sie können nur den Zeitplan und die Empfänger für bestehende Berichte bearbeiten, die in Unified Manager 9.5 und früheren Versionen erstellt und importiert wurden (als .rptdesign-Dateien). Wenn Sie einen der mit Unified Manager 9.5 oder früheren Versionen bereitgestellten Standardberichte angepasst haben, werden diese benutzerdefinierten Berichte nicht in das neue Berichtstool importiert.

Zum Bearbeiten vorhandener Berichte, die aus .rptdesign-Dateien importiert wurden, steht eine der folgenden Vorgehensweisen zur Verfügung; anschließend ist der importierte Bericht zu entfernen:

- eine neue Ansicht erstellen und einen Bericht aus dieser Ansicht planen (bevorzugt)
- Sie können die Daten abrufen, indem Sie den Mauszeiger über den Bericht bewegen, die SQL-Anweisung kopieren und ein externes Tool verwenden.

Die Standardansichten können ohne Anpassungen als Berichte generiert werden. Mit der neuen Berichtslösung können beliebige benutzerdefinierte Berichte erstellt werden.

Beziehung zwischen Zeitplan und Bericht

Sie können für jeden gespeicherten Bericht beliebig viele verschiedene Zeitpläne mit beliebigen Empfängerkombinationen erstellen. Den Zeitplan können Sie jedoch nicht für mehrere Berichte wiederverwenden.

Berichtschutz

Jeder Benutzer mit den entsprechenden Berechtigungen kann Berichte bearbeiten oder löschen. Es gibt keine Möglichkeit, andere Benutzer daran zu hindern, gespeicherte Ansichten oder Zeitpläne zu entfernen oder zu ändern.

Ereignisberichte

Obwohl Sie die Ereignisansicht anpassen und den resultierenden Bericht im CSV-Format herunterladen können, können wiederkehrende Ereignisberichte nicht zur Erstellung und Verteilung geplant werden.

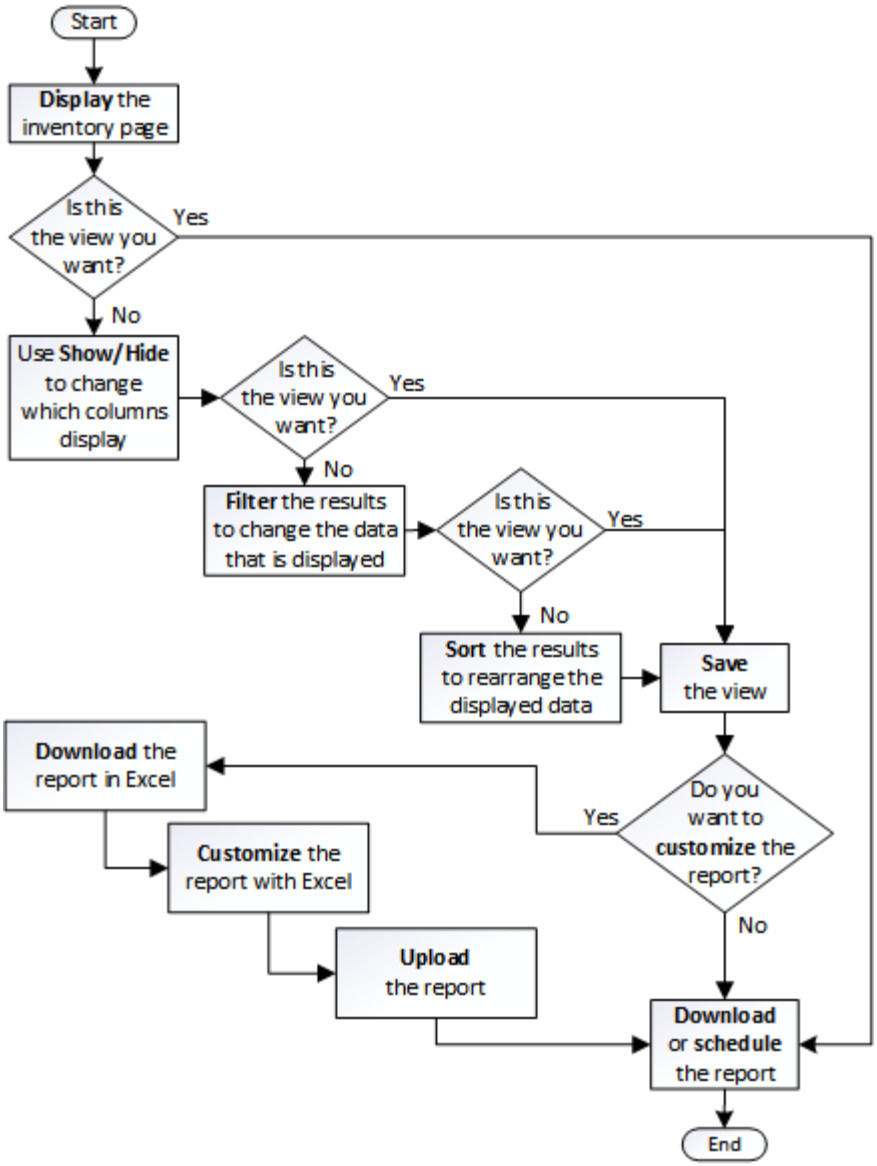
Berichtsanhänge

Berichte können nicht im Text einer E-Mail versendet werden. Stattdessen werden Berichte ausschließlich als PDF-, Excel- oder CSV-Anhang versendet.

Arbeiten mit Berichten

Berichtsworkflows in Active IQ Unified Manager verstehen

Entscheidungsbaum, der den Berichts Workflow beschreibt.



Erste Schritte mit der Berichtsfunktion in Active IQ Unified Manager

Es wird ein benutzerdefinierter Beispielbericht erstellt, um das Untersuchen von Ansichten und das Planen von Berichten kennenzulernen. Dieser Schnellstartbericht ermittelt eine Liste von Volumes, die Sie möglicherweise in den Cloud Tier verschieben möchten, da eine beträchtliche Menge inaktiver (kalter) Daten vorhanden ist. Dazu wird die Ansicht „Performance: All Volumes“ geöffnet, die Ansicht mithilfe von Filtern und Spalten angepasst, die benutzerdefinierte Ansicht als Bericht gespeichert und der Bericht für die wöchentliche Freigabe geplant.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen FabricPool Aggregate konfiguriert haben und Volumes auf diesen Aggregaten besitzen.

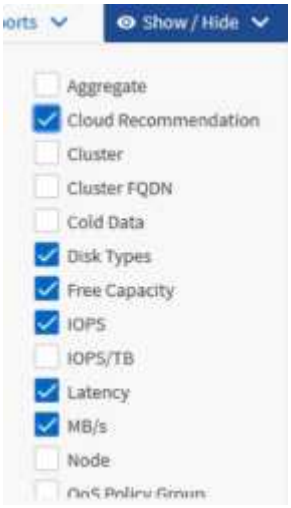
Im Folgenden wird beschrieben, wie Sie:

- Öffnen der Standardansicht

- Anpassen der Spalten durch Filtern und Sortieren der Daten
- Ansicht speichern
- Sie können die Generierung eines Berichts für die benutzerdefinierte Ansicht planen

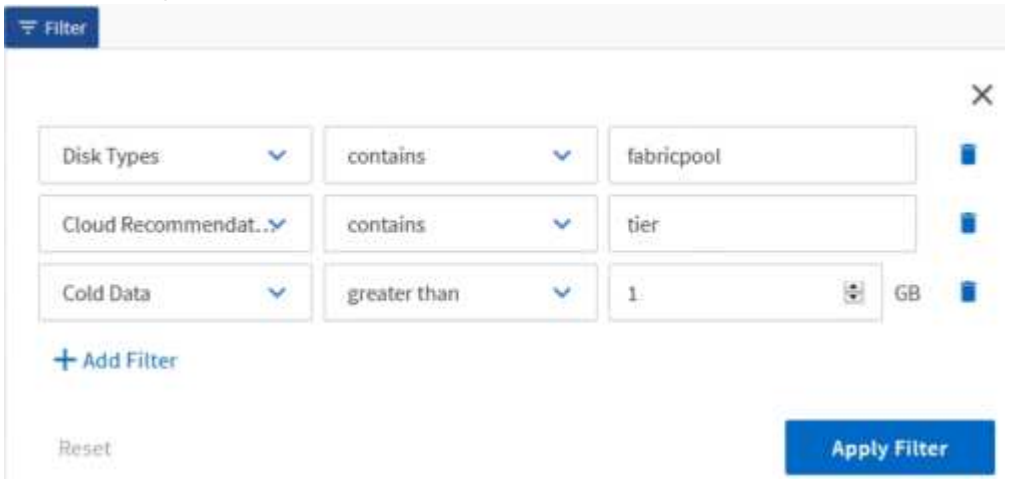
Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Performance** > **Alle Volumes**.
3. Über **Anzeigen/Ausblenden** lässt sich sicherstellen, dass die Spalte “Disk Types” in der Ansicht angezeigt wird.



Weitere Spalten können hinzugefügt oder entfernt werden, um eine Ansicht zu erstellen, die die für Ihren Bericht wichtigen Felder enthält.

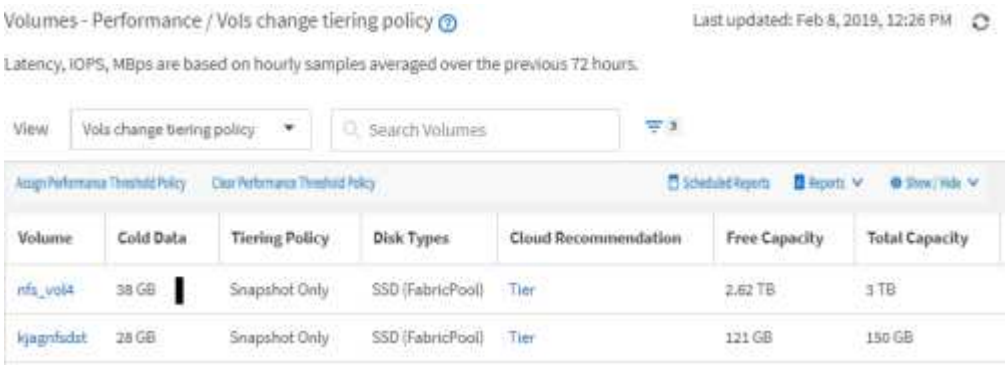
4. Die Spalte „`Disk Types`“ kann neben die Spalte „`Cloud Recommendation`“ gezogen werden.
5. Sie fügen die folgenden drei Filter hinzu, indem Sie auf das Filtersymbol und anschließend auf **Filter anwenden** klicken:
   - Datenträgertypen enthält FabricPool
   - Cloud Recommendation enthält Tier
   - Kalte Daten größer als 10 GB



Jeder Filter ist mit einem logischen UND verknüpft, sodass alle zurückgegebenen Volumes alle Kriterien

erfüllen müssen. Es können maximal fünf Filter hinzugefügt werden.

6. Durch Klicken auf den oberen Rand der Spalte „Kalte Daten“ werden die Ergebnisse so sortiert, dass die Volumes mit den meisten kalten Daten oben in der Ansicht erscheinen.
7. Wenn die Ansicht angepasst wird, lautet der Ansichtsname „Nicht gespeicherte Ansicht“. Die Ansicht sollte so benannt werden, dass sie widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel “Vols change tiering policy”. Anschließend lässt sich die Ansicht durch Klicken auf das Häkchen oder durch Drücken der Eingabetaste unter dem neuen Namen speichern.



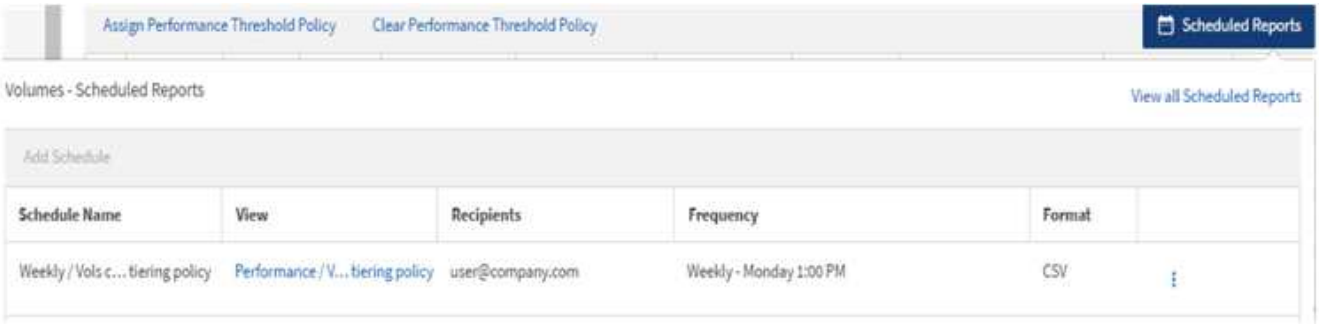
8. Sie können den Bericht als **CSV**-, **Excel**- oder **PDF**-Datei herunterladen, um die Ausgabe vor dem Planen oder Freigeben anzuzeigen.

   Die Datei kann mit einer installierten Applikation wie Microsoft Excel (CSV oder Excel) oder Adobe Acrobat (PDF) geöffnet oder gespeichert werden.

   > Sie können Ihren Bericht mithilfe komplexer Filter, Sortierungen, Pivot-Tabellen oder Diagramme weiter anpassen, indem Sie die Ansicht als Excel-Datei herunterladen. Nachdem Sie die Datei in Excel geöffnet haben, können Sie die erweiterten Funktionen nutzen, um Ihren Bericht anzupassen. Sobald das Ergebnis Ihren Anforderungen entspricht, können Sie die Excel-Datei hochladen. Diese Datei mit ihren Anpassungen wird beim Ausführen des Berichts auf die Ansicht angewendet.

   Weitere Informationen zur Anpassung von Berichten mit Excel enthält *Sample Microsoft Excel reports*.

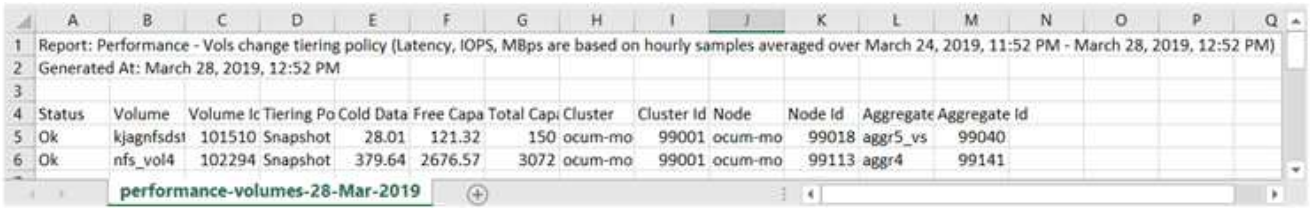
9. Auf der Inventarseite erfolgt die Auswahl der Schaltfläche **Geplante Berichte**. In der Liste erscheinen alle geplanten Berichte, die sich auf das Objekt beziehen, in diesem Fall Volumes.



10. Über **Zeitplan hinzufügen** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
11. Nach Eingabe eines Namens für den Bericht und Ausfüllen der übrigen Berichtsfelder erfolgt ein Klick auf das Häkchen (✓) am Ende der Zeile.

Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Der folgende Beispielbericht liegt im CSV-Format vor:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:52 PM - March 28, 2019, 12:52 PM)																
2	Generated At: March 28, 2019, 12:52 PM																
3																	
4	Status	Volume	Volume Ic	Tiering Po	Cold Data	Free Capa	Total Cap	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id				
5	Ok	kjagnfsdst	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040				
6	Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141				

performance-volumes-28-Mar-2019

Der folgende Beispielbericht liegt im PDF-Format vor:



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								
Ok								

Auf Grundlage der im Bericht angezeigten Ergebnisse kann es sinnvoll sein, ONTAP System Manager oder die ONTAP CLI zu verwenden, um die Tiering-Richtlinie für bestimmte Volumes in “auto” oder “all” zu ändern, um mehr kalte Daten auf das Cloud-Tier auszulagern.

Suche nach einem geplanten Bericht in Active IQ Unified Manager

Geplante Berichte können nach Name, Ansichtsname, Objekttyp oder Empfängern durchsucht werden.

1. Im linken Navigationsbereich ist **Storage Management** > **Report Schedules** auszuwählen.
2. Das Textfeld **Geplante Berichte suchen** dient zur Suche nach geplanten Berichten.

Berichte nach … finden	Ausprobieren …
Name des Zeitplans	Eingabe eines Teils des Namens des Berichtszeitplans.
Name der Ansicht	Einen Teil des Namens der Berichtsansicht eingeben. Standardansichten und benutzerdefinierte Ansichten erscheinen in der Ansichtsliste.
Empfänger	Eingabe eines Teils der E-Mail-Adresse.
Dateityp	Als Typ "PDF", "CSV" oder "XLSX" angeben.

3. Sie können auf eine Spaltenüberschrift klicken, um Berichte nach dieser Spalte in aufsteigender oder absteigender Reihenfolge zu sortieren, z. B. nach dem Namen des Zeitplans oder dem Format.

Berichte anpassen

Anpassen von Berichten in Active IQ Unified Manager

Es gibt viele Möglichkeiten zur Anpassung von Ansichten, sodass Sie einen Bericht erstellen können, der alle Informationen enthält, die Sie zum Managen Ihrer ONTAP Cluster benötigen.

Sie können mit einer Standard-Inventarseite oder einer benutzerdefinierten Ansicht beginnen und diese anschließend anpassen, indem Sie Spalten hinzufügen oder entfernen, die Spaltenreihenfolge ändern, die Daten filtern oder nach einer bestimmten Spalte in aufsteigender oder absteigender Reihenfolge sortieren.

Ab Unified Manager 9.8 können Sie die Ansicht auch als Excel-Datei herunterladen und mithilfe erweiterter Funktionen anpassen. Anschließend erfolgt der Upload der angepassten Excel-Datei. Wenn Sie einen Bericht mit dieser Ansicht planen, verwendet dieser die angepasste Excel-Datei, um aussagekräftige Berichte zu erstellen, die Sie teilen können.

Weitere Informationen zur Anpassung von Berichten mit Excel enthält *Sample Microsoft Excel reports*.

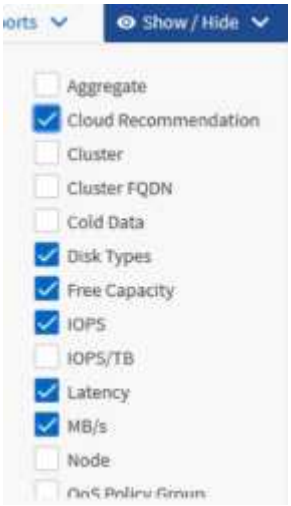
Zum Managen von Berichten ist die Rolle „Application Administrator“ oder „Storage Administrator“ erforderlich.

Spalten in einem Bericht in Active IQ Unified Manager anpassen

Mit **Show/Hide** können Sie die Spalten auswählen, die Sie in Ihrem Bericht verwenden möchten. Sie können die Spalten auf der Inventarseite per Drag-and-drop neu anordnen.

Schritte

1. Mit **Anzeigen/Ausblenden** lassen sich Spalten hinzufügen oder entfernen.



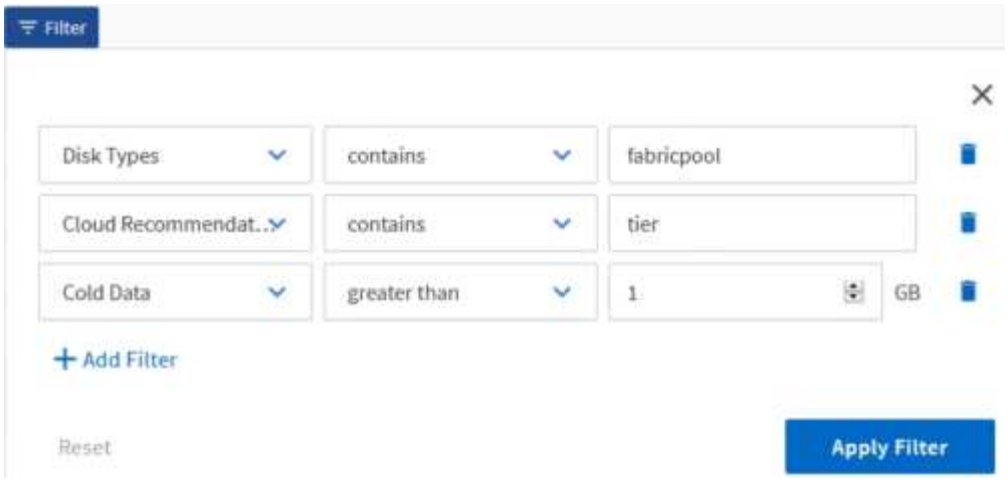
2. Auf der Inventarseite können Sie die Spalten per Drag & Drop in die gewünschte Reihenfolge für Ihren Bericht anordnen.
3. Zum Speichern Ihrer Änderungen ist die Benennung der nicht gespeicherten Ansicht erforderlich.

Daten in Active IQ Unified Manager filtern

Die Daten können so gefiltert werden, dass die Ergebnisse Ihren Berichtsanforderungen entsprechen. Durch das Filtern werden nur die Daten angezeigt, die für Sie von Interesse sind.

Schritte

1. Mit dem Filtersymbol lassen sich Filter hinzufügen, um die gewünschten Ergebnisse einzugrenzen; anschließend können Sie **Filter anwenden** auswählen.



2. Zum Speichern Ihrer Änderungen ist die Benennung der nicht gespeicherten Ansicht erforderlich.

Daten in Active IQ Unified Manager sortieren

Zum Sortieren der Ergebnisse können Sie eine Spalte auswählen und die aufsteigende oder absteigende Reihenfolge angeben. Durch das Sortieren der Daten lassen sich die Informationen priorisieren, die Sie für den Bericht benötigen.

Schritte

1. Durch Klicken auf den oberen Rand einer Spalte lassen sich die Ergebnisse so sortieren, dass die wichtigsten Informationen oben in der Ansicht angezeigt werden.
2. Zum Speichern Ihrer Änderungen ist die Benennung der nicht gespeicherten Ansicht erforderlich.

Suche zur Verfeinerung Ihrer Ansicht in Active IQ Unified Manager

Sobald die gewünschte Ansicht vorliegt, können die Ergebnisse mithilfe des Suchfelds weiter verfeinert werden, damit der Fokus auf den Ergebnissen liegt, die in den Bericht aufgenommen werden sollen.

Schritte

1. Die benutzerdefinierte oder Standardansicht, die Sie als Grundlage für Ihren Bericht verwenden möchten, wird geöffnet.
2. Im Suchfeld kann Text eingegeben werden, um die in der Ansicht aufgeführten Daten zu verfeinern. In jeder der angezeigten Spalten können Teildaten eingegeben werden. Wenn beispielsweise nach Knoten gesucht werden soll, deren Name "US_East" enthält, kann die vollständige Knotenliste eingegrenzt werden.

   Die Ergebnisse Ihrer Suche werden in der benutzerdefinierten Ansicht gespeichert und für den daraus resultierenden geplanten Bericht verwendet.

3. Zum Speichern Ihrer Änderungen ist die Benennung der nicht gespeicherten Ansicht erforderlich.

Excel dient zur Anpassung Ihres Berichts in Active IQ Unified Manager

Nachdem Sie die Ansicht gespeichert haben, können Sie sie im Excel-Arbeitsmappenformat (.xlsx) herunterladen. Beim Öffnen der Excel-Datei stehen Ihnen

erweiterte Excel-Funktionen zur Verfügung, um Ihren Bericht anzupassen.

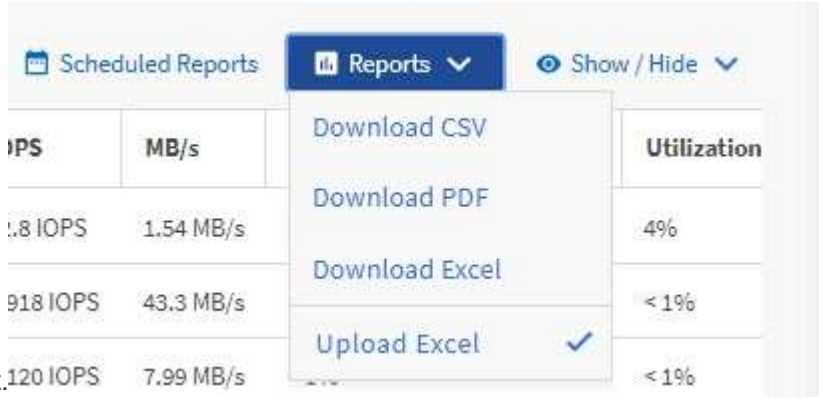
Bevor Sie beginnen

Sie können nur eine Excel Workbook-Datei mit der Dateiendung .xlsx hochladen.

Beispielsweise können Sie in Ihrem Bericht folgende erweiterte Excel-Funktionen verwenden:

- Sortierung über mehrere Spalten
- Komplexe Filterung
- Pivot-Tabellen
- Diagramme

- Die heruntergeladene Excel-Datei verwendet den Standarddateinamen für die Ansicht, nicht den von Ihnen gespeicherten Namen.
  - Das Format ist `<View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx`.
  - Beispielsweise hat eine benutzerdefinierte gespeicherte Ansicht namens `Volumes-not online` den Dateinamen `health-volumes-05-May-2020-19-18-00.xlsx`, wenn sie an diesem Tag und zu dieser Uhrzeit gespeichert wird.
- Sie können der Excel-Datei Tabellenblätter hinzufügen, vorhandene Tabellenblätter jedoch nicht ändern.
  - Vorhandene Tabellenblätter, Daten und Informationen sollten nicht geändert werden. Stattdessen können die Daten auf eine neu erstellte Seite kopiert werden.
  - Eine Ausnahme von der obigen Regel ist, dass Sie auf der Seite „`data`“ Formeln erstellen können. Die Formeln der Seite „`data`“ ermöglichen das Erstellen von Diagrammen auf neuen Seiten.
  - Ein neues Tabellenblatt sollte nicht „Daten“ oder „Informationen“ heißen.
- Falls eine angepasste Excel-Datei vorhanden ist, befindet sich neben dem Menüpunkt **Reports** > **Upload Excel** ein Häkchen. Beim Herunterladen der Excel-Datei wird die Version mit den Anpassungen



verwendet.

Schritte

1. Die Standard-, benutzerdefinierte oder gespeicherte Ansicht, die Sie als Grundlage für Ihren Bericht verwenden möchten, öffnen.
2. Die Auswahl erfolgt über **Reports** > **Download Excel**.

3. Die Datei wird gespeichert. Die Datei befindet sich in Ihrem Download-Ordner.
4. Die gespeicherte Datei in Excel öffnen. Die Datei nicht an einen neuen Speicherort verschieben. Falls die Arbeit an einem anderen Speicherort erfolgt, die Datei vor dem Hochladen unter dem ursprünglichen Dateinamen wieder am ursprünglichen Speicherort speichern.
5. Die Datei kann mithilfe von Excel-Funktionen wie komplexen Sortierungen, mehrstufigen Filtern, Pivot-Tabellen oder Diagrammen angepasst werden. Weitere Informationen sind in der Microsoft® Excel-Dokumentation zu finden.
6. Die geänderte Datei wird unter **Berichte** > **Excel hochladen** ausgewählt. Die zuletzt heruntergeladene Datei wird vom selben Speicherort hochgeladen.
7. Sie können sich mithilfe der Funktion **Geplante Berichte** einen Testbericht senden.

Herunterladen von Berichten in Active IQ Unified Manager

Sie können Berichte herunterladen und die Daten als CSV-Datei (Comma-Separated Values), als Microsoft Excel-Datei (.XLSX) oder als PDF-Datei auf einem lokalen Laufwerk oder einem Netzlaufwerk speichern. CSV- und XLSX-Dateien lassen sich mit Tabellenkalkulationsprogrammen wie Microsoft Excel und PDF-Dateien mit Readern wie Adobe Acrobat öffnen.

Schritte

1. Mit der Schaltfläche **Reports** lässt sich der Bericht in einem der folgenden Formate herunterladen:

Auswählen	Zu…
CSV herunterladen	Sie können den Bericht als CSV-Datei (Comma-Separated Values) speichern.
PDF herunterladen	Bericht als .pdf-Datei speichern.
Excel Download	Sie können den Bericht als Microsoft Excel (XLSX)-Datei speichern.

Berichte planen

Planen von Berichten in Active IQ Unified Manager

Sobald Sie eine Ansicht haben, die Sie wiederverwenden und als Bericht teilen möchten, können Sie diese mit Active IQ Unified Manager planen. Sie können geplante Berichte managen und die Empfänger sowie die Verteilungshäufigkeit für jeden Berichtsplan ändern.

In Unified Manager können Sie die meisten Ansichten oder Inventarseiten planen. Ausgenommen sind Ereignisse, also Berichte, die Sie als CSV-Dateien herunterladen können, jedoch nicht zur erneuten Generierung und Freigabe planen können. Auch Dashboards, Favoriten oder Konfigurationsseiten können nicht heruntergeladen oder geplant werden.

Ab Active IQ Unified Manager 9.8 können Sie Ansichten im Microsoft® Excel-Format herunterladen und anpassen. Dabei sind erweiterte Excel-Funktionen wie komplexe Sortierungen, mehrstufige Filter, Pivot-Tabellen und Diagramme verfügbar. Wenn Sie mit dem resultierenden Excel-Bericht zufrieden sind, können Sie die Excel-Datei hochladen, damit sie bei jeder geplanten Freigabe des Berichts verwendet wird.

Sie können die integrierten Ansichten oder von Ihnen angepasste Ansichten planen. Sie können auswählen, welcher Dateityp gesendet werden soll: CSV, PDF oder XSLX. Wenn Sie einen Bericht zum ersten Mal planen, können Sie ihn herunterladen und sich selbst als einzigen Empfänger festlegen, damit Sie den Bericht so sehen, wie Ihre Empfänger ihn sehen werden.

Bericht planen

Ein Bericht in Active IQ Unified Manager kann geplant werden

Sobald Sie eine Ansicht oder eine Excel-Datei haben, die Sie regelmäßig generieren und verteilen möchten, können Sie den Bericht planen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Die SMTP Servereinstellungen müssen auf der Seite **Allgemein** > **Benachrichtigungen** konfiguriert worden sein, damit die Berichts-Engine Berichte als E-Mail-Anhänge an die Empfängerliste des Unified Manager Server senden kann.
- Der E-Mail-Server muss so konfiguriert sein, dass Anhänge mit den generierten E-Mails versendet werden können.

Mit den folgenden Schritten kann ein Bericht für eine Ansicht getestet und seine Erstellung geplant werden. Die zu verwendende Ansicht wird ausgewählt oder angepasst. Im folgenden Verfahren wird eine Netzwerkansicht verwendet, die die Performance Ihrer Netzwerkschnittstellen anzeigt, Sie können jedoch jede beliebige Ansicht verwenden.

Schritte

1. Öffnen der Ansicht. Dieses Beispiel verwendet die Standardnetzwerkansicht, die die LIF Performance anzeigt. Im linken Navigationsbereich auf **Network > Network Interfaces** klicken.
2. Bei Bedarf lässt sich die Ansicht mithilfe der integrierten Unified Manager Funktionen anpassen.
3. Nachdem Sie die Ansicht angepasst haben, können Sie im Feld **View** einen eindeutigen Namen eingeben und auf das Häkchen klicken, um sie zu speichern.



4. Sie können die erweiterten Funktionen von Microsoft® Excel nutzen, um Ihren Bericht anzupassen. Weitere Informationen finden Sie unter "Verwenden von Excel zum Anpassen Ihres Berichts".
5. Um die Ausgabe vor der Planung oder Freigabe anzuzeigen:

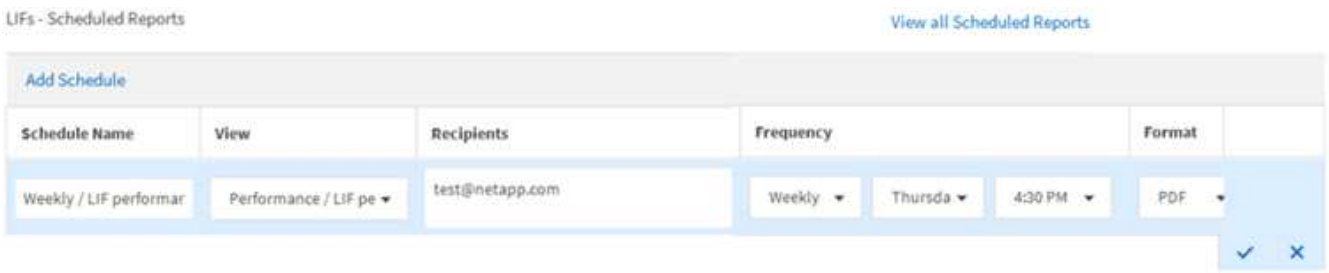
Option	Beschreibung
Wenn Sie Excel zur Anpassung des Berichts verwendet haben	Anzeige der bereits heruntergeladenen Excel-Datei.
Falls Sie Excel nicht zur Anpassung des Berichts verwendet haben	Der Bericht steht als **CSV**-, **PDF**- oder **XLSX**-Datei zum Download zur Verfügung.

Die Datei kann mit einer installierten Applikation wie Microsoft Excel (CSV/XSLX) oder Adobe Acrobat (PDF) geöffnet werden.

6. Wenn Sie mit dem Bericht zufrieden sind, erfolgt die Auswahl von **Scheduled Reports**.
7. Auf der Seite „Berichtszeitpläne“ erfolgt ein Klick auf **Zeitplan hinzufügen**.
8. Der Standardname, eine Kombination aus dem Ansichtsname und der Häufigkeit, kann übernommen oder der **Zeitplanname** angepasst werden.
9. Zum erstmaligen Testen des geplanten Berichts sollte zunächst nur die eigene Adresse als **Empfänger** hinzugefügt werden. Sobald alles passt, können die E-Mail-Adressen aller Berichtsempfänger hinzugefügt werden.
10. Sie geben an, wie häufig der Bericht erstellt und an die Empfänger gesendet werden soll. Sie können **täglich**, **wöchentlich** oder **monatlich** auswählen.
11. Zur Auswahl stehen die Formate **PDF**, **CSV** oder **XSLX**.

    Bei Berichten, deren Inhalt mit Excel angepasst wurde, ist immer **XSLX** zu wählen.

12. Zum Speichern des Berichtszeitplans ist das Häkchen (✓) auszuwählen.



Der Bericht wird sofort testweise versendet. Danach wird der Bericht generiert und mit der geplanten Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Importierte .rptdesign-Berichte in Active IQ Unified Manager planen

Bereits vorhandene Berichte, die in einer früheren Version von Unified Manager erstellt und importiert wurden, können geplant werden.

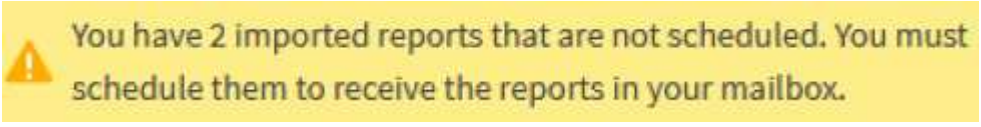
Für die Planung importierter Berichte ist Folgendes erforderlich:

- importierte, mit BIRT entworfene Berichte aus .rptdesign-Dateien in einer früheren Unified Manager Version
- gilt beim Upgrade auf Unified Manager 9.6 GA oder höher

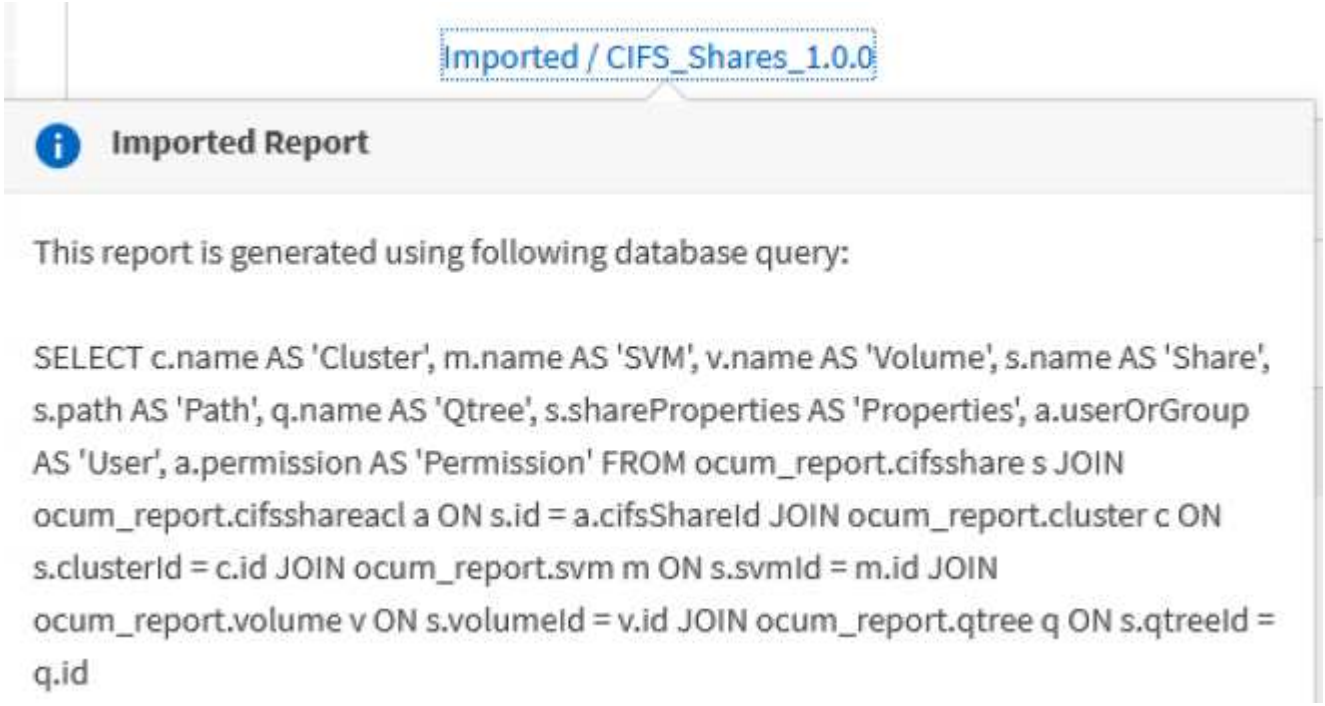
Nach dem Upgrade auf Unified Manager 9.6 GA oder höher werden die importierten Berichte auf der Seite „Berichtszeitpläne“ aufgelistet. Sie können den Zeitplan dieser Berichte bearbeiten, um die E-Mail-Adressen der Empfänger, die Häufigkeit und das Format (PDF oder CSV) festzulegen. Andernfalls können diese Berichte in der Unified Manager UI weder bearbeitet noch angezeigt werden.

Schritte

1. Die Seite „Berichtszeitpläne“ wird geöffnet. Wenn Sie Berichte importiert haben, erscheint eine Meldung.



2. Über den Namen der **Ansicht** lässt sich die SQL-Abfrage anzeigen, mit der der Bericht generiert wird.



3. Über das Symbol „Mehr“ ⋮ und **Bearbeiten** lassen sich die Details des Berichtszeitplans definieren und der Bericht speichern.

ⓘ Über das Symbol „Mehr“ ⋮ können Sie auch unerwünschte Berichte löschen.

Berichtszeitpläne managen

Verwaltung von Berichtsplänen in Active IQ Unified Manager

Sie können Ihre Berichtszeitpläne auf der Seite „Berichtszeitpläne“ managen. Dort können Sie bestehende Zeitpläne anzeigen, bearbeiten oder löschen.

ⓘ **Bevor Sie beginnen**

Auf der Seite „Berichtszeitpläne“ lassen sich keine neuen Berichte planen. Geplante Berichte lassen sich nur auf den Objektinventarseiten hinzufügen.

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich ist **Storage Management** > **Report Schedules** auszuwählen.
2. Auf der Seite „Berichtszeitpläne“:

Wenn Sie möchten…	Dann…
Vorhandenen Zeitplan anzeigen	Das Durchblättern der Liste der vorhandenen Berichte erfolgt mithilfe der Scrollleisten und Seitensteuerungen.

Wenn Sie möchten…	Dann…
Einen bestehenden Zeitplan bearbeiten	a. Für den gewünschten Zeitplan wählen Sie das Symbol „Mehr“ ⋮ aus. b. Klicken Sie auf **Bearbeiten**. c. Die notwendigen Änderungen sind vorzunehmen. d. Ihre Änderungen lassen sich durch Klicken auf das Häkchen speichern.
Löschen eines bestehenden Zeitplans	a. Für den gewünschten Zeitplan wählen Sie das Symbol „Mehr“ ⋮ aus. b. Klicken Sie auf **Delete**. c. Bestätigung Ihrer Entscheidung.

Geplante Berichte in Active IQ Unified Manager bearbeiten

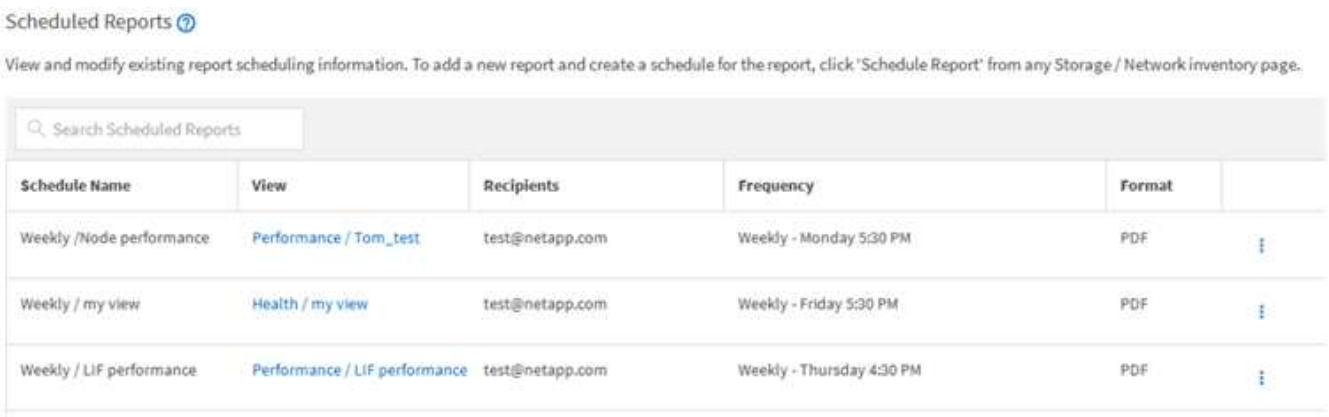
Nachdem Berichte geplant wurden, können Sie sie auf der Seite „Berichtstermine“ bearbeiten.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich ist **Storage Management** > **Report Schedules** auszuwählen.



Wenn Sie über die entsprechenden Berechtigungen verfügen, können Sie jeden Bericht und dessen Zeitplan im System ändern.

2. Zum Ändern des gewünschten Zeitplans ist das Symbol „Mehr ⋮ “ auszuwählen.
3. Klicken Sie auf **Bearbeiten**.
4. Sie können den **Zeitplannamen**, die **Empfängerliste**, die **Häufigkeit** und das **Format** für den Berichtszeitplan ändern.
5. Wenn Sie fertig sind, kann das Häkchen zum Speichern Ihrer Änderungen ausgewählt werden.

Geplante Berichte in Active IQ Unified Manager löschen

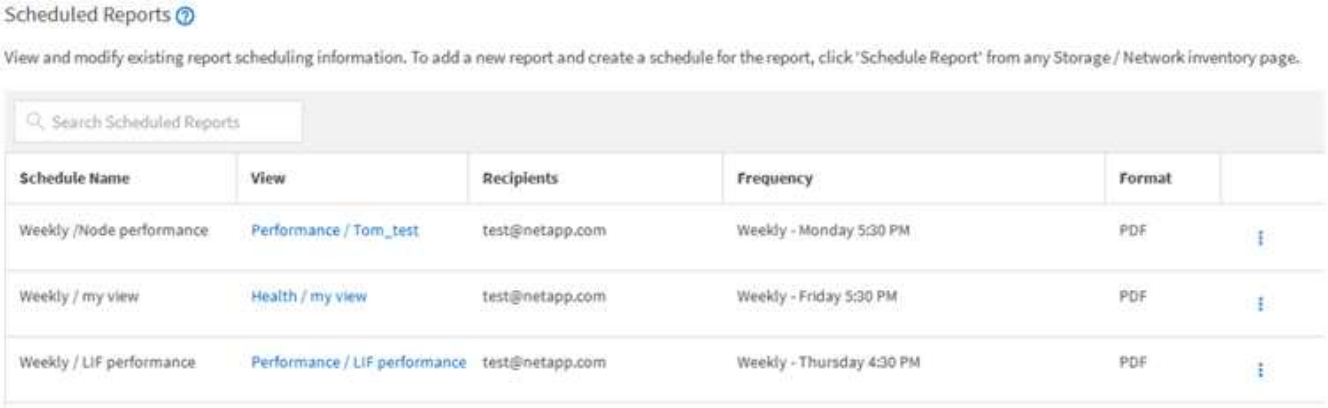
Nachdem Berichte terminiert wurden, können Sie sie auf der Seite „Report Schedules“ löschen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Schritte

1. Im linken Navigationsbereich ist **Storage Management** > **Report Schedules** auszuwählen.



> Wenn Sie über die entsprechenden Berechtigungen verfügen, können Sie jeden Bericht und dessen Zeitplan im System entfernen.

2. Zum Entfernen eines Zeitplans ist beim entsprechenden Zeitplan das Symbol „Mehr ⋮ “ zu wählen.
3. Klicken Sie auf **Delete**.
4. Bestätigung Ihrer Entscheidung.

   Der geplante Bericht wurde aus der Liste entfernt und wird nicht mehr nach dem festgelegten Zeitplan erstellt und verteilt.

> Wenn Sie eine benutzerdefinierte Ansicht von der Inventarseite löschen, werden auch alle benutzerdefinierten Excel-Dateien oder geplanten Berichte gelöscht, die diese Ansicht verwenden.

Beispielhafte benutzerdefinierte Berichte

Informationen zu beispielhaften benutzerdefinierten Berichten in Active IQ Unified Manager

Diese benutzerdefinierten Beispielberichte dienen häufig dazu, potenzielle Probleme zu erkennen und auf mögliche Schwierigkeiten zu reagieren, bevor Probleme auftreten.

Die Liste der Berichte in diesem Abschnitt ist nicht vollständig und wird im Laufe der Zeit erweitert. Sie können durch Feedback zur Dokumentation benutzerdefinierte Berichte vorschlagen, die diesem Abschnitt hinzugefügt werden sollen.

Zum Managen von Berichten ist die Rolle „Application Administrator“ oder „Storage Administrator“ erforderlich.

Anpassen von Cluster Storage Berichten

In Active IQ Unified Manager kann ein Bericht zur Anzeige der Kapazität nach Clustermodell erstellt werden.

Ein Bericht zur Analyse der Storage-Kapazität und -Auslastung von Clustern basierend auf dem Storage-Systemmodell kann erstellt werden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Im Folgenden finden Sie die Schritte zum Erstellen einer benutzerdefinierten Ansicht, die die Kapazität nach Clustermodell anzeigt, sowie zum anschließenden Planen der Berichterstellung für diese Ansicht.

Schritte

1. Im linken Navigationsbereich wird **Storage** > **Cluster** ausgewählt.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Kapazität** > **Alle Cluster**.
3. Mit **Anzeigen/Ausblenden** lassen sich Spalten wie “Cluster FQDN” und “OS Version” ausblenden, die im Bericht nicht benötigt werden.
4. Sinnvoll ist es, die Spalten „`Total Raw Capacity`“, „`Model/Family`“ und die drei Aggregatspalten in die Nähe der Spalte „`Cluster`“ zu ziehen.
5. Die Ergebnisse werden nach Clustertyp sortiert, wenn Sie auf den oberen Rand der Spalte „`Model/Family`“ klicken.
6. Die Ansicht sollte unter einem spezifischen Namen gespeichert werden, der widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel „`Kapazität nach Clustermodell`“.
7. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
8. Durch Klicken auf **Zeitplan hinzufügen** wird der Seite **Berichtszeitpläne** eine neue Zeile hinzugefügt, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
9. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht dargestellten Ergebnissen sollten Sie gegebenenfalls die Kapazität bestimmter Cluster erhöhen oder ältere Clustermodelle aufrüsten.

Cluster mit nicht zugewiesener LUN-Kapazität in Active IQ Unified Manager identifizieren

Sie können einen Bericht erstellen, um die Cluster mit der größten nicht zugewiesenen LUN-Kapazität von mehr als 0,5 TB zu finden und so festzustellen, wo Sie zusätzliche Workloads hinzufügen können.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mithilfe der folgenden Schritte lässt sich eine benutzerdefinierte Ansicht erstellen, die Cluster mit der größten nicht zugewiesenen LUN-Kapazität anzeigt; anschließend kann für diese Ansicht die Generierung eines Berichts geplant werden.

Schritte

1. Im linken Navigationsbereich wird **Storage** > **Cluster** ausgewählt.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Kapazität** > **Alle Cluster**.
3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Die Spalte “Unallocated LUN Capacity” nahe der Spalte “HA Pair” platzieren.
5. Nach dem Klick auf das Filtersymbol folgt das Hinzufügen des folgenden Filters und anschließend der Klick auf **Apply Filter**:
   - Nicht zugewiesene LUN-Kapazität größer als 0.5 TB
6. Am oberen Rand der Spalte „Nicht zugewiesene LUN-Kapazität“ lassen sich die Ergebnisse nach der größten Menge an nicht zugewiesener LUN-Kapazität sortieren.
7. Sie können die Ansicht unter einem spezifischen Namen speichern, der widerspiegelt, was die Ansicht anzeigt, z. B. „`Most unallocated LUN capacity`“, und auf das Häkchen (✓) klicken.
8. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
9. Über **Add Schedule** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
10. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Auf Grundlage der im Bericht dargestellten Ergebnisse kann es sinnvoll sein, die nicht zugewiesene LUN-Kapazität des Clusters zu nutzen.

Erstellen eines Berichts zum Anzeigen von HA-Paaren mit der höchsten verfügbaren Kapazität in Active IQ Unified Manager

Sie können einen Bericht erstellen, um die Hochverfügbarkeitspaare (HA) mit der größten Kapazität zur Provisionierung neuer Volumes und LUNs zu finden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mithilfe der folgenden Schritte wird eine benutzerdefinierte Ansicht erstellt, die HA-Paare nach der höchsten verfügbaren Kapazität zum Provisionieren neuer Volumes und LUNs sortiert anzeigt; anschließend wird die Erstellung eines Berichts für diese Ansicht geplant.

Schritte

1. Im linken Navigationsbereich wird **Storage** > **Cluster** ausgewählt.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Kapazität** > **Alle Cluster**.
3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Sie können die Spalte „`Aggregate Unused Capacity`“ nahe der Spalte „`HA Pair`“ platzieren.
5. Nach dem Klick auf das Filtersymbol folgt das Hinzufügen des folgenden Filters und anschließend der Klick

auf **Apply Filter**:

- Ungenutzte Aggregatkapazität größer als 0,5 TB

6. Die Ergebnisse lassen sich durch Klicken auf den oberen Rand der Spalte „`Ungenutzte Kapazität des Aggregats`“ nach der größten ungenutzten Aggregate-Kapazität sortieren.
7. Die Ansicht unter einem bestimmten Namen speichern, der widerspiegelt, was in der Ansicht angezeigt wird, z. B. „`Least used aggregate capacity`“, und auf das Häkchen (✓) klicken.
8. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
9. Über **Add Schedule** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
10. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht dargestellten Ergebnissen kann eine Ausbalancierung der HA Paare anhand der Aggregatkapazität sinnvoll sein.

Es kann ein Bericht erstellt werden, um Knoten anzuzeigen, auf denen ältere Versionen von ONTAP in Active IQ Unified Manager ausgeführt werden.

Sie können einen Bericht erstellen, der die auf allen Clusterknoten installierte Version der ONTAP Software anzeigt, damit Sie sehen können, welche Knoten aktualisiert werden sollten.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mithilfe der folgenden Schritte lässt sich eine benutzerdefinierte Ansicht erstellen, die Knoten mit älteren Versionen von ONTAP anzeigt; anschließend lässt sich die Generierung eines Berichts für diese Ansicht planen.

Schritte

1. Im linken Navigationsbereich können Sie **Storage** > **Nodes** auswählen.
2. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
3. Sie ziehen die Spalte „`OS Version`“ in die Nähe der Spalte „`Node`“.
4. Mit einem Klick auf den oberen Bereich der Spalte „`OS Version`“ lassen sich die Ergebnisse nach der ältesten Version von ONTAP sortieren.
5. Die Ansicht erhält einen spezifischen Namen, der widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel „`Knoten nach ONTAP Version`“.
6. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
7. Über **Add Schedule** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
8. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen

Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht dargestellten Ergebnissen sollten Sie möglicherweise Knoten aktualisieren, auf denen ältere Versionen von ONTAP ausgeführt werden.

Anpassen von Berichten zur Aggregatkapazität

Erstellung eines Berichts zum Anzeigen von Aggregaten, die in Active IQ Unified Manager ihre volle Kapazität erreichen

Sie können einen Bericht erstellen, um die Aggregate zu finden, die an ihre Kapazitätsgrenze stoßen, damit Sie zusätzliche Kapazität hinzufügen oder Workloads auf andere Aggregate verlagern können.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mithilfe der folgenden Schritte kann eine benutzerdefinierte Ansicht erstellt werden, die Aggregate anzeigt, die ihre volle Kapazität erreichen; anschließend kann die Generierung eines Berichts für diese Ansicht geplant werden.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Aggregates**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Kapazität** > **Alle Aggregate**.
3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Nach dem Klick auf das Filtersymbol folgt das Hinzufügen des folgenden Filters und anschließend der Klick auf **Apply Filter**:
   - Weniger als 45 Tage bis zur vollständigen Befüllung
5. Durch Klicken auf den oberen Bereich der Spalte “Days to Full” werden die Ergebnisse nach der geringsten Anzahl verbleibender Tage bis zum Erreichen der vollen Kapazität sortiert.
6. Die Ansicht wird unter einem spezifischen Namen gespeichert, der widerspiegelt, was die Ansicht anzeigt, z. B. „`Tage bis zur vollen Aggregatkapazität`“, anschließend wird auf das Häkchen (✓) geklickt.
7. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
8. Durch Klicken auf **Zeitplan hinzufügen** wird der Seite **Berichtszeitpläne** eine neue Zeile hinzugefügt, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
9. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht angezeigten Ergebnisse kann es sinnvoll sein, den Storage auf Aggregaten zu erhöhen, die ihre volle Kapazität erreichen. Zusätzlich kann es sinnvoll sein, den Schwellenwert für Tage bis zur vollständigen Kapazität auf mehr als die standardmäßigen 7 Tage zu erhöhen, damit Ereignisse empfangen werden, die mehr Zeit für eine Reaktion bieten, wenn der freie Speicherplatz auf Aggregaten knapp wird.

In Active IQ Unified Manager lässt sich ein Bericht erstellen, um Aggregate anzuzeigen, die zu 80 % oder mehr gefüllt sind

Sie können einen Bericht erstellen, um die Aggregate hervorzuheben, die zu 80 % oder mehr gefüllt sind.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten wird eine benutzerdefinierte Ansicht erstellt, in der Aggregate angezeigt werden, die zu 80 % oder mehr belegt sind; anschließend wird die Generierung eines Berichts für diese Ansicht geplant.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Aggregates**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Kapazität** > **Alle Aggregate**.
3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Die Spalten „`Available Data %`“ und „`Used Data %`“ sollten in die Nähe der Spalte „`Aggregate`“ gezogen werden.
5. Nach dem Klicken auf das Filtersymbol können die folgenden Filter hinzugefügt und anschließend **Filter anwenden** ausgewählt werden:
   - Der Anteil der genutzten Daten liegt über 80 %
6. Mit einem Klick auf den oberen Rand der Spalte „`Used Data %`“ lassen sich die Ergebnisse nach Kapazitätsprozent sortieren.
7. Die Ansicht kann unter einem bestimmten Namen gespeichert werden, der widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel „`Aggregate fast voll`“, und anschließend kann auf das Häkchen (✓) .
8. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
9. Über **Add Schedule** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
10. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht dargestellten Ergebnissen sollten Sie möglicherweise einige Daten aus bestimmten Aggregaten verschieben.

Es kann ein Bericht erstellt werden, um in Active IQ Unified Manager überbelegte Aggregate anzuzeigen.

Sie können einen Bericht erstellen, um die Storage-Kapazität und die Nutzung von Aggregaten zu analysieren und Aggregaten anzuzeigen, die überbelegt sind.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten wird eine benutzerdefinierte Ansicht erstellt, die Aggregate anzeigt, die den

Schwellenwert für Überbelegung überschreiten; anschließend wird die Generierung eines Berichts für diese Ansicht geplant.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Aggregates**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Kapazität** > **Alle Aggregate**.
3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Die Spalte „`Overcommitted Capacity %`“ ist in der Nähe der Spalte „`Aggregate`“ zu platzieren.
5. Nach dem Klicken auf das Filtersymbol können die folgenden Filter hinzugefügt und anschließend **Filter anwenden** ausgewählt werden:
   - Überbelegte Kapazität % ist größer als 100 %
6. Durch Klicken auf den oberen Bereich der Spalte „`Overcommitted Capacity %`“ werden die Ergebnisse nach Kapazitätsprozentsatz sortiert.
7. Die Ansicht erhält einen spezifischen Namen, der widerspiegelt, was in der Ansicht angezeigt wird, z. B. „`Aggregates overcommitted`“; anschließend folgt ein Klick auf das Häkchen (✓).
8. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
9. Über **Add Schedule** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
10. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht dargestellten Ergebnissen sollten Sie möglicherweise die Kapazität der Aggregate erhöhen oder einige Daten aus bestimmten Aggregaten verschieben.

Volumenkapazitätsberichte anpassen

Volumes mit nahezu ausgeschöpfter Kapazität und deaktivierter Snapshot Autodelete in Active IQ Unified Manager

Sie können einen Bericht erstellen, der die Liste der Volumes enthält, die sich ihrer vollen Kapazität nähern, während die Funktion Snapshot Autodelete deaktiviert ist. Die Ergebnisse können Ihnen helfen, Volumes zu identifizieren, für die Sie die Funktion Snapshot Autodelete möglicherweise konfigurieren möchten.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Im Folgenden wird beschrieben, wie eine benutzerdefinierte Ansicht erstellt wird, die die erforderlichen Spalten in der richtigen Reihenfolge anzeigt, und wie anschließend die Generierung eines Berichts für diese Ansicht geplant wird.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Kapazität** > **Alle Volumes**.

3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Die Spalten „`Snapshot Autodelete`“ und „`Days To Full`“ lassen sich per Drag-and-Drop in die Nähe der Spalte „`Available Data Capacity`“ ziehen.
5. Nach einem Klick auf das Filtersymbol werden die folgenden beiden Filter hinzugefügt und anschließend **Filter anwenden** ausgewählt:
   - Weniger als 30 Tage bis voll
   - Automatisches Löschen von Snapshots ist deaktiviert
6. Durch Auswählen des oberen Bereichs der Spalte **Tage bis voll** erscheinen die Volumes mit den wenigsten verbleibenden Tagen oben in der Liste.
7. Speichern Sie die Ansicht unter einem bestimmten Namen, der den Inhalt der Ansicht widerspiegelt, z. B. “Vols near capacity”.
8. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
9. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht dargestellten Ergebnissen könnte es sinnvoll sein, auf den Volumes Snapshot Autodelete zu aktivieren oder eine Möglichkeit zu finden, den verfügbaren Speicherplatz zu erhöhen.

Volumes mit deaktiviertem Thin Provisioning in Active IQ Unified Manager identifizieren

Wenn ein Volume nicht per Thin Provisioning bereitgestellt wird, belegt es den gesamten Speicherplatz auf der Festplatte, der bei der Erstellung des Volumes festgelegt wurde. Die Identifizierung von Volumes, bei denen Thin Provisioning deaktiviert ist, hilft Ihnen bei der Entscheidung, ob Sie Thin Provisioning für bestimmte Volumes aktivieren möchten.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Im Folgenden wird beschrieben, wie eine benutzerdefinierte Ansicht erstellt wird, die die erforderlichen Spalten in der richtigen Reihenfolge anzeigt, und wie anschließend die Generierung eines Berichts für diese Ansicht geplant wird.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Kapazität** > **Alle Volumes**.
3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Ziehen Sie die Spalten „`Used Data %`“ und „`Thin Provisioned`“ per Drag-and-Drop neben die Spalte „`Available Data Capacity`“.
5. Auf das Filtersymbol klicken, den folgenden Filter hinzufügen, **Thin provisioned** ist **No**, und dann **Apply Filter** auswählen.
6. Durch Klicken auf den oberen Bereich der Spalte „`Verwendete Daten %`“ werden die Ergebnisse so sortiert, dass die Volumes mit dem höchsten Prozentsatz oben in der Liste erscheinen.
7. Die Ansicht sollte unter einem Namen gespeichert werden, der widerspiegelt, was in der Ansicht angezeigt

wird, zum Beispiel “Vols no thin provisioning”.

8. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
9. Mit **Add Schedule** lässt sich der Seite **Report Schedules** eine neue Zeile hinzufügen, sodass die Zeitplaneigenschaften für den neuen Bericht definiert werden können.
10. Für den Berichtsplan wird ein Name eingegeben und die anderen Berichtsfelder werden ausgefüllt. Anschließend ist auf das Häkchen (✓) am Ende der Zeile zu klicken.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht dargestellten Ergebnissen kann es sinnvoll sein, Thin Provisioning auf bestimmten Volumes zu aktivieren.

Ermittlung von Volumes, die Daten in die Cloud-Ebene in Active IQ Unified Manager verschieben sollten

Sie können einen Bericht erstellen, der die Liste der Volumes enthält, die sich aktuell auf FabricPool Aggregaten befinden, die eine Cloud-Empfehlung vom Typ Tier haben und die eine große Menge an kalten Daten enthalten. Dieser Bericht kann Sie bei der Entscheidung unterstützen, ob die Tiering-Richtlinie für bestimmte Volumes in “auto” oder “all” geändert werden sollte, um mehr kalte (inaktive) Daten in die Cloud-Ebene auszulagern.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.
- Sie müssen FabricPool Aggregate konfiguriert haben und Volumes auf diesen Aggregaten besitzen.

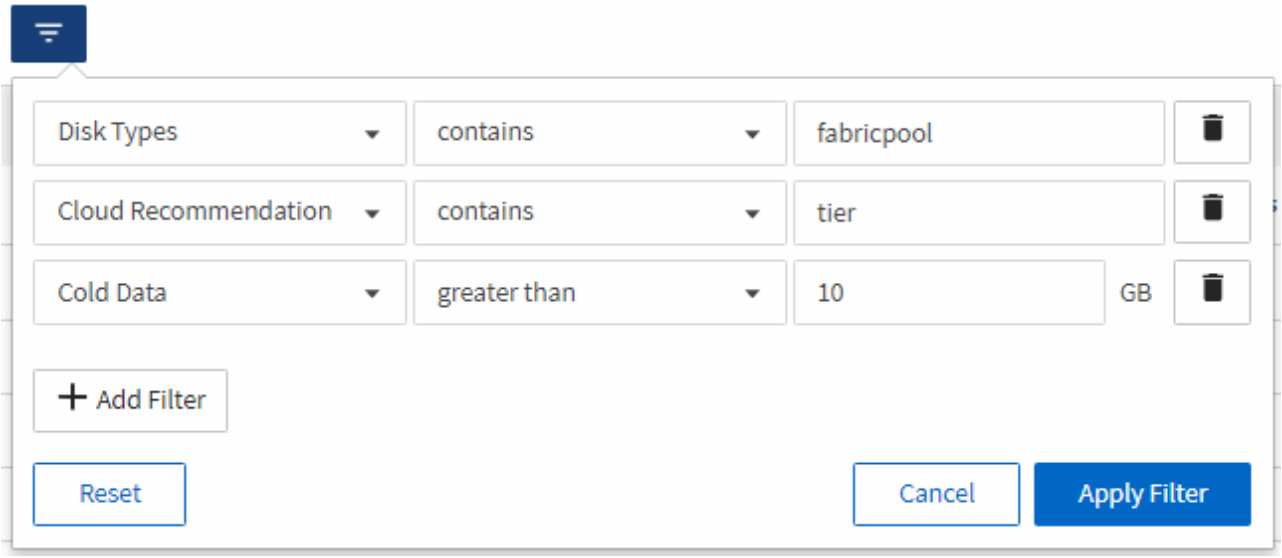
Im Folgenden wird beschrieben, wie eine benutzerdefinierte Ansicht erstellt wird, die die erforderlichen Spalten in der richtigen Reihenfolge anzeigt, und wie anschließend die Generierung eines Berichts für diese Ansicht geplant wird.

Schritte

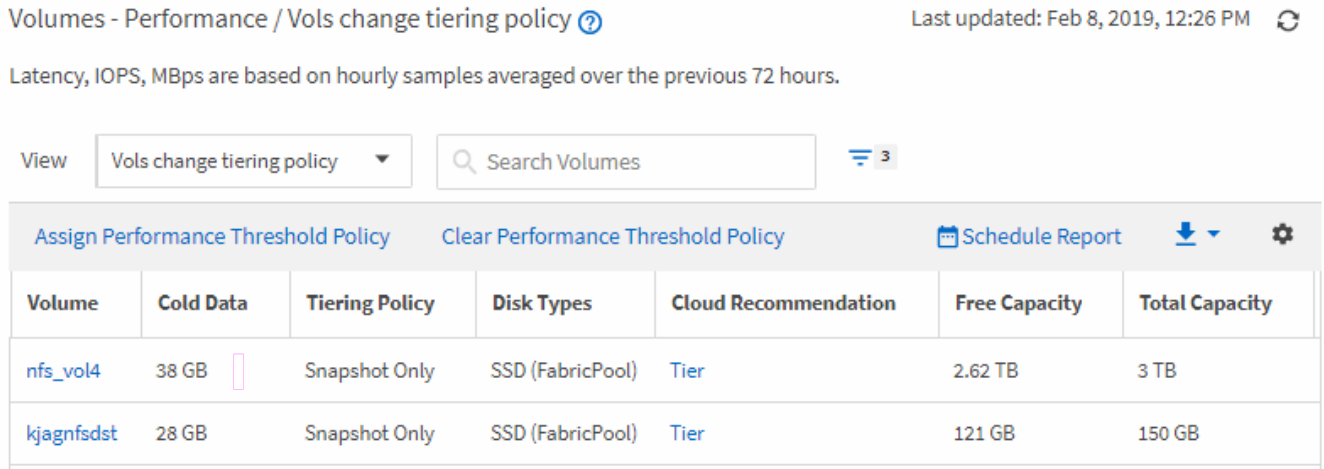
1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Performance** > **Alle Volumes**.
3. Im Spaltenauswahldialog muss die Spalte „`Disk Type`“ in der Ansicht erscheinen.

   Durch das Hinzufügen oder Entfernen weiterer Spalten lässt sich eine für Ihren Bericht wichtige Ansicht erstellen.

4. Die Spalte „`Disk Type`“ lässt sich per Drag & Drop in die Nähe der Spalte „`Cloud Recommendation`“ ziehen.
5. Nach dem Klicken auf das Filtersymbol die folgenden drei Filter hinzufügen und anschließend **Filter anwenden** auswählen:
   - Der Datenträgertyp enthält FabricPool
   - Cloud Recommendation enthält Tier
   - Kalte Daten größer als 10 GB



6. Durch Auswahl des oberen Bereichs der Spalte „Kalte Daten“ erscheinen die Volumes mit den meisten kalten Daten oben in der Ansicht.
7. Die Ansicht sollte unter einem Namen gespeichert werden, der widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel “Vols change tiering policy”.



8. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
9. Über **Add Schedule** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
10. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht dargestellten Ergebnissen kann es sinnvoll sein, mit System Manager oder der ONTAP CLI die Tiering-Richtlinie für bestimmte Volumes in “auto” oder “all” zu ändern, um mehr selten genutzte Daten in das Cloud Tier auszulagern.

Anpassen von Qtree Kapazitätsberichten

Erstellung eines Berichts zum Anzeigen von qtrees, die in Active IQ Unified Manager nahezu voll sind

Es kann ein Bericht erstellt werden, um die Storage-Kapazität und Auslastung von qtrees zu analysieren und qtrees anzuzeigen, die nahezu voll sind.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten lässt sich eine benutzerdefinierte Ansicht erstellen, in der nahezu volle qtrees angezeigt werden; anschließend lässt sich die Generierung eines Berichts für diese Ansicht planen.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Qtrees**.
2. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
3. Die Spalte “Disk Used %” neben der Spalte “Qtrees” platzieren.
4. Nach dem Klicken auf das Filtersymbol können die folgenden Filter hinzugefügt und anschließend **Filter anwenden** ausgewählt werden:
   - Die Festplattenauslastung beträgt mehr als 75%
5. Die Ergebnisse lassen sich durch Klicken auf den oberen Bereich der Spalte „`Disk Used %`“ nach Kapazitätsprozent sortieren.
6. Für die Ansicht wird ein spezifischer Name verwendet, der den angezeigten Inhalt widerspiegelt, z. B. “Qtrees fast voll”, danach folgt ein Klick auf das Häkchen (✓).
7. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
8. Mit **Add Schedule** lässt sich der Seite **Report Schedules** eine neue Zeile hinzufügen, sodass die Zeitplaneigenschaften für den neuen Bericht definiert werden können.
9. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht gezeigten Ergebnissen sollten Sie gegebenenfalls die Festplatten-Hard- und Soft-Limits anpassen, sofern diese festgelegt sind, oder die Daten auf die qtrees verteilen.

NFS-Freigabeberichte anpassen

Anpassen von NFS-Freigabeberichten in Active IQ Unified Manager

Sie können NFS-Freigabeberichte anpassen, um Informationen zu NFS-Exportrichtlinien und -regeln für Volumes auf Ihren Storage Systemen zu analysieren. Beispielsweise können Sie Berichte so anpassen, dass Volumes mit nicht zugänglichen Mountpfaden und Volumes mit der Standardexportrichtlinie angezeigt werden.

Ein Bericht zum Anzeigen von Volumes mit einem nicht zugänglichen Mount-Pfad in Active IQ Unified Manager

Sie können einen Bericht erstellen, um Volumes zu finden, deren Mount-Pfad nicht zugänglich ist.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die folgenden Schritte dienen dazu, eine benutzerdefinierte Ansicht für Volumes mit einem nicht zugänglichen Mountpfad zu erstellen und anschließend einen Bericht für diese Ansicht zu planen.

Schritte

1. Die Auswahl erfolgt im linken Navigationsbereich über **Storage** > **NFS Shares**.
2. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
3. Nach dem Klick auf das Filtersymbol folgt das Hinzufügen des folgenden Filters und anschließend der Klick auf **Apply Filter**:
   - Mount Path Active ist Nein
4. Die Ansicht wird unter einem bestimmten Namen gespeichert, der widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel „`Volumes with an inaccessible mount path`“, und anschließend wird auf das Häkchen (✓) geklickt.
5. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
6. Über **Zeitplan hinzufügen** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
7. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Auf Grundlage der im Bericht angezeigten Ergebnisse kann eine Korrektur der nicht zugänglichen Mount-Pfade sinnvoll sein.

Ein Bericht zum Anzeigen von Volumes mithilfe der Standard-Exportrichtlinie in Active IQ Unified Manager

Sie können einen Bericht erstellen, um Volumes zu finden, die die Standardexportrichtlinie verwenden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mithilfe der folgenden Schritte kann eine benutzerdefinierte Ansicht für Volumes erstellt werden, die die Standardexportrichtlinie verwenden; anschließend kann die Generierung eines Berichts für diese Ansicht geplant werden.

Schritte

1. Die Auswahl erfolgt im linken Navigationsbereich über **Storage** > **NFS Shares**.
2. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
3. Die Spalte “Export Policy” in die Nähe der Spalte “Volume” ziehen.
4. Nach dem Klick auf das Filtersymbol folgt das Hinzufügen des folgenden Filters und anschließend der Klick auf **Apply Filter**:
   - Export Policy enthält Standardwerte
5. Die Ansicht wird unter einem bestimmten Namen gespeichert, der widerspiegelt, was in der Ansicht

angezeigt wird, z. B. „`Volumes mit einer Standardexportrichtlinie`“, und danach wird auf das Häkchen (✓) geklickt.

6. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
7. Über **Zeitplan hinzufügen** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
8. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Auf Grundlage der im Bericht angezeigten Ergebnisse kann die Konfiguration einer benutzerdefinierten Exportrichtlinie sinnvoll sein.

Anpassung von Storage VM Berichten

Anpassen von Berichten zu Speicher-VMs in Active IQ Unified Manager

Sie können Berichte zu Storage VMs erstellen, um Volume-Informationen zu analysieren und den allgemeinen Systemstatus sowie die Storage-Verfügbarkeit anzuzeigen. Beispielsweise können Sie Berichte erstellen, um SVMs anzuzeigen, die die maximale Volume-Anzahl erreichen, und um gestoppte SVMs zu analysieren.

Erstellen eines Berichts zur Anzeige von Speicher-VMs, die in Active IQ Unified Manager die maximale Volume-Grenze erreichen

Sie können einen Bericht erstellen, um SVMs zu finden, die das maximale Volume-Limit erreichen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mithilfe der folgenden Schritte können Sie eine benutzerdefinierte Ansicht erstellen, die Storage VMs anzeigt, die das maximale Volume-Limit erreichen, und anschließend die Erstellung eines Berichts für diese Ansicht planen.

Schritte

1. Die Auswahl erfolgt im linken Navigationsbereich über **Storage** > **Storage VMs**.
2. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
3. Die Spalten „`Volume Count`“ und „`Maximum Allowed Volumes`“ in der Nähe der Spalte „`Storage VM`“ anordnen.
4. Wenn Sie auf den oberen Bereich der Spalte „`Maximum Allowed Volumes`“ klicken, werden die Ergebnisse nach der höchsten Anzahl von Volumes sortiert.
5. Die Ansicht unter einem spezifischen Namen speichern, der widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel „`SVMs reaching max volumes`“, und auf das Häkchen (✓) klicken.
6. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
7. Durch Klicken auf **Zeitplan hinzufügen** wird der Seite **Berichtszeitpläne** eine neue Zeile hinzugefügt, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.

8. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht dargestellten Ergebnissen kann es sinnvoll sein, die den Storage VMs zugewiesenen Volumes auszubalancieren oder, falls möglich, ONTAP System Manager zum Ändern der maximal zulässigen Volumes zu verwenden.

Ein Bericht zum Anzeigen gestoppter Speicher-VMs im Active IQ Unified Manager

Sie können einen Bericht erstellen, der eine Liste aller gestoppten SVMs anzeigt.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Im Folgenden werden die Schritte zum Erstellen einer benutzerdefinierten Ansicht beschrieben, in der angehaltene Storage VMs angezeigt werden; anschließend wird die Generierung eines Berichts für diese Ansicht geplant.

Schritte

1. Die Auswahl erfolgt im linken Navigationsbereich über **Storage** > **Storage VMs**.
2. Im Menü „View“ erfolgt die Auswahl von **Health** > **All Storage VMs**.
3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Die Spalte „`State`“ wird in die Nähe der Spalte „`Storage VM`“ gezogen.
5. Nach dem Klick auf das Filtersymbol folgt das Hinzufügen des folgenden Filters und anschließend der Klick auf **Apply Filter**:
   - Der Zustand ist angehalten
6. Die Ansicht unter einem spezifischen Namen speichern, der widerspiegelt, was in der Ansicht angezeigt wird, z. B. „`Stopped SVMs`“, und auf das Häkchen (✓) klicken.
7. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
8. Durch Klicken auf **Zeitplan hinzufügen** wird der Seite **Berichtszeitpläne** eine neue Zeile hinzugefügt, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
9. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht angezeigten Ergebnisse lässt sich prüfen, warum die SVM angehalten ist und ob die angehaltenen SVMs neu gestartet werden sollten.

Berichte zu Volume-Beziehungen anpassen

Anpassen von Volume-Beziehungsberichten in Active IQ Unified Manager

Der Bericht Volume Relationships Inventory ermöglicht Ihnen, die Details des Storage-Inventars in einem Cluster zu analysieren, den für Volumes erforderlichen Schutzgrad zu

verstehen und die Volume-Details nach Fehlerquelle, Muster und Zeitplänen zu filtern.

Erstellung eines Berichts zur Gruppierung von Volume-Beziehungen nach Fehlerursache in Active IQ Unified Manager

Es kann ein Bericht erstellt werden, der Volumes nach dem Grund gruppiert, aus dem sich die Beziehung in einem fehlerhaften Zustand befindet.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten können Sie eine benutzerdefinierte Ansicht erstellen, die Volumes nach Fehlerursache gruppiert, und anschließend die Erstellung eines Berichts für diese Ansicht planen.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Beziehung** > **Alle Beziehungen**.
3. Mit **Show/Hide** lässt sich sicherstellen, dass die Spalten „`Relationship Health`“ und „`Unhealthy Reason`“ in der Ansicht erscheinen.

   Durch das Hinzufügen oder Entfernen weiterer Spalten lässt sich eine für Ihren Bericht wichtige Ansicht erstellen.

4. Die Spalten „`Systemstatus der Beziehung`“ und „`Grund für den fehlerhaften Zustand`“ lassen sich in die Nähe der Spalte „`Status`“ ziehen.
5. Nach dem Klick auf das Filtersymbol folgt das Hinzufügen des folgenden Filters und anschließend der Klick auf **Apply Filter**:
   - Der Systemstatus der Beziehung ist schlecht
6. Mit einem Klick auf den oberen Bereich der Spalte „`Unhealthy Reason`“ lässt sich die Gruppierung der Volume-Beziehungen nach Fehlerquelle vornehmen.
7. Für die Ansicht empfiehlt sich ein spezifischer Name, der widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel “Vol Beziehungen nach Ausfall”.
8. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
9. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✔) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht dargestellten Ergebnisse können Sie die Ursache und die Auswirkungen der einzelnen Fehlertypen untersuchen.

Erstellung eines Berichts zum Gruppieren von Volume-Beziehungen nach Problem in Active IQ Unified Manager

Sie können einen Bericht erstellen, der Volume-Beziehungen nach Problem gruppiert.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten lässt sich eine benutzerdefinierte Ansicht erstellen, die Volume-Beziehungen nach Problem gruppiert; anschließend lässt sich die Generierung eines Berichts für diese Ansicht planen.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Beziehung** > **Alle Beziehungen**.
3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Die Spalte „`Unhealthy Reason`“ wird in die Nähe der Spalte „`State`“ gezogen.
5. Durch Klicken auf den oberen Bereich der Spalte „`Unhealthy Reason`“ können Sie die Volumes nach Problem gruppieren.
6. Speichern Sie die Ansicht unter einem bestimmten Namen, der den Inhalt der Ansicht widerspiegelt, z. B. “Vol relationships by issue”.
7. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
8. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht dargestellten Ergebnisse können Sie die Quelle und die Auswirkungen der einzelnen Problemtypen untersuchen.

Erstellung eines Berichts zum Anzeigen von Trends beim Volumentransfer in bestimmten Zeitabständen in Active IQ Unified Manager

Sie können einen Bericht erstellen, der Volume-Transfertrends in bestimmten Zeitintervallen anzeigt.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten lässt sich eine benutzerdefinierte Ansicht für Volumes in bestimmten Zeitintervallen erstellen und anschließend ein Bericht für diese Ansicht generieren.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Beziehung** > **Transferstatus des letzten Monats**.
3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Ziehen Sie die Spalte „Transfer Duration“ neben die Spalte „`Operational Result`“.
5. Nach dem Klick auf das Filtersymbol folgt das Hinzufügen des folgenden Filters und anschließend der Klick auf **Apply Filter**:
   - Endzeit der Übertragung in den letzten 7 Tagen
6. Über den oberen Rand der Spalte “Übertragungsdauer” lassen sich die Volumes nach Zeitintervall sortieren.
7. Für die Ansicht wird ein bestimmter Name verwendet, der widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel „`Volumes by duration`“.

8. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
9. Für den Berichtsplan wird ein Name eingegeben, die Häufigkeit auf **Wöchentlich** festgelegt und die anderen Berichtsfelder werden ausgefüllt; anschließend wird auf das Häkchen (✓) am Ende der Zeile geklickt.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht dargestellten Ergebnisse können Sie die Übertragungszeitintervalle untersuchen.

Ein Bericht zur Anzeige fehlgeschlagener oder erfolgreicher Volume-Übertragungen in Active IQ Unified Manager

Sie können einen Bericht erstellen, der den Status von Volume-Übertragungen anzeigt. In diesem Bericht können Sie sowohl fehlgeschlagene als auch erfolgreiche Volume-Übertragungen einsehen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten wird eine benutzerdefinierte Ansicht erstellt, die anzeigt, welche Übertragungen fehlgeschlagen sind und welche erfolgreich waren; anschließend wird die Generierung eines Berichts für diese Ansicht geplant.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Beziehung** > **Transferstatus des letzten Monats**.
3. Mit **Anzeigen/Ausblenden** können Sie alle Spalten ausblenden, die Sie im Bericht nicht benötigen.
4. Positionieren der Spalte “Operation Result” in der Nähe der Spalte “State”.
5. Mit einem Klick auf den oberen Bereich der Spalte “Operation Result” lassen sich die Volumes nach dem Status sortieren.
6. Als Name für die Ansicht eignet sich ein spezifischer Name, der widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel „`Volumes by transfer status`“.
7. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
8. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht dargestellten Ergebnisse können Sie den Transferstatus überprüfen.

Ein Bericht zum Anzeigen von Volume-Übertragungen basierend auf der Übertragungsgröße in Active IQ Unified Manager

Sie können einen Bericht erstellen, um Volume-Transfers basierend auf der Transfergröße anzuzeigen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten lässt sich eine benutzerdefinierte Ansicht für Volume-Übertragungen basierend auf der Übertragungsgröße erstellen und anschließend ein Bericht für diese Ansicht generieren.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ ist **Beziehung** > **Übertragungsrate des letzten Monats** auszuwählen.
3. Über den oberen Rand der Spalte „`Total Transfer Size`“ lassen sich die Volume-Übertragungen nach Größe sortieren.
4. Für die Ansicht sollte ein spezifischer Name verwendet werden, der widerspiegelt, was in der Ansicht angezeigt wird, zum Beispiel „`Volumes by transfer size`“.
5. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
6. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht dargestellten Ergebnisse können Sie die Volume-Beziehungen nach Übertragungsgröße untersuchen.

Ein Bericht zur Anzeige von nach Tag gruppierten Volume-Übertragungen in Active IQ Unified Manager

Sie können einen Bericht erstellen, um die Volume-Übertragungen nach Tag gruppiert anzuzeigen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Im Folgenden wird beschrieben, wie eine benutzerdefinierte Ansicht für nach Tagen gruppierte Volume-Übertragungen erstellt und anschließend ein Bericht für diese Ansicht generiert wird.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ ist **Beziehung** > **Übertragungsrate des letzten Monats** auszuwählen.
3. Ein Klick auf den oberen Rand der Spalte „`Day`“ sortiert die Volume-Übertragungen nach Tag.
4. Die Ansicht kann unter einem spezifischen Namen gespeichert werden, der widerspiegelt, was die Ansicht anzeigt, zum Beispiel „`Volume-Transfers pro Tag`“.
5. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
6. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht dargestellten Ergebnisse können Sie die Volume-Übertragungen pro Tag untersuchen.

Anpassung von Performanceberichten für Volumes

Erstellung eines Berichts zur Identifizierung von Volumes mit hohem Anteil an kalten Daten auf einem nicht-FabricPool Aggregat in Active IQ Unified Manager

Es kann ein Bericht erstellt werden, der Volumes mit einem hohen Anteil an kalten Daten auf einem nicht FabricPool Aggregat anzeigt. Dadurch lassen sich Volumes identifizieren, die auf ein FabricPool Aggregat verschoben werden sollten.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Die folgenden Schritte dienen zum Erstellen einer benutzerdefinierten Ansicht für Volumes mit einer großen Menge an kalten Daten auf einem nicht für FabricPool aktivierten Aggregat und zum anschließenden Planen der Berichtserstellung für diese Ansicht.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Im Menü „Ansicht“ erfolgt die Auswahl von **Performance** > **Alle Volumes**.
3. Über **Anzeigen/Ausblenden** können Sie sicherstellen, dass die Spalte “Disk Type” in der Ansicht angezeigt wird.

   Durch das Hinzufügen oder Entfernen weiterer Spalten lässt sich eine für Ihren Bericht wichtige Ansicht erstellen.

4. Die Spalte „`Disk Type`“ wird in der Nähe der Spalte „`Cold Data`“ platziert.
5. Nach dem Klick auf das Filtersymbol folgt das Hinzufügen des folgenden Filters und anschließend der Klick auf **Apply Filter**:
   - Kalte Daten größer als 100 GB
   - Der Datenträgertyp enthält SSD
6. Am oberen Rand der Spalte „`Disk Type`“ erfolgt die Sortierung der Volumes nach Datenträgertyp, sodass der Datenträgertyp SSD (FabricPool) ganz unten steht.
7. Für die Ansicht eignet sich ein spezifischer Name, der widerspiegelt, was sie anzeigt, zum Beispiel “Kalte Datenvolumina nicht FabricPool”.
8. Auf der Inventarseite die Schaltfläche **Geplante Berichte** auswählen.
9. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

   Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht dargestellten Ergebnisse lassen sich Volumes ermitteln, die sich gut für eine Verschiebung auf FabricPool Aggregate eignen.

Beispielberichte in Microsoft Excel

Beispielberichte in Microsoft Excel in Active IQ Unified Manager verstehen

Diese Beispielberichte in Microsoft Excel dienen als Einführung in die Berichtsoptionen, die mit den erweiterten Funktionen von Excel verfügbar sind.

Die erweiterten Funktionen von Excel ermöglichen die Erstellung vielfältiger, auf Ihre Bedürfnisse zugeschnittener Berichte. Ausführliche Informationen zur Verwendung von Excel finden Sie in der Produktdokumentation.

Zum Managen von Berichten ist die Rolle „Application Administrator“ oder „Storage Administrator“ erforderlich.

Es kann ein Bericht erstellt werden, der eine Tabelle und ein Diagramm der aggregierten Kapazität in Active IQ Unified Manager anzeigt.

Sie können einen Bericht zur Kapazitätsanalyse in einer Excel-Datei erstellen, indem Sie Summen und das Format eines gruppierten Säulendiagramms verwenden.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten können Sie eine Ansicht „Health: All Aggregates“ öffnen, die Ansicht in Excel herunterladen, ein Diagramm der verfügbaren Kapazität erstellen, die angepasste Excel-Datei hochladen und den Abschlussbericht planen.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Aggregates**.
2. Die Auswahl erfolgt über **Reports** > **Download Excel**.



   Je nach Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.

3. Falls erforderlich, kann auf **Bearbeitung aktivieren** geklickt werden.
4. Die heruntergeladene Datei lässt sich in Excel öffnen.
5. Ein neues Tabellenblatt (⊕) nach dem `data` Tabellenblatt erstellen und **Total Data Capacity** nennen.
6. Dem neuen Tabellenblatt „Gesamtdatenkapazität“ sind die folgenden Spalten hinzuzufügen:

a. Gesamte Datenkapazität (GB)

b. Zugesicherte Kapazität (GB)

c. Verwendete Datenkapazität (GB)

d. Verfügbare Datenkapazität (GB)

7. In die erste Zeile jeder Spalte wird die folgende Formel eingegeben; dabei ist darauf zu achten, dass sie auf das Datenblatt (data!) verweist und die korrekten Spalten- und Zeilenspezifizierer für die erfassten Daten verwendet (Total Data Capacity bezieht Daten aus Spalte E, Zeilen 2 bis 20).

a. =SUM(data!E$2:data!E$20)

b. =SUM(data!F$2:data!F$50)

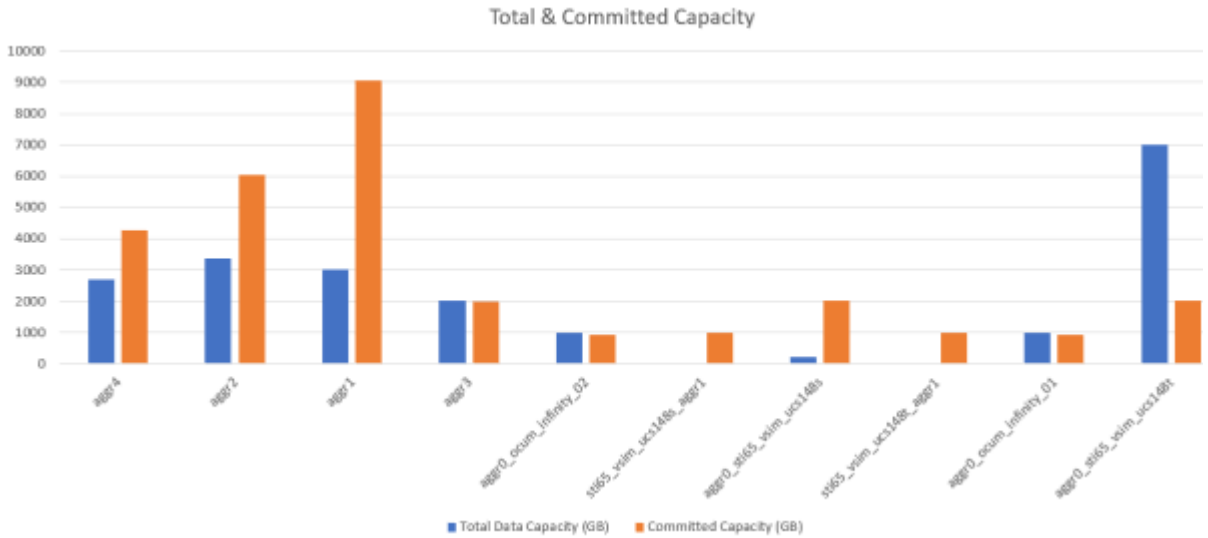
c. =SUM(data!G$2:data!G$50)

d. =SUM(data!H$2:data!H$50)

Die Formel summiert jede Spalte auf Basis der aktuellen Daten.

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. Im Datenblatt erfolgt die Auswahl der Spalten **Gesamtdatenkapazität (GB)** und **Zugesicherte Kapazität (GB)**.
2. Die Auswahl erfolgt im Menü **Einfügen** über **Empfohlene Diagramme** und anschließend über das Diagramm **Gruppierte Säulen**.
3. Mit einem Rechtsklick auf das Diagramm und der Auswahl von **Diagramm verschieben** lässt sich das Diagramm auf das `Total Data Capacity`Tabellenblatt verschieben.
4. Über die Menüs **Design** und **Format**, die bei ausgewähltem Diagramm verfügbar sind, können Sie das Aussehen des Diagramms anpassen.
5. Wenn Sie zufrieden sind, können Sie die Datei mit Ihren Änderungen speichern. Dateiname und Speicherort sind unverändert zu lassen.



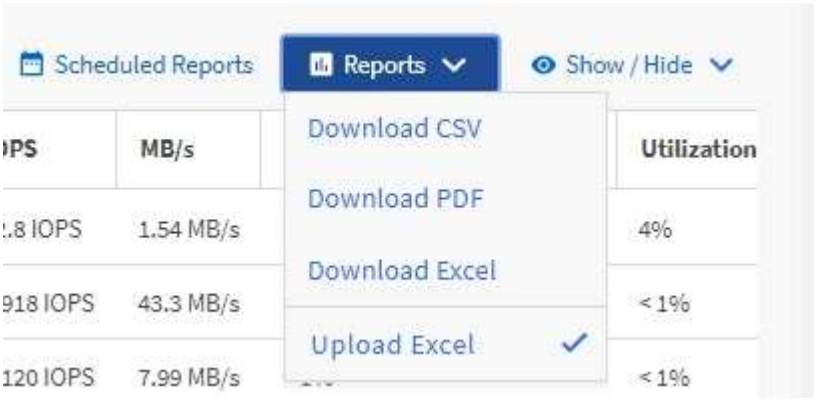
6. In Unified Manager befindet sich die Option unter **Reports** > **Upload Excel**.

Wichtig ist, dass Sie sich in derselben Ansicht befinden, in der Sie die Excel-Datei

heruntergeladen haben.

7. Auszuwählen ist die Excel-Datei, die Sie geändert haben.
8. Auf **Öffnen** klicken.
9. Anschließend **Absenden** auswählen.

   Neben dem Menüpunkt **Reports** > **Upload Excel** erscheint ein Häkchen.



10. Anschließend erfolgt die Auswahl von **Scheduled Reports**.
11. Über **Add Schedule** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.

    Für den Bericht ist das **XLSX** Format auszuwählen.

12. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Auf Grundlage der im Bericht dargestellten Ergebnisse kann es sinnvoll sein zu untersuchen, wie sich die verfügbare Kapazität in Ihrem Netzwerk optimal nutzen lässt.

Diagramme zur gesamten und verfügbaren Kapazität von Aggregaten in Active IQ Unified Manager

Für die Analyse der gesamten und zugesagten Storage-Kapazität in einem Excel-Diagrammformat lässt sich ein Bericht erstellen.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten lässt sich eine Ansicht „Gesundheit: Alle Aggregate“ öffnen, die Ansicht in Excel herunterladen, ein Diagramm für die Gesamt- und die zugesagte Kapazität erstellen, die angepasste Excel-Datei hochladen und der Abschlussbericht planen.

Schritte

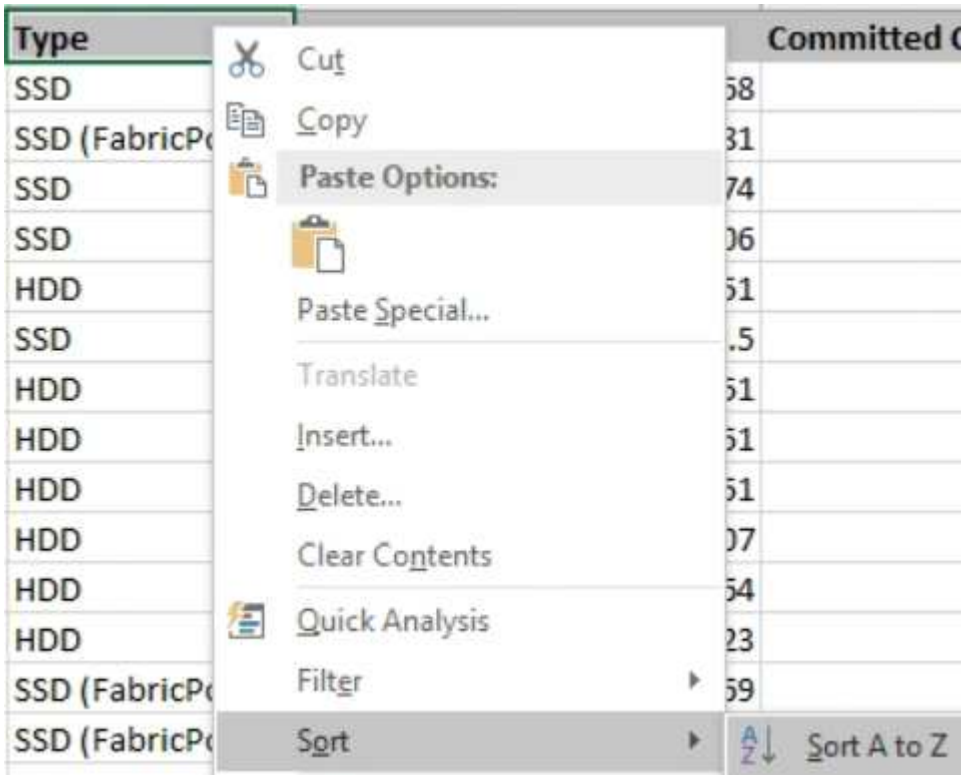
1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Aggregates**.

2. Die Auswahl erfolgt über **Reports** > **Download Excel**.



   Je nach Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.

3. Die heruntergeladene Datei lässt sich in Excel öffnen.
4. Falls erforderlich, kann auf **Bearbeitung aktivieren** geklickt werden.
5. Im Datenblatt können Sie mit der rechten Maustaste auf die Spalte „Typ“ klicken und **Sortieren** > **Sortieren A bis Z** auswählen.



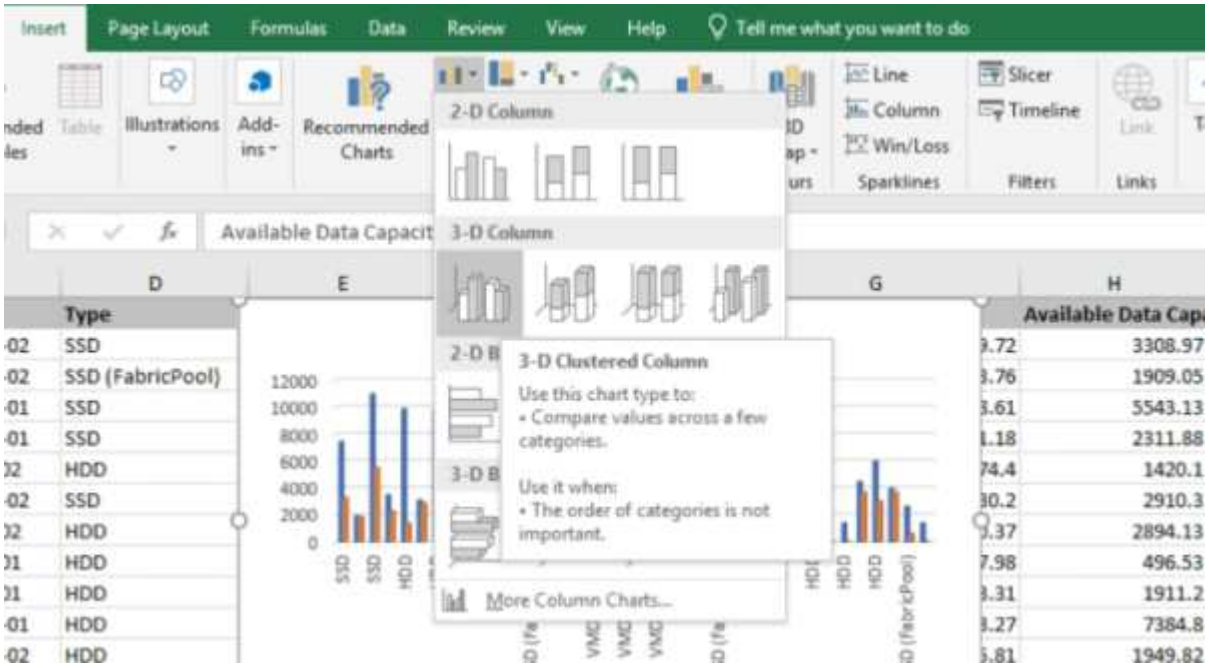
   Dadurch werden Ihre Daten nach Speichertyp sortiert, zum Beispiel:

   - HDD
   - Hybrid
   - SSD

◦ SSD (FabricPool)

6. Auswahl der Spalten `Type, Total Data Capacity,` und `Available Data Capacity`.
7. Im Menü **Einfügen** erfolgt die Auswahl eines `3-D column`Diagramms.

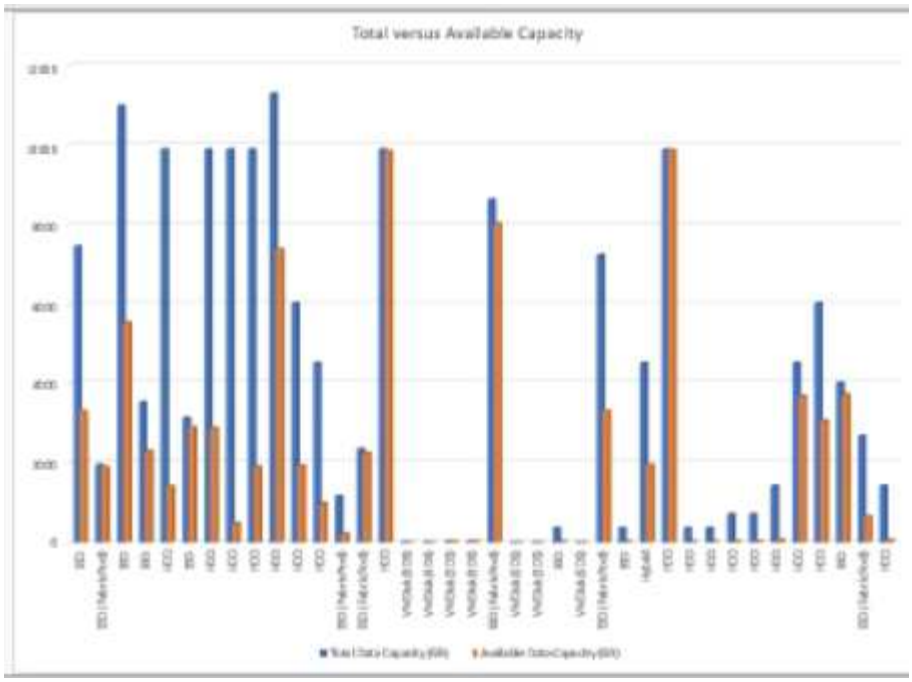
   Das Diagramm erscheint im Datenblatt.



8. Nach einem Rechtsklick auf das Diagramm steht die Option **Diagramm verschieben** zur Auswahl.
9. **New sheet** auswählen und das Blatt **Total Storage Charts** benennen.

   Das neue Tabellenblatt sollte nach den Informations- und Datenblättern erscheinen.

10. Als Diagrammtitel wird **Gesamtkapazität versus verfügbare Kapazität** verwendet.
11. Über die Menüs **Design** und **Format**, die bei ausgewähltem Diagramm verfügbar sind, können Sie das Aussehen des Diagramms anpassen.
12. Wenn Sie zufrieden sind, können Sie die Datei mit Ihren Änderungen speichern. Dateiname und Speicherort sind unverändert zu lassen.

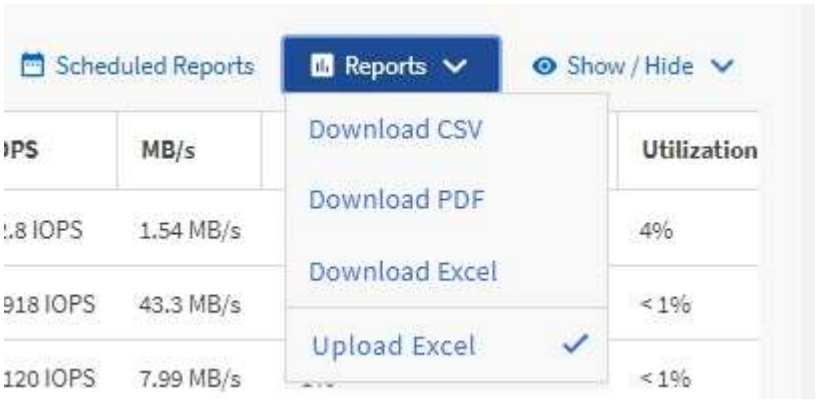


13. In Unified Manager befindet sich die Option unter **Reports** > **Upload Excel**.

> Wichtig ist, dass Sie sich in derselben Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

14. Auszuwählen ist die Excel-Datei, die Sie geändert haben.
15. Auf **Öffnen** klicken.
16. Anschließend **Absenden** auswählen.

    Neben dem Menüpunkt **Reports** > **Upload Excel** erscheint ein Häkchen.



17. Anschließend erfolgt die Auswahl von **Scheduled Reports**.
18. Durch Klicken auf **Zeitplan hinzufügen** wird der Seite **Berichtszeitpläne** eine neue Zeile hinzugefügt, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.

> Für den Bericht ist das **XLSX** Format auszuwählen.

19. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Auf Grundlage der im Bericht dargestellten Ergebnisse kann es sinnvoll sein, die Last auf Ihre Aggregate auszugleichen.

Es kann ein Bericht erstellt werden, um die verfügbaren Volumenkapazitätsdiagramme in Active IQ Unified Manager anzuzeigen.

Sie können einen Bericht erstellen, um die verfügbare Volumenkapazität in einem Excel-Diagramm zu analysieren.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten lässt sich eine Ansicht „Health: All Volumes“ öffnen, die Ansicht in Excel herunterladen, ein Diagramm zur verfügbaren Kapazität erstellen, die angepasste Excel-Datei hochladen und der Abschlussbericht planen.

Schritte

1. Auswahl im linken Navigationsbereich: **Storage** > **Volumes**.
2. Die Auswahl erfolgt über **Reports** > **Download Excel**.



   Je nach Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.

3. Falls erforderlich, kann auf **Bearbeitung aktivieren** geklickt werden.
4. Die heruntergeladene Datei lässt sich in Excel öffnen.
5. Auf dem `data` Blatt können Sie die Daten auswählen, die in den `Volume` und `Available Data` %-Spalten verwendet werden.
6. Im Menü **Einfügen** erfolgt die Auswahl einer Option `3-D piechart`.

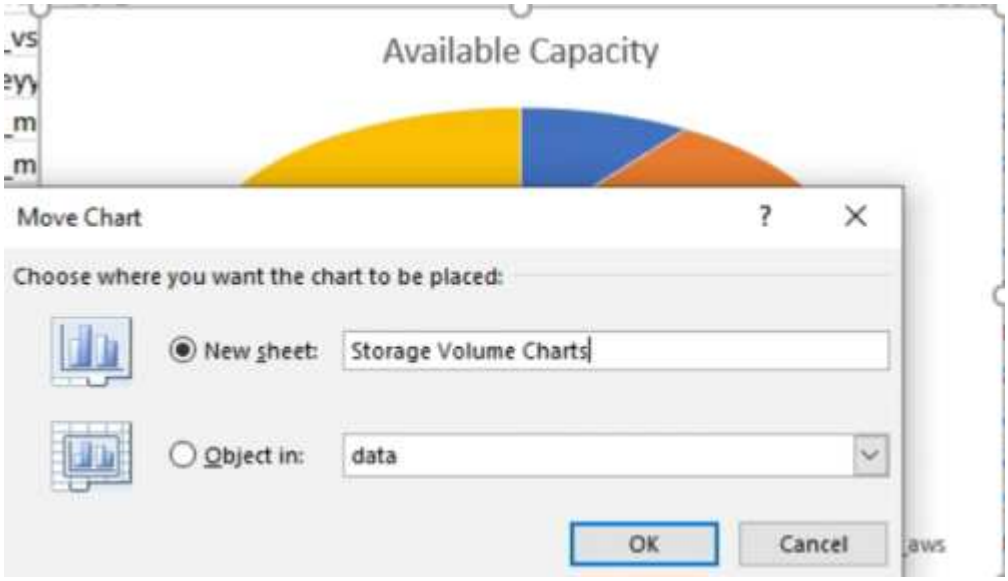
   Das Diagramm zeigt, welche Volumes über den größten verfügbaren Speicherplatz verfügen. Das Diagramm erscheint im Datenblatt.

   Je nach Netzwerkkonfiguration kann die Auswahl ganzer Spalten oder zu vieler Datenzeilen dazu führen, dass Ihr Kreisdiagramm unlesbar wird. Dieses Beispiel verwendet ein 3D-Kreisdiagramm, Sie können jedoch jeden beliebigen Diagrammtyp verwenden. Verwenden

Sie das Diagramm, das die zu erfassenden Daten am besten darstellt.

7. Als Diagrammtitel wird **Available Capacity** verwendet.
8. Nach einem Rechtsklick auf das Diagramm steht die Option **Diagramm verschieben** zur Auswahl.
9. Auszuwählen ist **New sheet**; das Blatt erhält den Namen **Storage Volume Charts**.

Das neue Tabellenblatt sollte nach den Informations- und Datenblättern erscheinen.

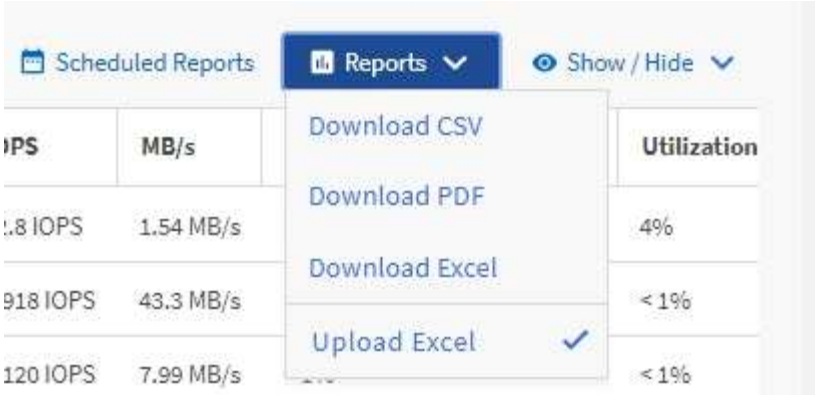


10. Über die Menüs **Design** und **Format**, die bei ausgewähltem Diagramm verfügbar sind, können Sie das Aussehen des Diagramms anpassen.
11. Wenn Sie zufrieden sind, können Sie die Datei mit Ihren Änderungen speichern.
12. In Unified Manager befindet sich die Option unter **Reports** > **Upload Excel**.

Wichtig ist, dass Sie sich in derselben Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

13. Auszuwählen ist die Excel-Datei, die Sie geändert haben.
14. Auf **Öffnen** klicken.
15. Anschließend **Absenden** auswählen.

Neben dem Menüpunkt **Reports** > **Upload Excel** erscheint ein Häkchen.



16. Anschließend erfolgt die Auswahl von **Scheduled Reports**.
17. Durch Klicken auf **Zeitplan hinzufügen** wird der Seite **Berichtszeitpläne** eine neue Zeile hinzugefügt, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
18. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

    Für den Bericht ist das **XLSX** Format auszuwählen.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht dargestellten Ergebnissen sollten Sie möglicherweise die Lastverteilung auf Ihre Volumes optimieren.

Ein Bericht zum Anzeigen von Aggregaten mit den meisten verfügbaren IOPS in Active IQ Unified Manager

Dieser Bericht zeigt, welche Aggregate pro Aggregattyp über die meisten verfügbaren IOPS verfügen und auf denen Sie neue Workloads provisionieren können.

Bevor Sie beginnen

- Die Rolle Application Administrator oder Storage Administrator ist erforderlich.

Mit den folgenden Schritten lässt sich eine Ansicht „Health: All Volumes“ öffnen, die Ansicht in Excel herunterladen, ein Diagramm zur verfügbaren Kapazität erstellen, die angepasste Excel-Datei hochladen und der Abschlussbericht planen.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Storage** > **Aggregates**.
2. Die Auswahl der Option **Performance: Alle Aggregate** erfolgt im Dropdown-Menü **Ansicht**.
3. Mit **Anzeigen/Ausblenden** werden die `Available IOPS` Spalte angezeigt und die `Cluster FQDN`, `Inactive Data Reporting`, und `Threshold Policy` Spalten ausgeblendet.
4. Die `Available IOPS`- und `Free Capacity`-Spalten lassen sich per Drag-and-drop neben der `Type` -Spalte platzieren.
5. Benutzerdefinierte Ansicht benennen und speichern `Available IOPS Per Aggr.`
6. Die Auswahl erfolgt über **Reports** > **Download Excel**.



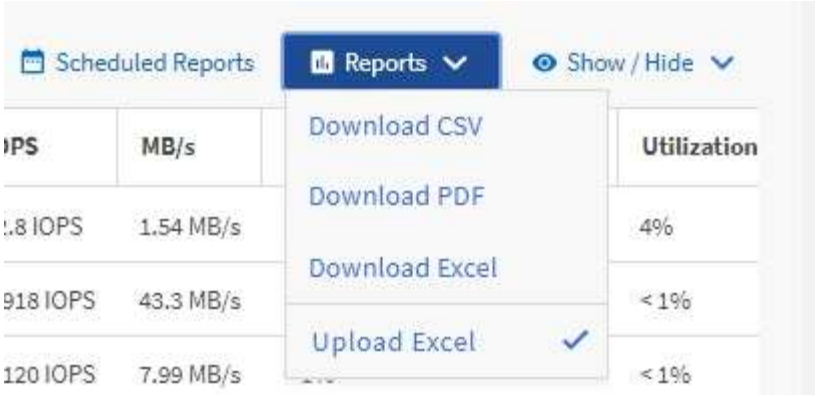
Je nach Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.

7. Falls erforderlich, kann auf **Bearbeitung aktivieren** geklickt werden.
8. Die heruntergeladene Datei lässt sich in Excel öffnen.
9. Im Datenblatt lässt sich durch Klicken auf das kleine Dreieck oben links im Blatt das gesamte Blatt auswählen.
10. Im Menüband **Daten** die Option **Sortieren** aus dem `Sort & Filter area.`
11. Folgende Sortierebenen sind festzulegen:
    a. Für **Sortieren nach** ist `Available IOPS` (IOPS), für **Sortieren auf** ist `Cell Values,` und für **Reihenfolge** ist `Largest to Smallest.` auszuwählen.
    b. Im nächsten Schritt erfolgt die Auswahl von **Ebene hinzufügen**.
    c. Für **Sortieren nach** ist `Type`, für **Sortieren auf** `Cell Values,` und für **Reihenfolge** `Z to A.` festzulegen.
    d. Im nächsten Schritt erfolgt die Auswahl von **Ebene hinzufügen**.
    e. Für **Sortieren nach** `Free Capacity (GB),`, für **Sortierkriterium** `Cell Values,` und für **Reihenfolge** `Largest to Smallest.` festlegen
    f. Klicken Sie auf **OK**.
12. Die Excel-Datei anschließend speichern und schließen.
13. In Unified Manager befindet sich die Option unter **Reports** > **Upload Excel**.

> Wichtig ist, dass Sie sich in derselben Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

14. Die geänderte Excel-Datei wird ausgewählt, in diesem Fall `performance-aggregates-<date>.xlsx.`
15. Auf **Öffnen** klicken.
16. Anschließend **Absenden** auswählen.

Neben dem Menüpunkt **Reports** > **Upload Excel** erscheint ein Häkchen.



17. Anschließend erfolgt die Auswahl von **Scheduled Reports**.
18. Über **Add Schedule** lässt sich der Seite „Berichtszeitpläne“ eine neue Zeile hinzufügen, sodass die Zeitplanmerkmale für den neuen Bericht definiert werden können.
19. Sie geben einen Namen für den Berichtsplan ein, füllen die anderen Berichtsfelder aus und klicken dann auf das Häkchen (✓) am Ende der Zeile.

    Für den Bericht ist das **XLSX** Format auszuwählen.

    Der Bericht wird sofort als Test gesendet. Danach wird der Bericht generiert und mit der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Auf Grundlage der im Bericht dargestellten Ergebnisse kann es sinnvoll sein, neue Workloads auf den Aggregaten mit den meisten verfügbaren IOPS zu provisionieren.

Storage mithilfe von REST APIs verwalten

Erste Schritte mit Active IQ Unified Manager

Erste Schritte mit Active IQ Unified Manager REST APIs

Active IQ Unified Manager bietet eine Reihe von APIs zum Managen Ihrer Storage Ressourcen auf den unterstützten Storage Systemen über eine RESTful-Webservice-Schnittstelle für beliebige Drittanbieterintegrationen.

In diesen Abschnitten finden Sie Informationen zu den Unified Manager APIs, Beispiel-Workflows zur Behebung spezifischer Probleme sowie Beispielcode. Mithilfe dieser Informationen können Sie RESTful-Clients von NetApp Manageability-Softwarelösungen für das Management von NetApp Systemen erstellen. Die APIs basieren auf dem Architekturstil Representational State Transfer (REST). Alle vier REST-Operationen Create, Read, Update und Delete, auch als CRUD bezeichnet, werden unterstützt.

Zusätzliche Ressourcen und Details zu den Vorteilen der Active IQ Unified Manager REST API finden Sie unter "Active IQ Unified Manager".

Vorgesehene Benutzer der Active IQ Unified Manager REST APIs

Die hier behandelten Themen richten sich an Entwickler, die Applikationen erstellen, die über REST-APIs mit der Active IQ Unified Manager Software interagieren.

Storage Administratoren und -Architekten können diese Informationen nutzen, um ein grundlegendes Verständnis dafür zu erlangen, wie die Unified Manager REST APIs zum Erstellen von Client Applikationen für das Managen und Überwachen von NetApp Storage Systemen verwendet werden können.

Diese Informationen sind relevant, wenn Sie den Storage-Provider, ONTAP cluster und Management-Administrations-APIs zum Managen Ihres Storage verwenden möchten.

Sie müssen über eine der folgenden Rollen verfügen: Operator, Storage Administrator oder Application Administrator. Sie müssen die IP-Adresse oder die vollqualifizierte Domain des Unified Manager Servers kennen, auf dem Sie die REST APIs ausführen möchten.

API-Zugriff und Kategorien in Active IQ Unified Manager verwalten

Mit den Active IQ Unified Manager APIs können Sie Storage-Objekte in Ihrer Umgebung managen und provisionieren. Einige dieser Funktionen sind auch über die Unified Manager Web-UI zugänglich.

Eine URL für den direkten Zugriff auf REST-APIs erstellen

Sie können über eine Programmiersprache wie Python, C#, C++++, JavaScript usw. direkt auf die REST APIs zugreifen. Für den Zugriff auf die REST APIs werden der Hostname oder die IP-Adresse und die URL im folgenden Format eingegeben

https://<hostname>/api

Der Standardport ist 443. Sie können den Port entsprechend Ihrer Umgebung konfigurieren.

Zugriff auf die Online-API-Dokumentationsseite

Sie können die mit dem Produkt bereitgestellte Referenzinhaltsseite *API Documentation* aufrufen, um die API-Dokumentation anzuzeigen und einen API-Aufruf manuell auszuführen, beispielsweise über die Schnittstelle Swagger. Der Zugriff auf diese Dokumentation erfolgt über **Menu Bar** > **Help button** > **API Documentation**.

Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL für den Zugriff auf die REST API-Seite im folgenden Format eingeben

https://<hostname>/docs/api/

Kategorien

Die API-Aufrufe sind funktional nach Bereichen oder Kategorien organisiert. Eine bestimmte API lässt sich über die entsprechende API-Kategorie auffinden.

Die mit Unified Manager bereitgestellten REST-APIs unterstützen Sie bei administrativen, Überwachungs- und Provisionierungsfunktionen. Die APIs sind in folgende Kategorien unterteilt.

- **Datacenter**

  Diese Kategorie umfasst die APIs, die Sie bei der Storage-Verwaltung und -Analyse im Datacenter mithilfe von Tools wie Work Flow Automation und Ansible unterstützen. Die REST-APIs dieser Kategorie liefern Informationen über Cluster, Knoten, Aggregate, Volumes, LUNs, Dateifreigaben, Namespaces und andere Elemente in Ihrem Datacenter.

- **Management-Server**

  Die APIs in der Kategorie **management-server** umfassen die `jobs, system,` und `events` APIs. Jobs sind Operationen, die für die asynchrone Ausführung geplant sind und mit dem Managen von Storage Objekten oder Workloads in Unified Manager zusammenhängen. Die `events` API gibt Ereignisse in Ihrem Datacenter zurück, und die `system` API gibt die Details der Unified Manager Instanz zurück.

- **storage-provider**

  Diese Kategorie enthält alle APIs für die Provisionierung, die für das Managen und die Provisionierung von Dateifreigaben, LUNs, Performance Service Levels und Storage-Effizienzrichtlinien erforderlich sind. Die APIs ermöglichen außerdem die Konfiguration von Zugriffsendpunkten und Active Directories sowie die Zuweisung von Performance Service Levels und Storage-Effizienzrichtlinien zu Storage-Workloads.

- **Verwaltung**

  Diese Kategorie enthält die APIs, die für die Ausführung administrativer Aufgaben verwendet werden, z. B. für die Pflege der Sicherungseinstellungen, das Anzeigen von Truststore-Zertifikaten für die Unified Manager Datenquellen und das Managen von ONTAP Clustern als Datenquellen für Unified Manager.

- **Gateway**

  Unified Manager ermöglicht es Ihnen, ONTAP REST-APIs über die APIs in der Gateway-Kategorie aufzurufen und die Storage Objekte in Ihrem Datacenter zu managen.

- **Sicherheit**

  Diese Kategorie enthält APIs zum Managen von Unified Manager Benutzern.

REST Services verstehen, die in Active IQ Unified Manager angeboten werden

Sie sollten sich mit den angebotenen REST Services und Operationen vertraut machen, bevor Sie die Active IQ Unified Manager APIs verwenden.

Die Provisionierungs- und Verwaltungs-APIs, die zur Konfiguration des API-Servers verwendet werden, unterstützen Lese- (GET) oder Schreibvorgänge (POST, PATCH, DELETE). Im Folgenden sind einige Beispiele für die von den APIs unterstützten GET-, PATCH-, POST- und DELETE-Operationen aufgeführt:

- Beispiel für GET: `GET /datacenter/cluster/clusters` ruft Clusterdetails in Ihrem Datacenter ab. Die maximale Anzahl der Datensätze, die von der `GET` Operation zurückgegeben wird, beträgt 1000.

> Die APIs ermöglichen Ihnen, die Datensätze nach unterstützten Attributen zu filtern, zu sortieren und zu ordnen.

- Beispiel für POST: `POST /datacenter/svm/svms` erstellt eine benutzerdefinierte Storage Virtual Machine (SVM).
- Beispiel für PATCH: `PATCH /datacenter/svm/svms/{key}` ändert die Eigenschaften einer SVM mithilfe ihres eindeutigen Schlüssels.
- Beispiel für DELETE: `DELETE /storage-provider/access-endpoints/{key}` löscht einen Zugriffsendpunkt von einer LUN, SVM oder Dateifreigabe mithilfe seines eindeutigen Schlüssels.

Die mit den APIs ausführbaren REST-Operationen hängen von der Rolle des Benutzers Operator, Storage Administrator oder Application Administrator ab.

Benutzerrolle	Unterstützte REST-Methode
Operator	Schreibgeschützter Zugriff auf die Daten. Benutzer mit dieser Rolle können alle GET-Anfragen ausführen.
Storage-Administrator	Lesezugriff auf alle Daten. Benutzer mit dieser Rolle können alle GET-Anfragen ausführen. Darüber hinaus verfügen sie über Schreibzugriff (zum Ausführen von PATCH-, POST- und DELETE-Anfragen), um bestimmte Aktivitäten auszuführen, z. B. das Managen von Storage Service Objekten und Storage Management Optionen.
Anwendungsadministrator	Lese- und Schreibzugriff auf alle Daten. Benutzer mit dieser Rolle können GET-, PATCH-, POST- und DELETE-Anfragen für alle Funktionen ausführen.

Weitere Informationen zu allen REST-Operationen enthält die *Online API Dokumentation*.

API-Versionsnummern in Active IQ Unified Manager verstehen

Die REST-API-URIs in Active IQ Unified Manager enthalten eine Versionsnummer. Zum Beispiel `/v2/datacenter/svm/svms`. Die Versionsnummer `v2` in `/v2/datacenter/svm/svms` gibt die in einer bestimmten Version verwendete API-Version an. Die Versionsnummer minimiert die Auswirkungen von API-Änderungen auf die Client-Software, indem eine Antwort zurückgegeben wird, die der Client verarbeiten

kann.

Der numerische Teil dieser Versionsnummer wird im Verhältnis zu Releases fortlaufend erhöht. URIs mit einer Versionsnummer bieten eine konsistente Schnittstelle, die in zukünftigen Releases die Abwärtskompatibilität beibehält. Dieselben APIs finden Sie auch ohne Versionsangabe, zum Beispiel `/datacenter/svm/svms`, die die Basis-APIs ohne Version kennzeichnen. Die Basis-APIs sind immer die neueste Version der APIs.

> In der oberen rechten Ecke Ihrer Swagger-Oberfläche können Sie die zu verwendende API-Version auswählen. Standardmäßig ist die höchste Version ausgewählt. Es wird empfohlen, die höchste verfügbare Version der jeweiligen API (bezogen auf die fortlaufende Versionsnummer) in Ihrer Unified Manager-Instanz zu verwenden.

Bei allen Anfragen ist die gewünschte API-Version explizit anzugeben. Wenn die Versionsnummer angegeben ist, liefert der Dienst keine Antwortelemente zurück, die Ihre Applikation nicht verarbeiten kann. In REST-Anfragen sollte der Versionsparameter angegeben werden. Ältere Versionen der APIs werden nach einigen Releases schließlich als veraltet markiert. In diesem Release ist die `v1`Version der APIs veraltet.

Verständnis des ONTAP Speicherressourcenmodells in Active IQ Unified Manager

Die Storage Ressourcen in ONTAP lassen sich grob in *physische Storage Ressourcen* und *logische Storage Ressourcen* unterteilen. Für ein effektives Management Ihrer ONTAP Systeme mithilfe der in Active IQ Unified Manager bereitgestellten APIs ist ein Verständnis des Storage Ressourcenmodells und der Beziehungen zwischen den verschiedenen Storage Ressourcen erforderlich.

- **Physische Storage Ressourcen**

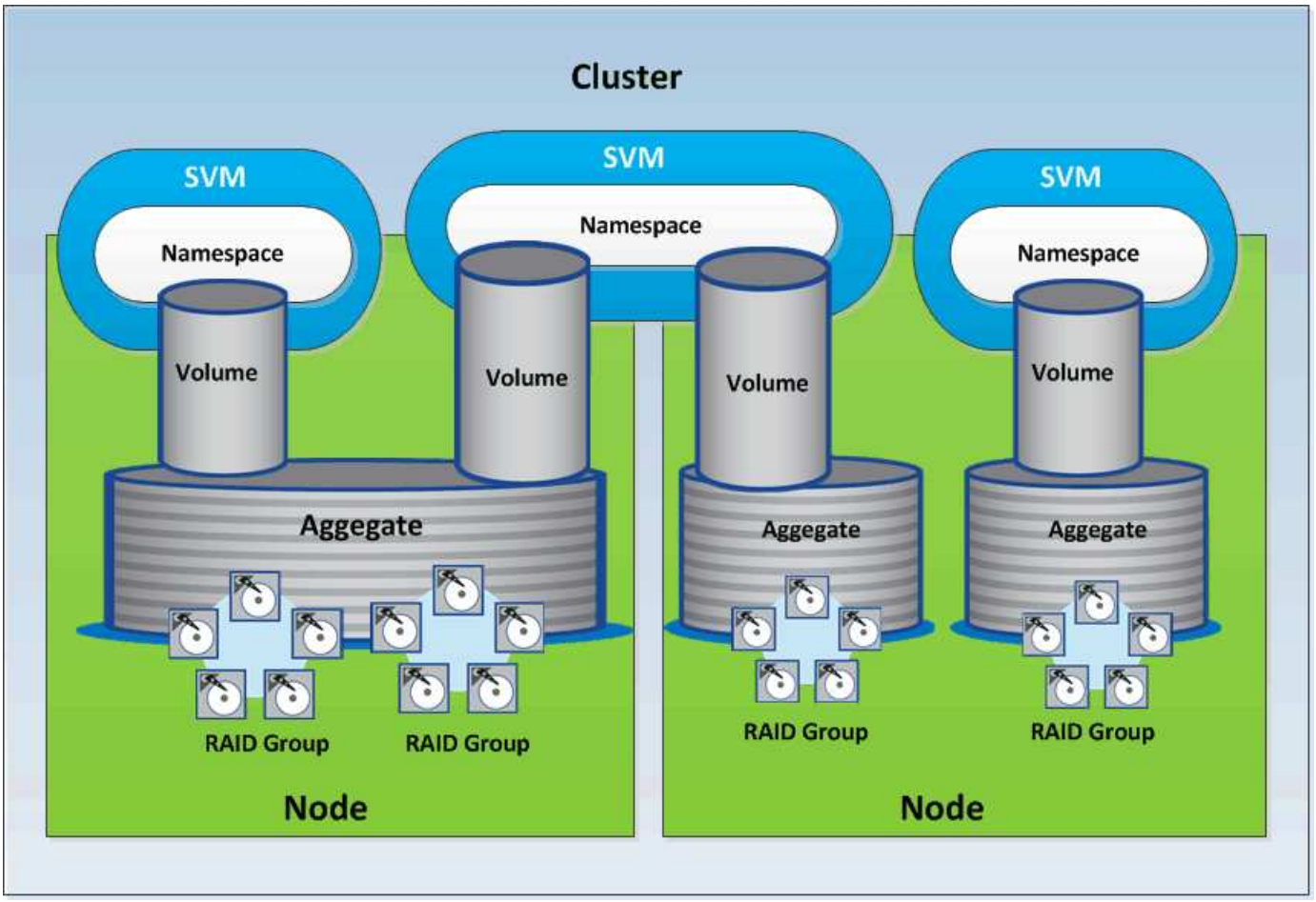
  Bezieht sich auf die physischen Storage Objekte, die von ONTAP bereitgestellt werden. Zu den physischen Storage Ressourcen gehören Festplatten, Cluster, Storage Controller, Knoten und Aggregate.

- **Logische Storage-Ressourcen**

  Bezeichnet die von ONTAP bereitgestellten Storage Ressourcen, die nicht an eine physische Ressource gebunden sind. Diese Ressourcen sind einer Storage Virtual Machine (SVM, ehemals Vserver) zugeordnet und existieren unabhängig von einer spezifischen physischen Storage Ressource wie einer Festplatte, einer Array LUN oder einem Aggregat.

  Zu den logischen Storage-Ressourcen gehören Volumes aller Typen und qtrees sowie die Funktionen und Konfigurationen, die mit diesen Ressourcen verwendet werden können, wie z. B. Snapshot Kopien, Deduplizierung, Komprimierung und Quotas.

Die folgende Abbildung zeigt die Storage Ressourcen in einem 2-Knoten-Cluster:



Zugriff über REST API und Authentifizierung in Active IQ Unified Manager

Zugriff auf REST APIs und Authentifizierung in Active IQ Unified Manager

Die Active IQ Unified Manager REST API ist über jeden REST Client oder jede Programmierplattform zugänglich, die HTTP-Anfragen mit einem grundlegenden HTTP-Authentifizierungsmechanismus ausgeben kann.

Beispiel einer Anfrage und Antwort:

- **Anfrage**

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

- **Antwort**

```
{
  "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* ist die IP-Adresse oder die vollqualifizierte Domain (FQDN) des API-Servers.
- Port 443

443 ist der Standardport für HTTPS. Sie können den HTTPS Port bei Bedarf anpassen.
Zum Senden von HTTP-Anfragen aus einem Webbrowser ist die Verwendung von REST API Browser Plugins erforderlich. Der Zugriff auf die REST API ist auch über Skriptplattformen wie cURL und Perl möglich.

Authentifizierung

Unified Manager unterstützt das grundlegende HTTP-Authentifizierungsschema für APIs. Für einen sicheren Informationsfluss (Anfrage und Antwort) sind die REST-APIs nur über HTTPS zugänglich. Der API-Server stellt allen Clients zur Serververifizierung ein selbstsigniertes SSL-Zertifikat bereit. Dieses Zertifikat kann durch ein benutzerdefiniertes Zertifikat (oder ein CA-Zertifikat) ersetzt werden.

Sie müssen den Benutzerzugriff auf den API-Server konfigurieren, um die REST-APIs aufzurufen. Die Benutzer können lokale Benutzer (Benutzerprofile in der lokalen Datenbank) oder LDAP-Benutzer sein (sofern

Sie den API-Server für die Authentifizierung über LDAP konfiguriert haben). Der Benutzerzugriff lässt sich verwalten, wenn Sie sich an der Benutzeroberfläche der Unified Manager Administration Console anmelden.

Informationen zu den HTTP-Statuscodes von Active IQ Unified Manager

Beim Ausführen der APIs oder bei der Fehlerbehebung ist es wichtig, die verschiedenen HTTP-Statuscodes und Fehlercodes zu kennen, die von Active IQ Unified Manager APIs verwendet werden.

Die folgende Tabelle listet die Fehlercodes im Zusammenhang mit der Authentifizierung auf:

HTTP-Statuscode	Statuscode-Titel	Beschreibung
200	OK	Wird bei erfolgreicher Ausführung synchroner API-Aufrufe zurückgegeben.
201	Erstellt	Erstellung neuer Ressourcen durch synchrone Aufrufe, wie z. B. die Konfiguration von Active Directory.
202	Akzeptiert	Wird bei erfolgreicher Ausführung asynchroner Aufrufe für Provisionierungsfunktionen wie das Erstellen von LUNs und Dateifreigaben zurückgegeben.
400	Ungültige Anforderung	Weist auf einen Fehler bei der Eingabevalidierung hin. Die Eingaben müssen korrigiert werden, beispielsweise durch die Verwendung gültiger Schlüssel in einem Anfragetext.
401	Nicht autorisierte Anforderung	Sie sind nicht berechtigt, die Ressource anzuzeigen/Nicht autorisiert.
403	Verbotene Anfrage	Der Zugriff auf die Ressource, die Sie erreichen wollten, ist nicht zulässig.
404	Ressource nicht gefunden	Die Ressource, die Sie erreichen wollten, wurde nicht gefunden.
405	Methode nicht zulässig	Methode nicht zulässig.
429	Zu viele Anfragen	Wird zurückgegeben, wenn der Benutzer innerhalb einer bestimmten Zeit zu viele Anfragen sendet.

HTTP-Statuscode	Statuscode-Titel	Beschreibung
500	Interner Serverfehler	Interner Serverfehler. Es konnte keine Antwort vom Server empfangen werden. Dieser interne Serverfehler kann dauerhaft sein oder auch nicht. Wenn Sie beispielsweise einen `GET` oder `GET ALL` Vorgang ausführen und diesen Fehler erhalten, wird empfohlen, den Vorgang mindestens fünfmal zu wiederholen. Wenn es sich um einen dauerhaften Fehler handelt, bleibt der zurückgegebene Statuscode 500. Wenn der Vorgang erfolgreich ist, lautet der zurückgegebene Statuscode 200.

Empfohlene Vorgehensweisen für die Verwendung von Active IQ Unified Manager APIs

Bei der Verwendung der APIs in Active IQ Unified Manager sollten Sie bestimmte empfohlene Vorgehensweisen beachten.

- Für eine gültige Ausführung müssen alle Antwortinhalte folgendes Format aufweisen:

```
application/json
```

- Die API-Versionsnummer steht in keinem Zusammenhang mit der Produktversionsnummer. Sie sollten die neueste Version der API verwenden, die für Ihre Unified Manager Instanz verfügbar ist. Weitere Informationen zu Unified Manager API-Versionen finden Sie im Abschnitt “REST API versioning in Active IQ Unified Manager”.
- Beim Aktualisieren von Array-Werten mithilfe der Unified Manager API muss die gesamte Zeichenfolge der Werte aktualisiert werden. Es ist nicht möglich, Werte an ein Array anzuhängen. Ein vorhandenes Array kann lediglich ersetzt werden.
- Sie können Filteroperatoren wie Pipe (|) und Wildcard (*) für alle Abfrageparameter verwenden, außer für Double-Werte, zum Beispiel IOPS und Performance in den metrics APIs.
- Von Abfragen von Objekten mit einer Kombination der Filteroperatoren Wildcard (*) und Pipe (|) ist abzuraten. Dabei könnte eine falsche Anzahl von Objekten abgerufen werden.
- Bei der Verwendung von Werten für Filter ist sicherzustellen, dass der Wert keine `?`Zeichen enthält. Dies dient der Verringerung des Risikos von SQL-Injection.
- Es ist zu beachten, dass die `GET` (all)-Anfrage für jede API maximal 1000 Datensätze zurückgibt. Auch wenn die Abfrage mit dem `max_records` Parameter auf einen Wert über 1000 gesetzt wird, werden nur 1000 Datensätze zurückgegeben.
- Für die Durchführung administrativer Funktionen empfiehlt sich die Verwendung der Unified Manager UI.

Fehlerbehebung mithilfe von Systemprotokollen in Active IQ Unified Manager

Systemprotokolle ermöglichen es Ihnen, die Ursachen von Fehlern zu analysieren und Probleme bei der Fehlerbehebung zu untersuchen, die beim Ausführen der APIs auftreten können.

Für die Fehlerbehebung bei Problemen im Zusammenhang mit den API-Aufrufen sind die Protokolle am folgenden Speicherort abrufbar.

Protokollspeicherort	Verwenden
`/var/log/ocie/access_log.log`	Enthält alle Details zum API-Aufruf, wie z. B. den Benutzernamen des Benutzers, der die API aufruft, Startzeit, Ausführungszeit, Status und URL. Mithilfe dieser Protokolldatei können Sie die häufig genutzten APIs überprüfen oder Fehler bei jedem GUI-Workflow beheben. Außerdem können Sie sie auf Grundlage der Ausführungszeit zur Skalierung von Analysen verwenden.
`/var/log/ocum/ocumserver.log`	Enthält alle API-Ausführungsprotokolle. Mit dieser Protokolldatei können Sie Fehler bei den API-Aufrufen beheben und die API-Aufrufe debuggen.
`/var/log/ocie/server.log`	Enthält alle Wildfly Server Deployments und Protokolle zu Services für Start/Stopp. Mithilfe dieser Protokolldatei können Sie die Grundursache von Problemen ermitteln, die beim Starten, Stoppen oder Deployment des Wildfly Servers auftreten.
`/var/log/ocie/au.log`	Enthält Protokolle im Zusammenhang mit der Acquisition Unit. Sie können diese Protokolldatei verwenden, wenn Sie in ONTAP Objekte erstellt, geändert oder gelöscht haben, diese Änderungen jedoch nicht in den Active IQ Unified Manager REST APIs berücksichtigt werden.

Informationen dazu, wie Active IQ Unified Manager Jobobjekte für die asynchrone Verarbeitung verwendet

Active IQ Unified Manager stellt die `jobs`API bereit, die Informationen über die während der Ausführung anderer APIs ausgeführten Jobs abruft. Kenntnisse darüber, wie die asynchrone Verarbeitung mithilfe des Job-Objekts funktioniert, sind erforderlich.

Einige API-Aufrufe, insbesondere solche zum Hinzufügen oder Ändern von Ressourcen, können länger dauern als andere. Unified Manager verarbeitet diese zeitaufwändigen Anfragen asynchron.

Asynchrone Anfragen werden mithilfe des Job-Objekts beschrieben.

Nach einem asynchronen API-Aufruf signalisiert der HTTP-Antwortcode 202, dass die Anfrage erfolgreich validiert und akzeptiert, aber noch nicht abgeschlossen wurde. Die Anfrage wird als Hintergrundaufgabe verarbeitet, die nach der ersten HTTP-Antwort an den Client weiterhin ausgeführt wird. Die Antwort enthält das Job-Objekt, das die Anfrage verankert, einschließlich seiner eindeutigen Kennung.

Abfrage des Job-Objekts, das einer API-Anfrage zugeordnet ist

Das in der HTTP-Antwort zurückgegebene Job-Objekt enthält mehrere Eigenschaften. Sie können die Eigenschaft state abfragen, um festzustellen, ob die Anfrage erfolgreich abgeschlossen wurde. Ein Job-Objekt kann sich in einem der folgenden Zustände befinden:

- `NORMAL`
- `WARNING`
- `PARTIAL_FAILURES`
- `ERROR`

Es gibt zwei Techniken, die Sie beim Abfragen eines Job-Objekts verwenden können, um einen Endzustand für die Aufgabe zu erkennen, entweder Erfolg oder Misserfolg:

- Bei einer Standard-Abfrage wird der aktuelle Jobstatus sofort zurückgegeben.
- Long Polling-Anfrage: Wenn sich der Jobstatus zu `NORMAL, ERROR,` oder `PARTIAL_FAILURES.` ändert

Schritte bei einer asynchronen Anfrage

Sie können die folgende allgemeine Vorgehensweise verwenden, um einen asynchronen API-Aufruf durchzuführen:

1. Führe den asynchronen API-Aufruf aus.
2. Sie erhalten eine HTTP-Antwort 202, die die erfolgreiche Annahme der Anfrage signalisiert.
3. Extrahieren Sie die Kennung für das Job-Objekt aus dem Antworttext.
4. Innerhalb einer Schleife auf das Erreichen des Endzustands durch das Job-Objekt `NORMAL, ERROR,` oder `PARTIAL_FAILURES.` warten
5. Überprüfung des Endstatus des Jobs und Abruf des Jobergebnisses.

Informationen zum Hello API Server Beispielprogramm in Active IQ Unified Manager

Der Hello API server ist ein Beispielprogramm, das zeigt, wie eine REST API in Active IQ Unified Manager mit einem einfachen REST Client aufgerufen wird. Das Beispielprogramm liefert grundlegende Informationen über den API Server im JSON Format (der Server unterstützt nur `application/json`Format).

Die verwendete URI lautet: `https://<hostname>/api/datacenter/svm/svms`. Dieser Beispielcode benötigt die folgenden Eingabeparameter:

- Die IP-Adresse oder der FQDN des API-Servers

- Optional: Portnummer (Standard: 443)
- Benutzername
- Passwort
- Antwortformat (`application/json`)

Zum Aufrufen von REST-APIs können Sie auch andere Skripte wie Jersey und RESTEasy verwenden, um einen Java-REST-Client für Active IQ Unified Manager zu schreiben. Die folgenden Hinweise zum Beispielcode sollten beachtet werden:

- Verwendet eine HTTPS-Verbindung zu Active IQ Unified Manager, um die angegebene REST-URI aufzurufen
- Ignoriert das von Active IQ Unified Manager bereitgestellte Zertifikat
- Überspringt die Hostnamenüberprüfung während des Handschlags
- Verwendet `javax.net.ssl.HttpsURLConnection` für eine URI-Verbindung
- Verwendet eine Drittanbieter-Bibliothek (`org.apache.commons.codec.binary.Base64`) zum Erstellen der Base64-kodierten Zeichenkette, die bei der HTTP-Basisauthentifizierung verwendet wird

Zum Kompilieren und Ausführen des Beispielcodes benötigen Sie den Java-Compiler 1.8 oder höher.

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpsURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
necessary steps
     * to invoke the REST URI and show the response
```

```
     */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
            System.exit(1);
        }
        setUserArguments(args);
        String serverBaseUrl = "https://" + server;
        if (null != port) {
            serverBaseUrl = serverBaseUrl + ":" + port;
        }
        server_url = serverBaseUrl + "/api/datacenter/svm/svms";
        try {
            HttpsURLConnection connection =
getAllTrustingHttpsUrlConnection();
            if (connection == null) {
                System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
                System.exit(1);
            }
            System.out.println("Invoking API: " + server_url);
            connection.setRequestMethod("GET");
            connection.setRequestProperty("Accept", "application/" +
response_format);
            String authString = getAuthorizationString();
            connection.setRequestProperty("Authorization", "Basic " +
authString);
            if (connection.getResponseCode() != 200) {
                System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
                        + connection.getResponseMessage());
                System.exit(1);
            }
            BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
            String response;
            System.out.println("Response:");
            while ((response = br.readLine()) != null) {
                System.out.println(response);
            }
            connection.disconnect();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    /* Print the usage of this sample code */ private static void
```

```
printUsage() {
        System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
        System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
        System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
        System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
        System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
        System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
    }

    /* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
            String[] args) {
        server = args[0];
        user = args[1];
        password = args[2];
        if (server.contains(":")) {
            String[] parts = server.split(":");
            server = parts[0];
            port = parts[1];
        }
    }

    /*
     * * Create a trust manager which accepts all certificates and * use
this trust
     * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
     * SSL Context and skip * server hostname verification during SSL
handshake. * *
     * Note: Trusting all certificates or skipping hostname verification *
is not
     * required for API Services to work. These are done here to * keep
this sample
     * REST Client code as simple as possible.
     */ private static HttpsURLConnection
getAllTrustingHttpsUrlConnection()    {        HttpsURLConnection conn =
null;        try {            /* Creating a trust manager that does not
validate certificate chains */            TrustManager[]
trustAllCertificatesManager = new                    TrustManager[]{new
X509TrustManager(){
```

```
     public X509Certificate[] getAcceptedIssuers(){return  null;}
     public void checkClientTrusted(X509Certificate[]
certs, String authType){}
     public void checkServerTrusted(X509Certificate[]
certs, String authType){}            }};            /* Initialize the
SSLContext with the all-trusting trust manager */
     SSLContext sslContext = SSLContext.getInstance("TLS");
sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));            URL url = new URL(server_url);            conn =
(HttpsURLConnection) url.openConnection();            /* Do not perform an
actual hostname verification during SSL Handshake.            Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {               public
boolean verify(String host, SSLSession                        session) {
return true;               }            });        } catch (Exception e)
{            e.printStackTrace();        }        return conn;    }

    /*
     * * This forms the Base64 encoded string using the username and
password *
     * provided by the user. This is required for HTTP Basic
Authentication.
     */ private static String getAuthorizationString() {
        String userPassword = user + ":" + password;
        byte[] authEncodedBytes =
Base64.encodeBase64(userPassword.getBytes());
        String authString = new String(authEncodedBytes);
        return authString;
    }

}
```

Unified Manager REST-APIs

Kategorien für Active IQ Unified Manager REST APIs verstehen

In diesem Abschnitt sind die REST APIs für Active IQ Unified Manager nach Kategorien aufgeführt.

Sie können in Ihrer Unified Manager Instanz die Online-Dokumentationsseite anzeigen, die die Details zu jedem REST API-Aufruf enthält. Dieses Dokument wiederholt die Details der Online-Dokumentation nicht. Jeder in diesem Dokument aufgeführte oder beschriebene API-Aufruf enthält nur die Informationen, die Sie benötigen, um den Aufruf auf der Dokumentationsseite zu finden. Nachdem Sie einen bestimmten API-Aufruf gefunden haben, können Sie die vollständigen Details dieses Aufrufs prüfen, einschließlich der

Eingabeparameter, Ausgabeformate, HTTP-Statuscodes und des Typs der Anforderungsverarbeitung.

Die folgenden Informationen sind für jeden API-Aufruf innerhalb eines Workflows enthalten, um den Aufruf auf der Dokumentationsseite zu finden:

- Kategorie

  Die API-Aufrufe sind auf der Dokumentationsseite in funktional verwandte Bereiche oder Kategorien unterteilt. Einen bestimmten API-Aufruf finden Sie, wenn Sie bis zum Ende der Seite scrollen und anschließend auf die entsprechende API-Kategorie klicken.

- HTTP-Verb (Aufruf)

  Das HTTP-Verb identifiziert die an einer Ressource ausgeführte Aktion. Jeder API-Aufruf erfolgt über ein einzelnes HTTP-Verb.

- Pfad

  Der Pfad bestimmt die spezifische Ressource, die die Aktion im Rahmen eines Aufrufs verwendet. Die Pfadzeichenfolge wird an die Kern-URL angehängt, um die vollständige URL zu bilden, die die Ressource identifiziert.

Verwaltung von Speicherobjekten in einem Rechenzentrum mithilfe von APIs in Active IQ Unified Manager

Die REST-APIs in der `datacenter` Kategorie ermöglichen Ihnen das Managen der Storage Objekte in Ihrem Datacenter, wie z. B. Cluster, Knoten, Aggregate, Storage VMs, Volumes, LUNs, Dateifreigaben und Namespaces. Diese APIs stehen zum Abfragen der Konfiguration der Objekte zur Verfügung, während einige von ihnen das Hinzufügen, Löschen oder Ändern dieser Objekte ermöglichen.

Die meisten dieser APIs sind GET-Aufrufe, die clusterübergreifende Aggregation mit Unterstützung für Filtern, Sortieren und Paginierung bereitstellen. Bei der Ausführung dieser APIs geben sie Daten aus der Datenbank zurück. Daher müssen neu erstellte Objekte im nächsten Datenabrufzyklus erkannt werden, damit sie in der Antwort erscheinen.

Um die Details eines bestimmten Objekts abzufragen, müssen Sie die eindeutige ID dieses Objekts eingeben, um dessen Details anzuzeigen. Informationen zu Metriken und Analysen der Storage Objekte finden Sie beispielsweise unter "Anzeigen von Performance-Kennzahlen".

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-
2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

Die CURL-Befehle, Beispiele, Anfragen und Antworten zu den APIs sind über Ihre Swagger API Schnittstelle verfügbar. Sie können die Ergebnisse anhand bestimmter Parameter filtern und sortieren, wie in Swagger angegeben. Diese APIs ermöglichen es Ihnen, die Ergebnisse nach bestimmten Storage Objekten wie Cluster, Volume oder Storage VM zu filtern.

APIs für Storage-Objekte in Ihrem Datacenter

HTTP-Verb	Pfad	Beschreibung

GET	`/datacenter/cluster/clusters`
	
	`/datacenter/cluster/clusters/{key}`
		Mit dieser Methode lassen sich die Details der ONTAP Cluster im gesamten Datacenter anzeigen. Die API liefert Informationen wie die IPv4- oder IPv6-Adresse des Clusters, Informationen über den Node, z. B. den Systemstatus des Node, die Performance Kapazität und das High Availability (HA) Paar, und gibt an, ob der Cluster ein All SAN Array ist.

GET	`/datacenter/cluster/licensing/licenses` `/datacenter/cluster/licensing/licenses/{key}`	Diese Funktion liefert Details zu den auf den Clustern in Ihrem Datacenter installierten Lizenzen. Sie können Ihre Ergebnisse anhand der erforderlichen Kriterien filtern. Informationen wie der Lizenzschlüssel, der Clusterschlüssel, das Ablaufdatum und der Lizenzumfang werden angezeigt. Sie können einen Lizenzschlüssel eingeben, um die Details einer bestimmten Lizenz abzurufen.

GET	`/datacenter/cluster/nodes`
	
	`/datacenter/cluster/nodes/{key}`
		Mit dieser Methode können Sie die Details der Knoten im Datacenter anzeigen. Sie können Informationen über den Cluster, den Systemstatus des Knotens, die Performancekapazität und das High Availability (HA)-Paar des Knotens anzeigen.

GET	`/datacenter/protocols/cifs/shares`
	
	`/datacenter/protocols/cifs/shares/{key}`
		Mit dieser Methode können Sie die Details der CIFS-Freigaben im Datacenter anzeigen. Neben Cluster-, SVM- und Volume-Details werden auch Informationen zur Access Control List (ACL) zurückgegeben.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	Mit dieser Methode können Sie die Details der Exportrichtlinien für die unterstützten NFS Services anzeigen. Sie können die Exportrichtlinien für einen Cluster oder eine Storage VM abfragen und den Exportrichtlinienschlüssel für die Provisionierung von NFS-Dateifreigaben wiederverwenden. Weitere Informationen zum Zuweisen und Wiederverwenden von Exportrichtlinien für Workloads finden Sie unter “Provisioning CIFS and NFS file shares”.
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	Mit dieser Methode können Sie die Sammlung der Aggregate im Datacenter oder ein bestimmtes Aggregat anzeigen, um Workloads darauf zu provisionieren oder sie zu überwachen. Informationen wie Cluster- und Knotendetails, die genutzte Performance-Kapazität, der verfügbare und verwendete Speicherplatz sowie die Storage-Effizienz werden zurückgegeben.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	Mit dieser Methode lässt sich die Sammlung von LUNs im gesamten Datacenter anzeigen. Informationen zur LUN, wie Cluster- und SVM-Details, QoS-Richtlinien und Initiatorgruppen, lassen sich anzeigen.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	Mit dieser Methode können Sie die Details aller QoS Richtlinien anzeigen, die für die Storage Objekte im Datacenter gelten. Informationen wie die Cluster- und SVM-Details, die Details der festen oder adaptiven Richtlinie sowie die Anzahl der Objekte, für die diese Richtlinie gilt, werden zurückgegeben.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	Mit dieser Methode können Sie die Qtree-Details im gesamten Datacenter für alle FlexVol Volumes oder FlexGroup Volumes anzeigen. Informationen wie die Cluster- und SVM-Details, das FlexVol Volume und die Exportrichtlinie werden zurückgegeben.
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	Mit dieser Methode lässt sich die Sammlung von Volumes im Datacenter anzeigen. Informationen über die Volumes, z. B. SVM- und Clusterdetails, QoS- und Exportrichtlinien sowie dazu, ob das Volume vom Typ Lesen/Schreiben, Datenschutz oder Lastverteilung ist, werden zurückgegeben. Für FlexVol- und FlexClone-Volumes können Sie die Informationen zu den jeweiligen Aggregaten anzeigen. Für ein FlexGroup-Volume gibt die Abfrage die Liste der zugehörigen Aggregate zurück.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/protocols/san/igroups`
	
	`/datacenter/protocols/san/igroups/{key}`
		Sie können Initiatorgruppen (igroups) zuweisen, die zum Zugriff auf bestimmte LUN-Ziele berechtigt sind. Falls bereits eine Initiatorgruppe vorhanden ist, können Sie diese zuweisen. Alternativ können Sie igroups erstellen und sie den LUNs zuordnen.
		
		Mit diesen Methoden können Sie Initiatorgruppen abfragen, erstellen, löschen bzw. ändern.
		
		Wichtige Punkte:
		
		• `POST:`Beim Erstellen einer Initiatorgruppe können Sie die Storage VM festlegen, auf der Sie den Zugriff zuweisen möchten.
		• `DELETE:` Zum Löschen einer bestimmten Initiatorgruppe muss der Schlüssel der Initiatorgruppe als Eingabeparameter angegeben werden. Wenn einer LUN bereits eine Initiatorgruppe zugewiesen wurde, kann diese Initiatorgruppe nicht gelöscht werden.
		• `PATCH:` Als Eingabeparameter muss der Schlüssel der Initiatorgruppe angegeben werden, um eine bestimmte Initiatorgruppe zu ändern. Außerdem müssen Sie die Eigenschaft eingeben, die aktualisiert werden soll, sowie deren Wert.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/svm/svms`
	
	`/datacenter/svm/svms/{key}`
		Mit diesen Methoden können Sie Storage Virtual Machines (storage VMs) anzeigen, erstellen, löschen und ändern.
		
		• `POST`: Sie müssen das Storage VM-Objekt, das Sie erstellen möchten, als Eingabeparameter angeben. Sie können eine benutzerdefinierte Storage VM erstellen und ihr anschließend die erforderlichen Eigenschaften zuweisen.
		• `DELETE`: Zum Löschen einer bestimmten Storage VM müssen Sie den Storage VM Schlüssel angeben.
		• `PATCH:`Sie müssen den Storage VM-Schlüssel angeben, um eine bestimmte Storage VM zu ändern. Außerdem müssen Sie die Eigenschaften, die Sie aktualisieren möchten, zusammen mit ihren Werten eingeben.

Wichtige Punkte:

Wenn in Ihrer Umgebung die SLO-basierte Workload Provisionierung aktiviert ist, muss beim Erstellen der Storage VM sichergestellt sein, dass sie alle Protokolle unterstützt, die für die Provisionierung von LUNs und Dateifreigaben darauf erforderlich sind, z. B. CIFS oder SMB, NFS, FCP und iSCSI. Die Provisionierung Workflows können fehlschlagen, wenn die Storage VM die erforderlichen Services nicht unterstützt. Es wird empfohlen, die Services für die jeweiligen Workload-Typen ebenfalls auf der Storage VM zu aktivieren.

Wenn Sie die SLO-basierte Workload Provisionierung in Ihrer Umgebung aktiviert haben, können Sie die Storage VM, auf der Storage Workloads provisioniert wurden, nicht löschen. Wenn Sie eine Storage VM löschen, auf der ein CIFS- oder SMB-Server konfiguriert wurde, löscht diese API auch den CIFS- oder SMB-Server sowie die lokale Active Directory-Konfiguration. Der Name des CIFS- oder SMB-Servers bleibt jedoch in der Active Directory-Konfiguration bestehen, und Sie müssen ihn manuell vom Active Directory-Server löschen.

APIs für Netzwerkelemente in Ihrem Datacenter

Die folgenden APIs in der Kategorie Datacenter rufen Informationen über die Ports und Netzwerkschnittstellen in Ihrer Umgebung ab, insbesondere über die FC-Ports, FC-Schnittstellen, Ethernet-Ports und IP-Schnittstellen.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	Ruft Informationen zu allen Ethernet-Ports in Ihrer Datacenter-Umgebung ab. Mit einem Portschlüssel als Eingabeparameter können Sie die Informationen dieses spezifischen Ports anzeigen. Abgerufen werden unter anderem Clusterdetails, die Broadcast-Domäne, Portdetails wie Status, Geschwindigkeit und Typ sowie die Information, ob der Port aktiviert ist.
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	Mit dieser Methode können Sie die Details der FC-Schnittstellen in Ihrer Datacenter-Umgebung anzeigen. Mit einem Schnittstellenschlüssel als Eingabeparameter können Sie die Informationen zu dieser spezifischen Schnittstelle anzeigen. Dabei werden Informationen wie Clusterdetails, Details zum Home-Knoten und Details zum Home-Port abgerufen.
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	Ruft Informationen zu allen FC-Ports ab, die in den Knoten Ihrer Datacenter-Umgebung verwendet werden. Mit einem Portschlüssel als Eingabeparameter können Sie die Informationen des jeweiligen Ports anzeigen. Abgerufen werden unter anderem Clusterdetails, Portbeschreibung, unterstütztes Protokoll und Portstatus.
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	Mit dieser Methode lassen sich die Details der IP-Schnittstellen in Ihrer Datacenter-Umgebung anzeigen. Mit einem Schnittstellenschlüssel als Eingabeparameter lassen sich die Informationen zu dieser spezifischen Schnittstelle anzeigen. Dabei werden Informationen wie Clusterdetails, IPspace-Details, Home-Node-Details und die Angabe, ob Failover aktiviert ist, abgerufen.

Zugriff auf ONTAP APIs über Proxyzugriff in Active IQ Unified Manager

Die Gateway-APIs bieten Ihnen den Vorteil, die Anmeldeinformationen von Active IQ

Unified Manager zum Ausführen von ONTAP REST APIs und zum Managen von Storage Objekten zu verwenden. Diese APIs sind verfügbar, wenn die API Gateway Funktion in der Unified Manager Web-UI aktiviert ist.

Unified Manager REST APIs unterstützen nur eine begrenzte Anzahl von Aktionen, die auf den Unified Manager Datenquellen, also ONTAP Clustern, ausgeführt werden können. Die anderen Funktionen sind über ONTAP APIs verfügbar. Die Gateway APIs ermöglichen Unified Manager, als Durchleitungsoberfläche für das Tunneln aller API-Anforderungen an die von ihm verwalteten ONTAP Cluster zu dienen, ohne dass eine separate Anmeldung bei jedem einzelnen Datacenter Cluster erforderlich ist. Es dient als zentraler Verwaltungspunkt für die Ausführung der APIs über die von Ihrer Unified Manager Instanz verwalteten ONTAP Cluster. Die API Gateway Funktion ermöglicht Unified Manager, als zentrale Kontrollebene zu dienen, über die mehrere ONTAP Cluster gemanagt werden können, ohne dass eine einzelne Anmeldung bei jedem Cluster erforderlich ist. Die Gateway APIs ermöglichen es, in Unified Manager angemeldet zu bleiben und die ONTAP Cluster durch Ausführen von ONTAP REST API Vorgängen zu managen.

Alle Benutzer können Abfragen mittels der GET-Operation ausführen. Anwendungsadministratoren können alle ONTAP REST-Operationen ausführen.

Das Gateway fungiert als Proxy, um die API-Anfragen zu tunneln, indem es Header und Body der Anfragen im gleichen Format wie in den ONTAP APIs beibehält. Sie können Ihre Unified Manager Anmeldedaten verwenden und die spezifischen Vorgänge ausführen, um auf die ONTAP Cluster zuzugreifen und sie zu managen, ohne Anmeldedaten einzelner Cluster angeben zu müssen. Es übernimmt weiterhin die Cluster-Authentifizierung und das Cluster-Management, leitet die API-Anfragen jedoch so um, dass sie direkt auf dem jeweiligen Cluster ausgeführt werden. Die von den APIs zurückgegebene Antwort entspricht der Antwort der entsprechenden ONTAP REST APIs, die direkt von ONTAP ausgeführt werden.

HTTP-Verb	Pfad (URL)	Beschreibung
`GET`	`/gateways`	Diese GET-Methode ruft die Liste aller von Unified Manager gemanagten Cluster ab, die ONTAP REST-Aufrufe unterstützen. Sie können die Clusterdetails überprüfen und anhand der Cluster-UUID oder der Universal Unique Identifier (UUID) weitere Methoden ausführen. Die Gateway-APIs rufen nur die Cluster ab, die von ONTAP 9.5 oder höher unterstützt und über HTTPS zu Unified Manager hinzugefügt wurden.

HTTP-Verb	Pfad (URL)	Beschreibung

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
 	
`OPTIONS` (nicht auf Swagger verfügbar)
 	
`HEAD` (nicht auf Swagger verfügbar)
	`/gateways/{uuid}/{path}`
	
	Der Wert für {uuid} muss durch die Cluster UUID ersetzt werden, auf der die REST Operation ausgeführt werden soll. Es ist außerdem sicherzustellen, dass die UUID zu einem von ONTAP 9.5 oder höher unterstützten Cluster gehört und über HTTPS zu Unified Manager hinzugefügt wurde. {path} muss durch die ONTAP REST URL ersetzt werden. Aus der URL muss `/api/` entfernt werden.
		Dies ist eine zentrale Proxy-API, die POST-, DELETE-, PATCH- und GET-Anfragen für alle ONTAP REST-APIs unterstützt. Für keine der APIs gelten Einschränkungen, solange sie von ONTAP unterstützt werden. Die Tunneling- bzw. Proxy-Funktionalität kann nicht deaktiviert werden.
		
		Die `OPTIONS`Methode gibt alle Operationen zurück, die von einer ONTAP REST API unterstützt werden. Wenn eine ONTAP API beispielsweise nur die `GET`Operation unterstützt, liefert die Ausführung der `OPTIONS`Methode über diese Gateway-API `GET`als Antwort. Diese Methode wird von Swagger nicht unterstützt, kann aber mit anderen API-Tools ausgeführt werden.
		
		Die `OPTIONS` Methode bestimmt, ob eine Ressource verfügbar ist. Dieser Vorgang kann verwendet werden, um die Metadaten zu einer Ressource in den HTTP-Antwortheadern anzuzeigen. Diese Methode wird von Swagger nicht unterstützt, kann jedoch mit anderen API-Tools ausgeführt werden.

Grundlagen des API Gateway Tunneling

Die Gateway APIs ermöglichen es, ONTAP Objekte über Unified Manager zu managen. Unified Manager managt die Cluster und Authentifizierungsdetails und leitet die Anfragen an den ONTAP REST Endpunkt weiter. Die Gateway API transformiert die URL und die Hypermedia as the Engine of Application State (HATEOAS) Links im Header und im Antworttext mit der Basis URL des API Gateway. Die Gateway API fungiert als Proxy Basis URL, an die die ONTAP REST URL angehängt wird und über die der erforderliche ONTAP REST Endpunkt ausgeführt wird.

Damit eine ONTAP API über das API Gateway erfolgreich ausgeführt werden kann, muss die API von der Version des ONTAP Clusters unterstützt werden, auf dem sie ausgeführt wird. Die Ausführung einer API, die auf dem ONTAP Cluster nicht unterstützt wird, liefert keine Ergebnisse.

In diesem Beispiel lautet die Gateway-API (Proxy-Basis-URL): `/gateways/{uuid}/`

Die verwendete ONTAP API lautet: `/storage/volumes`. Die ONTAP API REST URL wird als Wert für den

Pfadparameter angegeben.

Beim Hinzufügen des Pfads ist sicherzustellen, dass “/” symbol at the beginning of the URL. For the API `/storage/volumes`, add `storage/volumes.` entfernt wurde.

Die angehängte URL lautet: `/gateways/{uuid}/storage/volumes`

Beim Ausführen des `GET` Vorgangs wird folgende URL generiert:
`GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes`

Das `/api` Tag der ONTAP REST URL wird in der angehängten URL entfernt, und das für die gateway API wird beibehalten.

Beispiel für einen cURL-Befehl

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes" -H "accept: application/hal+json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

Die API gibt die Liste der Storage Volumes in diesem Cluster zurück. Das Antwortformat entspricht dem, das Sie erhalten, wenn Sie dieselbe API in ONTAP ausführen. Die zurückgegebenen Statuscodes sind die ONTAP REST-Statuscodes.

API-Bereich festlegen

Alle APIs haben einen Kontext, der innerhalb des Clusters festgelegt ist. APIs, die auf Basis von Storage VMs arbeiten, haben ebenfalls den Cluster als Geltungsbereich, das heißt, die API-Operationen werden auf einer bestimmten Storage VM innerhalb eines verwalteten Clusters ausgeführt. Beim Ausführen der `/gateways/{uuid}/{path}` API ist darauf zu achten, dass die Cluster UUID (Unified Manager datasource UUID) für den Cluster eingegeben wird, auf dem die Operation ausgeführt wird. Zum Festlegen des Kontexts auf eine bestimmte Storage VM innerhalb dieses Clusters ist der Storage VM Schlüssel als Parameter X-Dot-SVM-UUID oder der Storage VM Name als Parameter X-Dot-SVM-Name einzugeben. Der Parameter wird als Filter im String-Header hinzugefügt, und die Operation wird innerhalb des Geltungsbereichs dieser Storage VM in diesem Cluster ausgeführt.

Beispiel für einen cURL-Befehl

```
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>"
```

Weitere Informationen zur Verwendung von ONTAP REST-APIs finden Sie unter "ONTAP REST API-Automatisierung"

Administrative Aufgaben mithilfe von APIs in Active IQ Unified Manager ausführen

Sie können die APIs der Kategorie `administration` verwenden, um

Sicherungseinstellungen zu ändern, die Informationen zur Sicherungsdatei und Clusterzertifikate zu überprüfen und ONTAP Cluster auch als Active IQ Unified Manager Datenquellen zu managen.

Sie benötigen die Rolle Application Administrator, um diese Vorgänge auszuführen. Alternativ können Sie die Web-Benutzeroberfläche von Unified Manager verwenden, um diese Einstellungen zu konfigurieren.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`PATCH`
	`/admin/backup-settings`
	
	`/admin/backup-settings`
		Mit der `GET`Methode können Sie die Einstellungen des in Unified Manager standardmäßig konfigurierten Sicherungszeitplans anzeigen. Sie können Folgendes überprüfen:
		
		• Ob der Zeitplan aktiviert oder deaktiviert ist
		• Häufigkeit der geplanten Datensicherung (täglich oder wöchentlich)
		• Zeitpunkt der Datensicherung
		• Maximale Anzahl der Backup-Dateien, die in der Applikation aufbewahrt werden sollten
		
		Die Uhrzeit der Datensicherung wird in der Zeitzone des Servers angegeben.
		
		Die Einstellungen für die Datenbanksicherung sind in Unified Manager standardmäßig verfügbar, und es lässt sich kein Sicherungszeitplan erstellen. Die Standardeinstellungen lassen sich jedoch mit der `PATCH`Methode ändern.

`GET`	`/admin/backup-file-info`	Bei jeder Änderung des Sicherungsplans für Unified Manager wird eine Sicherungsdumpdatei generiert. Mit dieser Methode können Sie überprüfen, ob die Sicherungsdatei gemäß den geänderten Sicherungseinstellungen generiert wurde und ob die Informationen in der Datei mit den geänderten Einstellungen übereinstimmen.

HTTP-Verb	Pfad	Beschreibung
GET	/admin/datasource-certificate	Mit dieser Methode können Sie das Datenquellenzertifikat (Clusterzertifikat) aus dem Truststore anzeigen. Die Validierung des Zertifikats ist erforderlich, bevor ein ONTAP Cluster als Unified Manager Datenquelle hinzugefügt wird.
GET POST PATCH DELETE	/admin/datasources/clusters /admin/datasources/clusters/{key}	Mit der GET Methode können Sie die Details der von Unified Manager gemanagten Datenquellen (ONTAP Cluster) abrufen. Sie können Unified Manager auch einen neuen Cluster als Datenquelle hinzufügen. Zum Hinzufügen eines Clusters benötigen Sie dessen Hostnamen, Benutzernamen und Passwort. Zum Ändern und Löschen eines Clusters, das von Unified Manager als Datenquelle gemanagt wird, dient der ONTAP Clusterschlüssel.

Benutzerverwaltung in Active IQ Unified Manager mithilfe von APIs

Mit den APIs in der security Kategorie können Sie den Benutzerzugriff auf ausgewählte Clusterobjekte in Active IQ Unified Manager steuern. Sie können lokale Benutzer oder Datenbankbenutzer hinzufügen. Sie können auch Remote-Benutzer oder Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Basierend auf den Berechtigungen der Rollen, die Sie den Benutzern zuweisen, können diese die Storage Objekte managen oder die Daten in Unified Manager anzeigen.

Sie benötigen die Rolle Application Administrator, um diese Vorgänge auszuführen. Alternativ können Sie die Web-Benutzeroberfläche von Unified Manager verwenden, um diese Einstellungen zu konfigurieren.

Die APIs unter der security Kategorie verwenden den Parameter users, also den Benutzernamen, und nicht den Parameter key als eindeutigen Bezeichner für die Benutzerentität.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`POST`
	`/security/users`
	
	`/security/users`
		Mit diesen Methoden können Sie Details zu Benutzern abrufen oder neue Benutzer zu Unified Manager hinzufügen.
		
		Sie können Benutzern basierend auf ihren Benutzertypen spezifische Rollen zuweisen. Beim Hinzufügen von Benutzern müssen Sie Passwörter für den lokalen Benutzer, den Wartungsbenutzer und den Datenbankbenutzer angeben.

`GET`
 	
`PATCH`
 	
`DELETE`
	`/security/users/{name}`	Mit der GET-Methode lassen sich alle Details eines Benutzers abrufen, z. B. Name, E-Mail-Adresse, Rolle und Berechtigungstyp. Mit der PATCH-Methode lassen sich die Details aktualisieren. Mit der DELETE-Methode lässt sich der Benutzer entfernen.

Leistungsmetriken mithilfe von APIs in Active IQ Unified Manager anzeigen

Active IQ Unified Manager stellt Ihnen eine Reihe von APIs unter der `/datacenter` Kategorie zur Verfügung, mit denen Sie die Performance-Daten Ihrer Cluster und Storage Objekte in einem Datacenter anzeigen können. Diese APIs rufen die Performance-Daten der verschiedenen Storage Objekte wie Cluster, Nodes, LUNs, Volumes, Aggregate, Storage VMs, FC-Schnittstellen, FC-Ports, Ethernet-Ports und IP-Schnittstellen ab.

Die `/metrics` und `/analytics` APIs bieten unterschiedliche Ansichten der Performance-Metriken, mit denen Sie für die folgenden Storage Objekte in Ihrem Datacenter verschiedene Detailebenen aufschlüsseln können:

- Cluster
- Knoten
- Storage VMs
- Aggregate
- Volumes
- LUNs
- FC Schnittstellen
- FC-Ports
- Ethernet-Ports
- IP Schnittstellen

Die folgende Tabelle vergleicht die `/metrics` und `/analytics` APIs hinsichtlich der Details der abgerufenen Performance-Daten.

Kennzahlen	Analysen
Performancedetails für ein einzelnes Objekt. Beispielsweise erfordert die `/datacenter/cluster/clusters/{key}/metrics` API die Eingabe des Cluster-Schlüssels als Pfadparameter, um die Metriken für diesen spezifischen Cluster abzurufen.	Performance-Details für mehrere Objekte desselben Typs in einem Datacenter. Beispielsweise ruft die `/datacenter/cluster/clusters/analytics` API die kollektiven Metriken aller Cluster in einem Datacenter ab.
Performance-Kennzahlenbeispiel für ein Storage-Objekt basierend auf dem Zeitintervallparameter für den Abruf.	Der aggregierte Gesamtwert der Performance für einen bestimmten Typ von Storageobjekt über einen bestimmten Zeitraum (mehr als 72 Stunden).
Der Abruf umfasst grundlegende Details des Objekts, beispielsweise zu einem Knoten oder Cluster.	Es werden keine spezifischen Details abgerufen.
Akkumulierte Zählerwerte wie Minimum, Maximum, 95. Perzentil und die durchschnittlichen Performance Werte über einen Zeitraum werden für ein einzelnes Objekt abgerufen, z. B. Lese-, Schreib-, Gesamt- und andere Zähler.	Für alle Objekte desselben Typs wird ein einzelner aggregierter Wert angezeigt.

Kennzahlen	Analysen
Der Zeitbereich und die Abtastdaten basieren auf dem folgenden Zeitplan: der Zeitbereich für die Daten. Beispiele sind 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m. Bei einem Bereich von mehr als 3 Tagen (72 hr) werden 1-Stunden-Abtastwerte verwendet, andernfalls 5-Minuten-Abtastwerte. Der Zeitraum für jeden Zeitbereich ist wie folgt: • 1h: Messwerte der letzten Stunde, in 5-Minuten-Intervallen erfasst. • 12h: Messwerte der letzten 12 Stunden, im Abstand von 5 Minuten erfasst. • 1d: Messwerte des letzten Tages, im Abstand von 5 Minuten erfasst. • 2d: Metriken der letzten 2 Tage, im 5-Minuten-Intervall erfasst. • 3d: Metriken der letzten 3 Tage, erfasst in einem 5-Minuten-Intervall. • 15d: Kennzahlen der letzten 15 Tage, erfasst über 1 Stunde. • 1w: Kennzahlen der letzten Woche, erfasst über einen Zeitraum von einer Stunde. • 1m: Kennzahlen des letzten Monats, über 1 Stunde erfasst. • 2m: Kennzahlen der letzten 2 Monate, erfasst über 1 Stunde. • 3m: Metriken der letzten 3 Monate, erfasst über 1 Stunde. • 6m: Kennzahlen der letzten 6 Monate, im Abstand von 1 Stunde erfasst. Verfügbare Werte: 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m Standardwert: 1h	Über 72 Stunden. Die Dauer, über die diese Stichprobe berechnet wird, wird im ISO-8601-Standardformat dargestellt.

Beispielausgabe für Metrik-APIs

Beispielsweise ruft die `/datacenter/cluster/nodes/{key}/metrics` API unter anderem die folgenden Details für einen Node ab:

Der Wert 95. Perzentil in der Zusammenfassung gibt an, dass 95 % der für den Zeitraum gesammelten Proben einen Zählerwert aufweisen, der kleiner ist als der als 95. Perzentil angegebene Wert.

```
{
```

```
      "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
        }
      },
```

Beispielausgabe für Analyse-APIs

Beispielsweise ruft die `/datacenter/cluster/nodes/analytics` API unter anderem die folgenden Werte für alle Knoten ab:

```
{     "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"
        }
      }
    },
```

Liste der verfügbaren APIs

Die folgende Tabelle beschreibt die `/metrics` und `/analytics` APIs im Detail.

> Die von diesen APIs zurückgegebenen IOPS- und Performance-Metriken sind Double-Werte, zum Beispiel `100.53`. Das Filtern dieser Gleitkommawerte anhand der Pipe-Zeichen (|) und Platzhalterzeichen (*) wird nicht unterstützt.

HTTP-Verb	Pfad	Beschreibung
`GET`	`/datacenter/cluster/clusters/{key}/metrics`	Ruft Performance-Daten (Stichproben und Zusammenfassung) für einen Cluster ab, der durch den Eingabeparameter des Cluster-Schlüssels angegeben wird. Informationen wie der Cluster-Schlüssel und die UUID, der Zeitraum, IOPS, der Durchsatz und die Anzahl der Stichproben werden zurückgegeben.
`GET`	`/datacenter/cluster/clusters/analytics`	Ruft Performance-Metriken auf hoher Ebene für alle Cluster in einem Datacenter ab. Sie können Ihre Ergebnisse anhand der gewünschten Kriterien filtern. Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) werden zurückgegeben.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/cluster/nodes/{key}/metrics	Performance-Daten (Stichprobe und Zusammenfassung) für einen Knoten, der durch den Eingabeparameter des Knotenschlüssels angegeben ist, werden abgerufen. Informationen wie die Knoten-UUID, der Zeitraum, eine Zusammenfassung der IOPS, des Durchsatzes, der Latenz und der Performance, die Anzahl der erfassten Stichproben und die prozentuale Auslastung werden zurückgegeben.
GET	/datacenter/cluster/nodes/analytics	Es werden Performance-Metriken auf hoher Ebene für alle Knoten in einem Datacenter abgerufen. Die Ergebnisse lassen sich anhand der gewünschten Kriterien filtern. Informationen wie Knoten- und Clusterschlüssel sowie Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) werden zurückgegeben.
GET	/datacenter/storage/aggregates/{key}/metrics	Ruft Performance-Daten (Stichproben und Zusammenfassung) für ein durch den Eingabeparameter des Aggregatschlüssels angegebenes Aggregat ab. Informationen wie der Zeitraum, eine Zusammenfassung der IOPS, Latenz, Durchsatz und Performance-Kapazität, die Anzahl der für jeden Zähler erfassten Stichproben und der Prozentsatz der Auslastung werden zurückgegeben.
GET	/datacenter/storage/aggregates/analytics	Ruft übergeordnete Performance-Metriken für alle Aggregate in einem Datacenter ab. Sie können Ihre Ergebnisse anhand der gewünschten Kriterien filtern. Informationen wie Aggregat- und Clusterschlüssel sowie Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) werden zurückgegeben.

HTTP-Verb	Pfad	Beschreibung

GET	`/datacenter/storage/luns/{key}/metrics`
	
	`/datacenter/storage/volumes/{key}/metrics`
		Es werden Performance-Daten (Messwerte und Zusammenfassung) für eine LUN oder eine Dateifreigabe (Volume) abgerufen, die durch den Eingabeparameter des LUN- oder Volume-Schlüssels angegeben ist. Informationen wie die Zusammenfassung der minimalen, maximalen und durchschnittlichen Werte für Lese-, Schreib- und Gesamt-IOPS, Latenz und Durchsatz sowie die Anzahl der für jeden Zähler erfassten Messwerte werden zurückgegeben.

GET	`/datacenter/storage/luns/analytics`
	
	`/datacenter/storage/volumes/analytics`
		Ruft übergeordnete Performance-Metriken für alle LUNs oder Volumes in einem Datacenter ab. Sie können Ihre Ergebnisse anhand der gewünschten Kriterien filtern. Informationen wie Storage VM- und Cluster-Schlüssel sowie Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) werden zurückgegeben.

GET	`/datacenter/svm/svms/{key}/metrics`	Ruft Performance-Daten (Stichprobe und Zusammenfassung) für eine Storage VM ab, die durch den Eingabeparameter des Storage VM-Schlüssels angegeben wird. Eine Zusammenfassung der IOPS basierend auf jedem unterstützten Protokoll, wie z. B. `nvmf, fcp, iscsi,` und `nfs`, des Durchsatzes, der Latenz und der Anzahl der erfassten Stichproben wird zurückgegeben.
GET	`/datacenter/svm/svms/analytics`	Ruft allgemeine Performance-Metriken für alle Storage VMs in einem Datacenter ab. Sie können Ihre Ergebnisse anhand der gewünschten Kriterien filtern. Die Rückgabe umfasst Informationen wie die Storage VM UUID, aggregierte IOPS, Latenz, Durchsatz und den Erfassungszeitraum (in Stunden).

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/network/ethernet/ports/{key}/metrics	Ruft die Performance-Metriken für einen bestimmten Ethernet-Port ab, der durch den Eingabeparameter des Portschlüssels angegeben wird. Wenn ein Intervall (Zeitbereich) aus dem unterstützten Bereich angegeben ist, gibt die API die akkumulierten Zähler zurück, etwa minimale, maximale und durchschnittliche Performance-Werte für diesen Zeitraum.
GET	/datacenter/network/ethernet/ports/analytics	Abgerufen werden die wichtigsten Performance Kennzahlen aller Ethernet-Ports in Ihrer Datacenter-Umgebung. Informationen wie Cluster- und Node-Schlüssel und UUID, Durchsatz, Erfassungszeitraum und Auslastungsgrad der Ports werden zurückgegeben. Die Ergebnisse können anhand der verfügbaren Parameter gefiltert werden, z. B. nach Portschlüssel, Auslastungsgrad, Cluster- und Node-Name sowie UUID.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Ruft die Performance-Kennzahlen für eine bestimmte Netzwerk-FC-Schnittstelle ab, die durch den Eingabeparameter des Schnittstellenschlüssels angegeben wird. Wenn ein Intervall (Zeitbereich) aus dem unterstützten Bereich angegeben wird, gibt die API die akkumulierten Zähler zurück, z. B. minimale, maximale und durchschnittliche Performance-Werte über den Zeitraum.
GET	/datacenter/network/fc/interfaces/analytics	Ruft die allgemeinen Performance Kennzahlen für alle Ethernet-Ports in Ihrer Datacenter-Umgebung ab. Informationen wie Cluster- und FC-Schnittstellenschlüssel und -UUID, Durchsatz, IOPS, Latenz und Storage VM werden zurückgegeben. Die Ergebnisse können anhand der verfügbaren Parameter gefiltert werden, z. B. nach Cluster- und FC-Schnittstellenname und -UUID, Storage VM, Durchsatz usw.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/network/fc/ports/{key}/metrics	Ruft die Performance Kennzahlen für einen bestimmten FC-Port ab, der durch den Eingabeparameter des Port-Key angegeben wird. Wenn ein Intervall (Zeitbereich) aus dem unterstützten Bereich angegeben wird, gibt die API die akkumulierten Zähler zurück, z. B. minimale, maximale und durchschnittliche Performance Werte über den Zeitraum.
GET	/datacenter/network/fc/ports/analytics	Es werden die wichtigsten Performance-Kennzahlen für alle FC-Ports in Ihrer Datacenter-Umgebung abgerufen. Informationen wie Cluster- und Node-Schlüssel und -UUID, Durchsatz, Erfassungszeitraum und Auslastungsgrad der Ports werden zurückgegeben. Die Ergebnisse können anhand der verfügbaren Parameter gefiltert werden, z. B. nach Port-Schlüssel, Auslastungsgrad, Cluster- und Node-Name und -UUID usw.
GET	/datacenter/network/ip/interfaces/{key}/metrics	Ruft die Performance-Kennzahlen einer Netzwerk-IP-Schnittstelle gemäß dem Eingabeparameter des Schnittstellelschlüssels ab. Bei Angabe eines Intervalls (Zeitbereichs) aus dem unterstützten Bereich liefert die API Informationen wie die Anzahl der Messwerte, akkumulierte Zählerstände, den Durchsatz sowie die Anzahl der empfangenen und gesendeten Pakete.
GET	/datacenter/network/ip/interfaces/analytics	Die wichtigsten Performance-Kennzahlen aller Netzwerk-IP-Schnittstellen in Ihrer Datacenter-Umgebung werden abgerufen. Informationen wie der Cluster- und IP-Schnittstellen-Schlüssel und die UUID sowie Durchsatz, IOPS und Latenz werden zurückgegeben. Das Ergebnis lässt sich anhand der verfügbaren Parameter filtern, z. B. nach Cluster- und IP-Schnittstellenname und UUID, IOPS, Latenz, Durchsatz usw.

Aufträge und Systemdetails können über APIs in Active IQ Unified Manager angezeigt werden

Sie können die `jobs` API in der `management-server` Kategorie verwenden, um die Ausführungsdetails asynchroner Operationen anzuzeigen. Die `system` API in der `management-server` Kategorie ermöglicht Ihnen die Anzeige der Instanzdetails in Ihrer Active IQ Unified Manager Umgebung.

Jobs anzeigen

In Active IQ Unified Manager werden Vorgänge wie das Hinzufügen und Ändern von Ressourcen über synchrone und asynchrone API-Aufrufe ausgeführt. Aufrufe, die zur asynchronen Ausführung geplant sind, lassen sich über ein für diesen Aufruf erstelltes Job-Objekt nachverfolgen. Jedes Job-Objekt besitzt einen eindeutigen Schlüssel zur Identifizierung. Jedes Job-Objekt gibt die Job-Objekt-URI zurück, über die auf den Job zugegriffen und sein Fortschritt verfolgt werden kann. Mit dieser API lassen sich die Details jeder Ausführung abrufen.

Mithilfe dieser API können Sie alle Jobobjekte Ihres Datacenter einschließlich historischer Daten abfragen. Standardmäßig werden bei einer Abfrage aller Jobs die Details der letzten 20 Jobs angezeigt, die über die Web-Oberfläche und die API-Schnittstelle ausgelöst wurden. Die integrierten Filter können zum Anzeigen bestimmter Jobs verwendet werden. Sie können auch den Job key verwenden, um die Details eines bestimmten Jobs abzufragen und die nächsten Operationen auf den Ressourcen auszuführen.

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/jobs`	Gibt die Job-Details aller Jobs zurück. Ohne Sortierung wird das zuletzt übermittelte Job-Objekt oben angezeigt.
Management-Server	GET	`/management-server/jobs/{key}` Zum Anzeigen der spezifischen Details dieses Jobs den Job-Schlüssel des Job-Objekts eingeben.	Gibt die Details des spezifischen Job-Objekts zurück.

Systemdetails anzeigen

Mithilfe der `/management-server/system` API können Sie die instanzspezifischen Details Ihrer Unified Manager Umgebung abfragen. Die API liefert Informationen über das Produkt und die Services, wie z. B. die auf Ihrem System installierte Version von Unified Manager, die UUID, den Herstellernamen, das Host-Betriebssystem sowie Namen, Beschreibung und Status der auf der Unified Manager Instanz ausgeführten Services.

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/system`	Für die Ausführung dieser API sind keine Eingabeparameter erforderlich. Standardmäßig gibt das System die Systemdetails der aktuellen Unified Manager Instanz zurück.

Verwaltung von Ereignissen und Warnmeldungen mithilfe von APIs in Active IQ Unified Manager

Die APIs `events`, `alerts` und `scripts` in der Kategorie `management-server` ermöglichen Ihnen, die Ereignisse, Warnungen und die mit den Warnungen verbundenen Skripte in Ihrer Active IQ Unified Manager Umgebung zu managen.

Ereignisse anzeigen und ändern

Unified Manager empfängt die Ereignisse, die auf ONTAP für die von Unified Manager überwachten und verwalteten Cluster generiert werden. Mithilfe dieser APIs können Sie die für Ihre Cluster generierten Ereignisse anzeigen, beheben und aktualisieren.

Durch Ausführen der `GET`Methode für die `/management-server/events`API lassen sich die Ereignisse in Ihrem Datacenter einschließlich historischer Daten abfragen. Mit den integrierten Filtern wie Name, Impact-Level, Impact-Bereich, Schweregrad, Status, Ressourcenname und Ressourcentyp lassen sich bestimmte Ereignisse anzeigen. Die Parameter für Ressourcentyp und Bereich geben Informationen über das Storage Objekt zurück, auf dem das Ereignis aufgetreten ist, und der Impact-Bereich gibt Informationen über das Problem zurück, für das das Ereignis ausgelöst wird, z. B. Verfügbarkeit, Kapazität, Konfiguration, Sicherheit, Schutz und Performance.

Durch Ausführen des PATCH-Vorgangs für diese API können Sie den Workflow zur Behebung des Ereignisses aktivieren. Sie können ein Ereignis sich selbst oder einem anderen Benutzer zuweisen und den Empfang des Ereignisses bestätigen. Nachdem Sie die Schritte auf den Ressourcen zur Behebung des Problems durchgeführt haben, das das Ereignis ausgelöst hat, können Sie diese API verwenden, um das Ereignis als gelöst zu markieren.

Weitere Informationen zu Ereignissen finden Sie unter "Informationen zu Active IQ Plattformereignissen".

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/events /management-server/events/{key}`	Wenn Sie die Methode „Get ALL“ ausführen, enthält der Antworttext die Ereignisdetails aller Ereignisse in Ihrem Datacenter. Wenn Sie die Ereignisdetails anhand eines bestimmten Schlüssels abrufen, können Sie die Details eines bestimmten Ereignisses anzeigen und die nächsten Operationen für die Ressourcen ausführen. Der Antworttext enthält die Details dieses Ereignisses.
Management-Server	PATCH	`management-server/events/{key}`	Mit dieser API lässt sich ein Ereignis zuweisen oder der Status in „Bestätigt“ oder „Abgeschlossen“ ändern. Diese Methode kann auch verwendet werden, um das Ereignis Ihnen selbst oder einem anderen Benutzer zuzuweisen. Es handelt sich um einen synchronen Vorgang.

Benachrichtigungen verwalten

Ereignisse werden automatisch und kontinuierlich generiert. Unified Manager generiert eine Warnung nur dann, wenn ein Ereignis bestimmte Filterkriterien erfüllt. Sie können die Ereignisse auswählen, für die Warnungen generiert werden sollen. Mithilfe der `/management-server/alerts` API lassen sich Warnungen so konfigurieren, dass automatisch Benachrichtigungen gesendet werden, wenn bestimmte Ereignisse oder Ereignisse bestimmter Schweregrade auftreten.

Weitere Informationen zu Warnmeldungen finden Sie unter "Informationen zu Benachrichtigungen".

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/alerts` `/management-server/alerts/{key}`	Sie können mithilfe des Warnungsschlüssels alle vorhandenen Warnmeldungen in Ihrer Umgebung oder eine bestimmte Warnmeldung abfragen. Sie können Informationen zu den in Ihrer Umgebung generierten Warnmeldungen anzeigen, z. B. die Beschreibung der Warnmeldung, die Aktion, die E-Mail-Adresse, an die die Benachrichtigung gesendet wird, sowie Ereignis und Schweregrad.
Management-Server	POST	`/management-server/alerts`	Mit dieser Methode können Sie Warnungen für bestimmte Ereignisse hinzufügen. Sie müssen den Warnungsnamen, die physische oder logische Ressource bzw. das Ereignis, für das die Warnung gilt, den Aktivierungsstatus der Warnung und die Verwendung von SNMP-Traps angeben. Optional können Sie weitere Details hinzufügen, für die die Warnung ausgelöst werden soll, z. B. die Aktion, die E-Mail-Adresse für Benachrichtigungen, die Skriptdetails (falls Sie ein Warnungsskript verwenden) usw.

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	PATCH und DELETE	`management-server/events/{key}`	Mithilfe dieser Methoden können Sie bestimmte Benachrichtigungen bearbeiten und löschen. Sie können verschiedene Attribute ändern, z. B. Beschreibung, Name sowie die Aktivierung und Deaktivierung der Benachrichtigung. Sie können eine Benachrichtigung löschen, sobald sie nicht mehr benötigt wird.

Beachten Sie bei der Auswahl einer Ressource zum Hinzufügen einer Warnung, dass die Auswahl eines Clusters als Ressource nicht automatisch die Storage Objekte innerhalb dieses Clusters auswählt. Wenn Sie beispielsweise eine Warnung für alle kritischen Ereignisse aller Cluster erstellen, erhalten Sie nur Warnungen für kritische Clusterereignisse. Sie erhalten keine Warnungen für kritische Ereignisse auf Knoten, Aggregaten usw.

Skripte managen

Mithilfe der `/management-server/scripts`API können Sie eine Warnung mit einem Skript verknüpfen, das bei Auslösung der Warnung ausgeführt wird. Skripte ermöglichen die automatische Änderung oder Aktualisierung mehrerer Storage Objekte in Unified Manager. Das Skript ist einer Warnung zugeordnet. Wenn ein Ereignis eine Warnung auslöst, wird das Skript ausgeführt. Sie können benutzerdefinierte Skripte hochladen und ihre Ausführung testen, wenn eine Warnung generiert wird. Sie können eine Warnung mit Ihrem Skript verknüpfen, sodass das Skript ausgeführt wird, wenn in Unified Manager für ein Ereignis eine Warnung ausgelöst wird.

Weitere Informationen zu Skripten finden Sie unter "Skripte managen".

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/scripts`	Mit dieser API lassen sich alle vorhandenen Skripte in Ihrer Umgebung abfragen. Mit den Standardfilter- und Sortierfunktionen lassen sich nur bestimmte Skripte anzeigen.
Management-Server	POST	`/management-server/scripts`	Mit dieser API kann eine Beschreibung für das Skript hinzugefügt und die mit einer Warnung verknüpfte Skriptdatei hochgeladen werden.

Arbeitslasten verwalten

Speicherworkloads mithilfe von APIs in Active IQ Unified Manager anzeigen

Die hier aufgeführten APIs ermöglichen die Anzeige einer konsolidierten Liste von Storage Workloads für alle ONTAP Cluster in Ihrem Datacenter. Die APIs bieten außerdem eine Übersicht über die Anzahl der in Ihrer Active IQ Unified Manager Umgebung provisionierten Storage Workloads sowie über deren Kapazitäts- und Performance-Statistiken (IOPS).

Storage Workloads anzeigen

Sie können die folgende Methode verwenden, um alle Storage Workloads in allen Clustern in Ihrem Datacenter anzuzeigen. Informationen zum Filtern der Antwort anhand bestimmter Spalten finden Sie in der API-Referenzdokumentation Ihrer Unified Manager Instanz.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/workloads`

Zusammenfassung der Storage Workloads anzeigen

Mit der folgenden Methode können die genutzte Kapazität, die verfügbare Kapazität, die genutzten IOPS, die verfügbaren IOPS sowie die Anzahl der von jedem Performance Service Level gemanagten Storage Workloads bewertet werden. Die angezeigten Storage Workloads können sich auf beliebige LUNs, NFS-Dateifreigaben oder CIFS-Freigaben beziehen. Die API bietet eine Übersicht über die Storage Workloads, eine Übersicht über die vom Unified Manager provisionierten Storage Workloads, eine Datacenter Übersicht sowie eine Übersicht über den gesamten, genutzten und verfügbaren Speicherplatz und die IOPS im Datacenter in Bezug auf die zugewiesenen Performance Service Levels. Die als Antwort auf diese API empfangenen Informationen werden zum Ausfüllen des Dashboards in der Unified Manager Benutzeroberfläche verwendet.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/workloads-summary`

Verwaltung von Zugriffsendpunkten mithilfe von APIs in Active IQ Unified Manager

Sie müssen Zugriffsendpunkte oder logische Schnittstellen (LIFs) erstellen, die für die Provisionierung von Storage Virtual Machines (SVMs), LUNs und Dateifreigaben erforderlich sind. In Ihrer Active IQ Unified Manager Umgebung können Sie die Zugriffsendpunkte für die SVMs, LUNs oder Dateifreigaben anzeigen, erstellen, ändern und löschen.

Zugriffsendpunkte anzeigen

Eine Liste der Zugriffs-Endpunkte in Ihrer Unified Manager Umgebung kann mit der folgenden Methode angezeigt werden. Zum Abfragen einer Liste von Zugriffs-Endpunkten einer bestimmten SVM, LUN oder Dateifreigabe ist die Eingabe der eindeutigen Kennung für die SVM, LUN oder Dateifreigabe erforderlich. Außerdem kann der eindeutige Schlüssel des Zugriffs-Endpunkts eingegeben werden, um die Details des jeweiligen Zugriffs-Endpunkts abzurufen.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

Zugriffsendpunkte hinzufügen

Sie können benutzerdefinierte Zugriffsendpunkte erstellen und ihnen die erforderlichen Eigenschaften zuweisen. Als Eingabeparameter sind die Details des Zugriffsendpunkts anzugeben, den Sie erstellen möchten. Für die Erstellung eines Zugriffsendpunkts auf jedem Node können diese API, der System Manager oder die ONTAP CLI verwendet werden. Sowohl IPv4- als auch IPv6-Adressen werden für die Erstellung von Zugriffsendpunkten unterstützt.

> Für die erfolgreiche Provisionierung von LUNs und Dateifreigaben müssen Sie Ihre SVM mit einer Mindestanzahl an Zugriffspunkten pro Knoten konfigurieren. Sie sollten Ihre SVM mit mindestens zwei Zugriffspunkten pro Knoten konfigurieren, von denen einer das CIFS- und/oder NFS-Protokoll und der andere das iSCSI- oder FCP-Protokoll unterstützt.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/access-endpoints`

Zugriffs-Endpunkte löschen

Ein bestimmter Zugriffsendpunkt kann mit der folgenden Methode gelöscht werden. Zum Löschen eines bestimmten Zugriffsendpunkts muss der Schlüssel des Zugriffsendpunkts als Eingabeparameter angegeben werden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	LÖSCHEN	`/storage-provider/access-endpoints/{key}`

Zugriffsendpunkte ändern

Sie können einen Zugriffsendpunkt ändern und seine Eigenschaften aktualisieren, indem Sie die folgende Methode verwenden. Sie müssen den Schlüssel des Zugriffs-Endpunkts angeben, um einen bestimmten Zugriffsendpunkt zu ändern. Außerdem müssen Sie die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/access-endpoints/{key}`

Verwalten von Active Directory Zuordnungen mithilfe von APIs in Active IQ Unified Manager

Mithilfe der hier aufgeführten APIs können Sie die Active Directory-Zuordnungen auf den SVMs managen, die für die Provisionierung von CIFS-Freigaben auf den SVMs

erforderlich sind. Active Directory-Zuordnungen müssen für die Zuordnung der SVMs mit ONTAP konfiguriert werden.

Anzeigen von Active Directory-Zuordnungen

Die Konfigurationsdetails der Active Directory-Zuordnungen für eine SVM lassen sich mit der folgenden Methode anzeigen. Zum Anzeigen der Active Directory-Zuordnungen auf einer SVM ist die Eingabe des SVM-Schlüssels erforderlich. Zum Abfragen der Details einer bestimmten Zuordnung ist die Eingabe des Zuordnungsschlüssels erforderlich.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

Hinzufügen der Active Directory Zuordnung

Sie können Active Directory-Zuordnungen auf einer SVM mit der folgenden Methode erstellen. Sie müssen die Zuordnungsdetails als Eingabeparameter angeben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/active-directories-mappings`

Dateifreigaben können mithilfe von APIs in Active IQ Unified Manager verwaltet werden

Mit der `/storage-provider/file-shares`API können Sie die CIFS- und NFS-Dateifreigabe-Volumes in Ihrer Datacenter-Umgebung anzeigen, hinzufügen, ändern und löschen.

Vor der Provisionierung der Dateifreigabevolumes ist sicherzustellen, dass die SVM erstellt und mit den unterstützten Protokollen provisioniert wurde. Wenn bei der Provisionierung Performance Service Levels (PSLs) oder Storage Efficiency Policies (SEPs) zugewiesen werden, sollten die PSLs bzw. SEPs vor dem Erstellen der Dateifreigaben erstellt werden.

Dateifreigaben anzeigen

Mit der folgenden Methode lassen sich die in Ihrer Unified Manager Umgebung verfügbaren Dateifreigabe-Volumes anzeigen. Wenn Sie einen ONTAP Cluster als Datenquelle in Active IQ Unified Manager hinzugefügt haben, werden die Storage-Workloads dieser Cluster Ihrer Unified Manager Instanz automatisch hinzugefügt. Diese API ruft die Dateifreigaben ab, die Ihrer Unified Manager Instanz automatisch und manuell hinzugefügt wurden. Die Details einer bestimmten Dateifreigabe lassen sich anzeigen, indem diese API mit dem Dateifreigabeschlüssel ausgeführt wird.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/file-shares`
		
		`/storage-provider/file-shares/{key}`

Dateifreigaben hinzufügen

Die folgende Methode ermöglicht das Hinzufügen von CIFS- und NFS-Dateifreigaben in Ihrer SVM. Als Eingabeparameter werden die Details der Dateifreigabe benötigt, die erstellt werden soll. Diese API kann nicht zum Hinzufügen von FlexGroup Volumes verwendet werden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/file-shares`

> Je nachdem, ob die Parameter der Zugriffssteuerungsliste (ACL) oder die Parameter der Exportrichtlinie angegeben werden, werden CIFS-Freigaben oder NFS-Dateifreigaben erstellt. Wenn Sie keine Werte für die ACL-Parameter angeben, werden keine CIFS-Freigaben erstellt, und standardmäßig werden NFS-Freigaben erstellt, die allen Zugriff gewähren.

Erstellen von Datensicherungsvolumes: Wenn Sie Dateifreigaben zu Ihrer SVM hinzufügen, ist der Typ des Volumes, das standardmäßig eingebunden wird, `rw`(Lesen/Schreiben). Für die Erstellung von Datensicherungsvolumes (DP-Volumes) ist `dp` als Wert für den `type` Parameter anzugeben.

Löschen von Dateifreigaben

Sie können die folgende Methode verwenden, um eine bestimmte Dateifreigabe zu löschen. Zum Löschen einer bestimmten Dateifreigabe müssen Sie den Dateifreigabeschlüssel als Eingabeparameter angeben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	LÖSCHEN	`/storage-provider/file-shares/{key}`

Dateifreigaben ändern

Sie können die folgende Methode verwenden, um eine Dateifreigabe zu ändern und ihre Eigenschaften zu aktualisieren.

Um eine bestimmte Dateifreigabe zu ändern, benötigen Sie den Dateifreigabeschlüssel. Zusätzlich müssen Sie die zu aktualisierende Eigenschaft sowie deren Wert angeben.

> Es ist zu beachten, dass Sie mit einem einzigen Aufruf dieser API nur eine Eigenschaft aktualisieren können. Für mehrere Aktualisierungen muss diese API entsprechend oft ausgeführt werden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/file-shares/{key}`

Verwaltung von LUNs mithilfe von APIs in Active IQ Unified Manager

Mit der `/storage-provider/luns` API können Sie die LUNs in Ihrer Datacenter-Umgebung anzeigen, hinzufügen, ändern und löschen.

Vor der Provisionierung der LUNs ist sicherzustellen, dass die SVM erstellt und mit den unterstützten Protokollen provisioniert wurde. Wenn bei der Provisionierung Performance Service Levels (PSLs) oder Storage Efficiency Policies (SEPs) zugewiesen werden, sollten die PSLs bzw. SEPs vor der Erstellung der LUN erstellt werden.

LUNs anzeigen

Mit der folgenden Methode lassen sich die LUNs in Ihrer Unified Manager Umgebung anzeigen. Wenn Sie einen ONTAP Cluster als Datenquelle in Active IQ Unified Manager hinzugefügt haben, werden die Storage Workloads für diese Cluster automatisch Ihrer Unified Manager Instanz hinzugefügt. Diese API ruft alle LUNs ab, die Ihrer Unified Manager Instanz automatisch und manuell hinzugefügt wurden. Die Details einer bestimmten LUN lassen sich anzeigen, indem diese API mit dem LUN Schlüssel ausgeführt wird.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/luns`
		
		`/storage-provider/luns/{key}`

LUNs hinzufügen

Sie können die folgende Methode verwenden, um Ihren SVMs LUNs hinzuzufügen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/luns`

Wenn Sie in Ihrer cURL-Anfrage einen Wert für den optionalen Parameter volume_name_tag in der Eingabe angeben, wird dieser Wert bei der Benennung des Volumes während der LUN-Erstellung verwendet. Dieses Tag erleichtert die Suche nach dem Volume. Wenn Sie den Volume-Schlüssel in der Anfrage angeben, wird die Tag-Vergabe übersprungen.

LUNs löschen

Sie können die folgende Methode verwenden, um eine bestimmte LUN zu löschen. Sie müssen den LUN-Schlüssel angeben, um eine bestimmte LUN zu löschen.

Wenn Sie in ONTAP ein Volume erstellt und anschließend über Unified Manager LUNs auf diesem Volume bereitgestellt haben, wird beim Löschen aller LUNs mithilfe dieser API auch das Volume aus dem ONTAP Cluster gelöscht.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	LÖSCHEN	`/storage-provider/luns/{key}`

LUNs modifizieren

Sie können die folgende Methode verwenden, um eine LUN zu ändern und ihre Eigenschaften zu aktualisieren. Sie müssen den LUN-Schlüssel angeben, um eine bestimmte LUN zu ändern. Außerdem müssen Sie die LUN-Eigenschaft, die Sie aktualisieren möchten, sowie ihren Wert eingeben. Für die Aktualisierung von LUN-Arrays mithilfe dieser API sollten Sie die Empfehlungen unter “Empfehlungen für die Verwendung der APIs” beachten.

Sie können mit einem einzigen Aufruf dieser API nur eine Eigenschaft aktualisieren. Für mehrere Aktualisierungen müssen Sie die API entsprechend oft ausführen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/luns/{key}`

Verwaltung von Performance Service Levels mithilfe von APIs in Active IQ Unified Manager

Sie können Performance Service Levels mithilfe der Storage Provider APIs auf Ihrem Active IQ Unified Manager anzeigen, erstellen, ändern und löschen.

Performance Service Levels anzeigen

Mit der folgenden Methode lassen sich die Performance Service Levels anzeigen, um sie Storage Workloads zuzuweisen. Die API listet alle systemdefinierten und benutzererstellten Performance Service Levels auf und ruft die Attribute aller Performance Service Levels ab. Wenn ein bestimmtes Performance Service Level abgefragt werden soll, muss die eindeutige ID des Performance Service Levels eingegeben werden, um dessen Details abzurufen.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

Hinzufügen von Performance Service Levels

Sie können die folgende Methode verwenden, um benutzerdefinierte Performance Service Levels zu erstellen und sie Ihren Storage Workloads zuzuweisen, wenn die systemdefinierten Performance Service Levels die erforderlichen Service Level Objectives (SLOs) für die Storage Workloads nicht erfüllen. Anschließend erfolgt die Eingabe der Details für das Performance Service Level, das erstellt werden soll. Bei den IOPS-Eigenschaften muss ein gültiger Wertebereich eingegeben werden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/performance-service-levels`

Löschen von Performance Service Levels

Sie können mit der folgenden Methode ein bestimmtes Performance Service Level löschen. Ein Performance Service Level kann nicht gelöscht werden, wenn es einer Workload zugewiesen ist oder wenn es das einzige verfügbare Performance Service Level ist. Zum Löschen eines bestimmten Performance Service Level müssen Sie dessen eindeutige ID als Eingabeparameter angeben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	LÖSCHEN	`/storage-provider/performance-service-levels/{key}`

Performance Service Levels ändern

Sie können die folgende Methode verwenden, um ein Performance Service Level zu ändern und dessen Eigenschaften zu aktualisieren. Systemdefinierte oder einem Workload zugewiesene Performance Service Level können nicht geändert werden. Um ein bestimmtes Performance Service Level zu ändern, benötigen Sie die eindeutige ID. Außerdem müssen Sie die zu aktualisierende IOPS-Eigenschaft sowie einen gültigen Wert angeben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/performance-service-levels/{key}`

Anzeige der Aggregate-Funktionen basierend auf Performance Service Levels

Sie können die folgende Methode verwenden, um die Aggregatfunktionen basierend auf Performance Service Levels abzufragen. Diese API gibt die Liste der in Ihrem Datacenter verfügbaren Aggregate zurück und zeigt die Funktionen im Hinblick auf die Performance Service Levels an, die von diesen Aggregaten unterstützt werden können. Bei der Provisionierung von Workloads auf einem Volume können Sie die Fähigkeit eines Aggregats anzeigen, ein bestimmtes Performance Service Level zu unterstützen, und Workloads auf der Grundlage dieser Fähigkeit provisionieren. Die Möglichkeit, das Aggregat anzugeben, ist nur verfügbar, wenn Sie einen Workload mithilfe von APIs provisionieren. Diese Funktionalität ist in der Unified Manager web UI nicht verfügbar.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

Verwaltung von Speichereffizienzrichtlinien mithilfe von APIs in Active IQ Unified Manager

Sie können Speichereffizienzrichtlinien mithilfe der Storage APIs des Speicheranbieters anzeigen, erstellen, ändern und löschen.

Folgende Punkte sind zu beachten:

- Es ist nicht zwingend erforderlich, beim Erstellen einer Arbeitslast auf Unified Manager eine Speichereffizienzrichtlinie zuzuweisen.
- Eine Storage-Effizienzrichtlinie kann nicht von einer Arbeitslast entfernt werden, nachdem ihr eine Richtlinie zugewiesen wurde.
- Wenn für einen Workload bestimmte Storage Einstellungen auf ONTAP Volumes festgelegt sind, wie z. B. Deduplizierung und Komprimierung, können diese Einstellungen durch die in der Storage Efficiency Policy angegebenen Einstellungen überschrieben werden, die Sie beim Hinzufügen der Storage Workloads in Unified Manager anwenden.

Anzeigen von Storage-Effizienzrichtlinien

Sie können die Speichereffizienzrichtlinien mithilfe der folgenden Methode anzeigen, bevor Sie sie Storage Workloads zuweisen. Diese API listet alle systemdefinierten und benutzerdefinierten Speichereffizienzrichtlinien auf und ruft deren Attribute ab. Um eine bestimmte Speichereffizienzrichtlinie abzufragen, müssen Sie deren eindeutige ID eingeben, um deren Details abzurufen.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

Hinzufügen von Storage-Effizienzrichtlinien

Mit der folgenden Methode lassen sich benutzerdefinierte Speichereffizienzrichtlinien erstellen und Ihren Storage-Workloads zuweisen, wenn die systemdefinierten Richtlinien die Anforderungen an die Provisionierung Ihrer Storage-Workloads nicht erfüllen. Als Eingabeparameter dienen die Details der Speichereffizienzrichtlinie, die erstellt werden soll.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/storage-efficiency-policies`

Storage-Effizienzrichtlinien löschen

Mit der folgenden Methode kann eine bestimmte Storage Efficiency Policy gelöscht werden. Eine Storage Efficiency Policy kann nicht gelöscht werden, wenn sie einem Workload zugewiesen ist oder wenn sie die einzige verfügbare Storage Efficiency Policy ist. Zum Löschen einer bestimmten Storage Efficiency Policy muss ihre eindeutige ID als Eingabeparameter angegeben werden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	LÖSCHEN	`/storage-provider/storage-efficiency-policies/{key}`

Storage-Effizienzrichtlinien ändern

Sie können die folgende Methode verwenden, um eine Storage Efficiency Policy zu ändern und ihre Eigenschaften zu aktualisieren. Eine Storage Efficiency Policy, die systemdefiniert ist oder einem Workload zugewiesen wurde, kann nicht geändert werden. Um eine bestimmte Storage Efficiency Policy zu ändern, müssen Sie die eindeutige ID der Storage Efficiency Policy angeben. Zusätzlich müssen Sie die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert angeben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/storage-efficiency-policies/{key}`

Gängige Arbeitsabläufe für das Storage Management

Informationen zu gängigen API-Workflows für die Speicherverwaltung in Active IQ Unified Manager

Die gängigen Workflows bieten Entwicklern von Client-Applikationen Beispiele dafür, wie Active IQ Unified Manager APIs von einer Client-Applikation aufgerufen werden können, um gängige Storage-Managementfunktionen auszuführen. Dieser Abschnitt enthält einige dieser Beispiel-Workflows.

Die Workflows beschreiben einige der häufig verwendeten Anwendungsfälle für das Storage-Management sowie Beispielcode zur Verwendung. Jede Aufgabe wird anhand eines Workflow-Prozesses beschrieben, der aus einem oder mehreren API-Aufrufen besteht.

Die in den Workflows verwendeten API-Aufrufe verstehen

Sie können von Ihrer Unified Manager Instanz aus die Seite der Online-Dokumentation anzeigen, die die Details zu jedem REST API-Aufruf enthält. Dieses Dokument wiederholt die Details der Online-Dokumentation nicht. Jeder API-Aufruf, der in den Workflow-Beispielen in diesem Dokument verwendet wird, enthält nur die Informationen, die Sie benötigen, um den Aufruf auf der Dokumentationsseite zu finden. Nachdem Sie einen bestimmten API-Aufruf gefunden haben, können Sie die vollständigen Details des Aufrufs prüfen, einschließlich der Eingabeparameter, Ausgabeformate, HTTP-Statuscodes und des Typs der Anfrageverarbeitung.

Die folgenden Informationen sind für jeden API-Aufruf innerhalb eines Workflows enthalten, um den Aufruf auf der Dokumentationsseite zu finden:

- Kategorie: Die API-Aufrufe sind auf der Dokumentationsseite in funktional verwandte Bereiche oder Kategorien unterteilt. Ein bestimmter API-Aufruf kann durch Scrollen zum Seitenende und Klicken auf die entsprechende API-Kategorie gefunden werden.
- HTTP-Verb (Aufruf): Das HTTP-Verb identifiziert die Aktion, die an einer Ressource ausgeführt wird. Jeder API-Aufruf wird über ein einzelnes HTTP-Verb ausgeführt.
- Pfad: Der Pfad bestimmt die spezifische Ressource, auf die sich die Aktion im Rahmen eines Aufrufs

bezieht. Die Pfadzeichenfolge wird an die Core-URL angehängt, um die vollständige URL zu bilden, die die Ressource identifiziert.

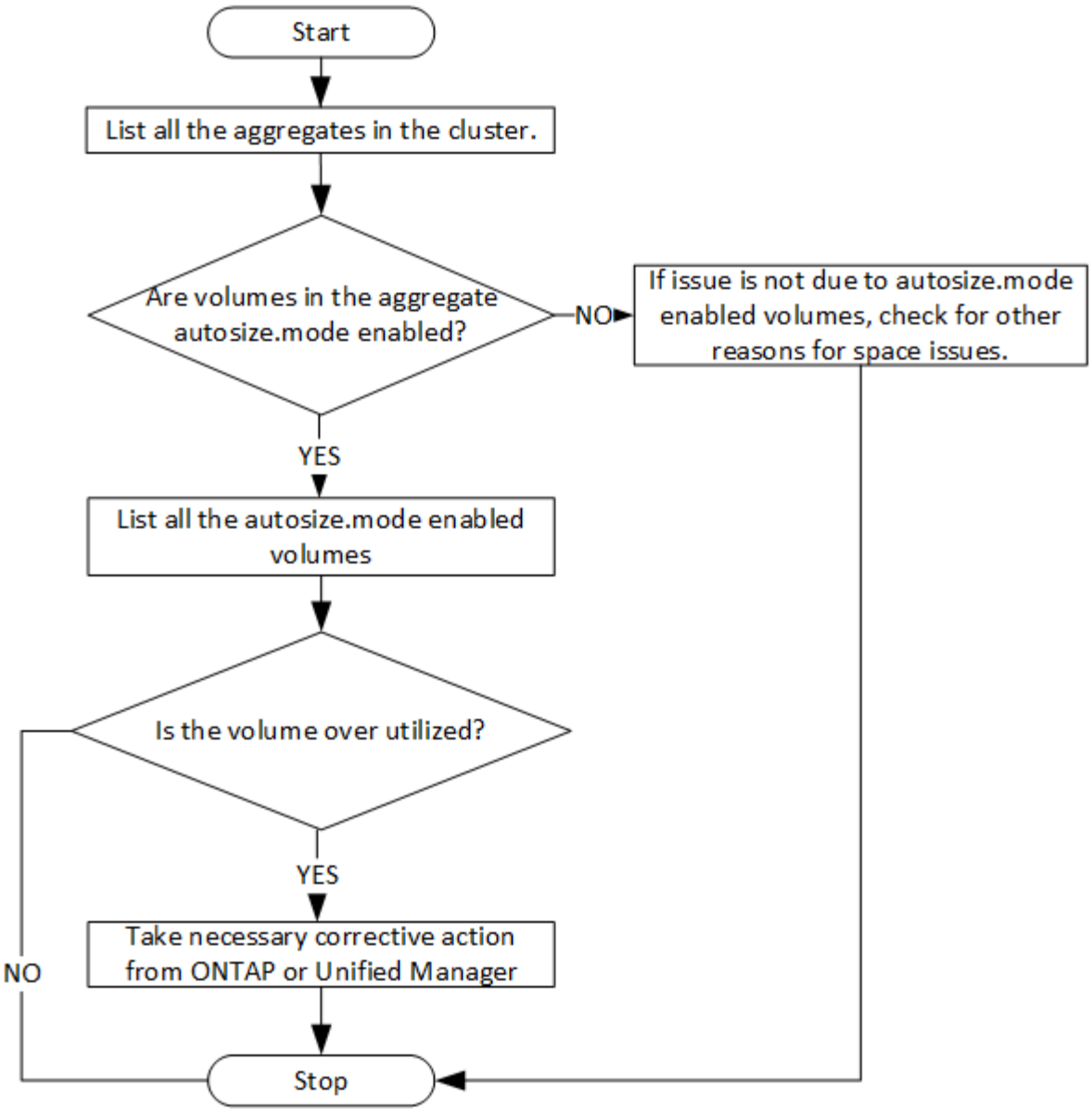
Ermittlung von Speicherplatzproblemen in Aggregaten mithilfe der Active IQ Unified Manager APIs

Mit den Datacenter-APIs in Active IQ Unified Manager kann die Verfügbarkeit und Auslastung des Speicherplatzes in Ihren Volumes überwacht werden. Speicherplatzprobleme in Ihren Volumes können ermittelt und über- oder unterausgelastete Storage-Ressourcen identifiziert werden.

Die Datacenter-APIs für Aggregate rufen die relevanten Informationen über verfügbaren und belegten Speicherplatz sowie Einstellungen zur Speichereffizienz ab. Sie können die abgerufenen Informationen auch anhand bestimmter Attribute filtern.

Eine Möglichkeit, Speicherplatzmangel in Ihren Aggregaten festzustellen, besteht darin, zu überprüfen, ob in Ihrer Umgebung Volumes mit aktiviertem Modus für die automatische Größenanpassung vorhanden sind. Anschließend folgt die Identifizierung der Volumes, die übermäßig ausgelastet sind, sowie gegebenenfalls die Durchführung von Korrekturmaßnahmen.

Das folgende Flussdiagramm veranschaulicht den Prozess des Abrufens von Informationen über Volumes mit aktivierter automatischer Größenanpassung:



Dieser Ablauf setzt voraus, dass die Cluster bereits in ONTAP erstellt und zu Unified Manager hinzugefügt wurden.

1. Ermittlung des Cluster-Schlüssels, sofern der Wert nicht bekannt ist:

Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/cluster/clusters`

2. Unter Verwendung des Cluster-Schlüssels als Filterparameter fragt die Abfrage die Aggregate auf diesem Cluster ab.

Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/storage/aggregates`

3. Anhand der Antwort ist die Speicherplatznutzung der Aggregate zu analysieren und festzustellen, welche Aggregate Speicherplatzprobleme aufweisen. Für jedes Aggregat mit Speicherplatzproblem ist der Aggregatschlüssel aus derselben JSON-Ausgabe zu ermitteln.
4. Mithilfe jedes Aggregatschlüssels werden alle Volumes gefiltert, deren Wert für den Parameter autosize.mode als `grow`.

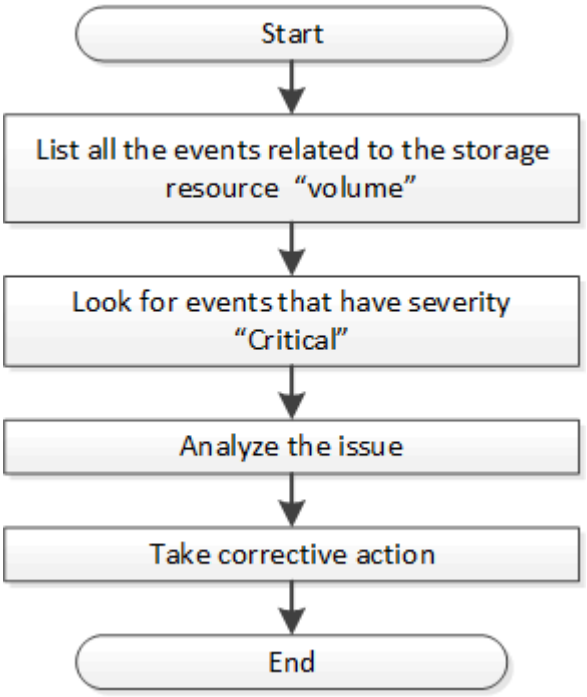
Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/storage/volumes`

5. Es erfolgt eine Analyse, welche Volumes übermäßig genutzt werden.
6. Zur Behebung der Speicherplatzprobleme in Ihrem Volume sind gegebenenfalls Korrekturmaßnahmen erforderlich, z. B. das Verschieben des Volumes auf andere Aggregate. Diese Aktionen können über ONTAP oder die Unified Manager Web-Benutzeroberfläche ausgeführt werden.

Probleme mit Speicherobjekten mithilfe der Event-APIs von Active IQ Unified Manager ermitteln

Wenn ein Storageobjekt in Ihrem Datacenter einen Schwellenwert überschreitet, erhalten Sie eine Benachrichtigung über dieses Ereignis. Mithilfe dieser Benachrichtigung können Sie das Problem analysieren und mithilfe der `events` APIs Korrekturmaßnahmen ergreifen.

Dieser Workflow verwendet das Beispiel eines Volume als Ressourcenobjekt. Mithilfe der `events` APIs können Sie die Liste der Ereignisse abrufen, die mit einem Volume verknüpft sind, die kritischen Probleme für dieses Volume analysieren und anschließend Korrekturmaßnahmen ergreifen, um das Problem zu beheben.



Mit den folgenden Schritten lassen sich die Probleme in Ihrem Volume ermitteln, bevor Korrekturmaßnahmen ergriffen werden.

Schritte

1. Analyse der kritischen Active IQ Unified Manager Ereignisbenachrichtigungen für die Volumes in Ihrem Datacenter.
2. Die Abfrage aller Ereignisse für die Volumes erfolgt mithilfe der folgenden Parameter in der API /management-server/events:
   `"resource_type": "volume"`
   `"severity": "critical"`

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	/management-server/events

3. Die Ausgabe kann angezeigt und die Probleme in den spezifischen Volumes analysiert werden.
4. Die erforderlichen Maßnahmen zur Behebung der Probleme können mithilfe der Unified Manager REST APIs oder der Web UI durchgeführt werden.

Fehlerbehebung bei ONTAP Volumes mithilfe der Active IQ Unified Manager Gateway APIs

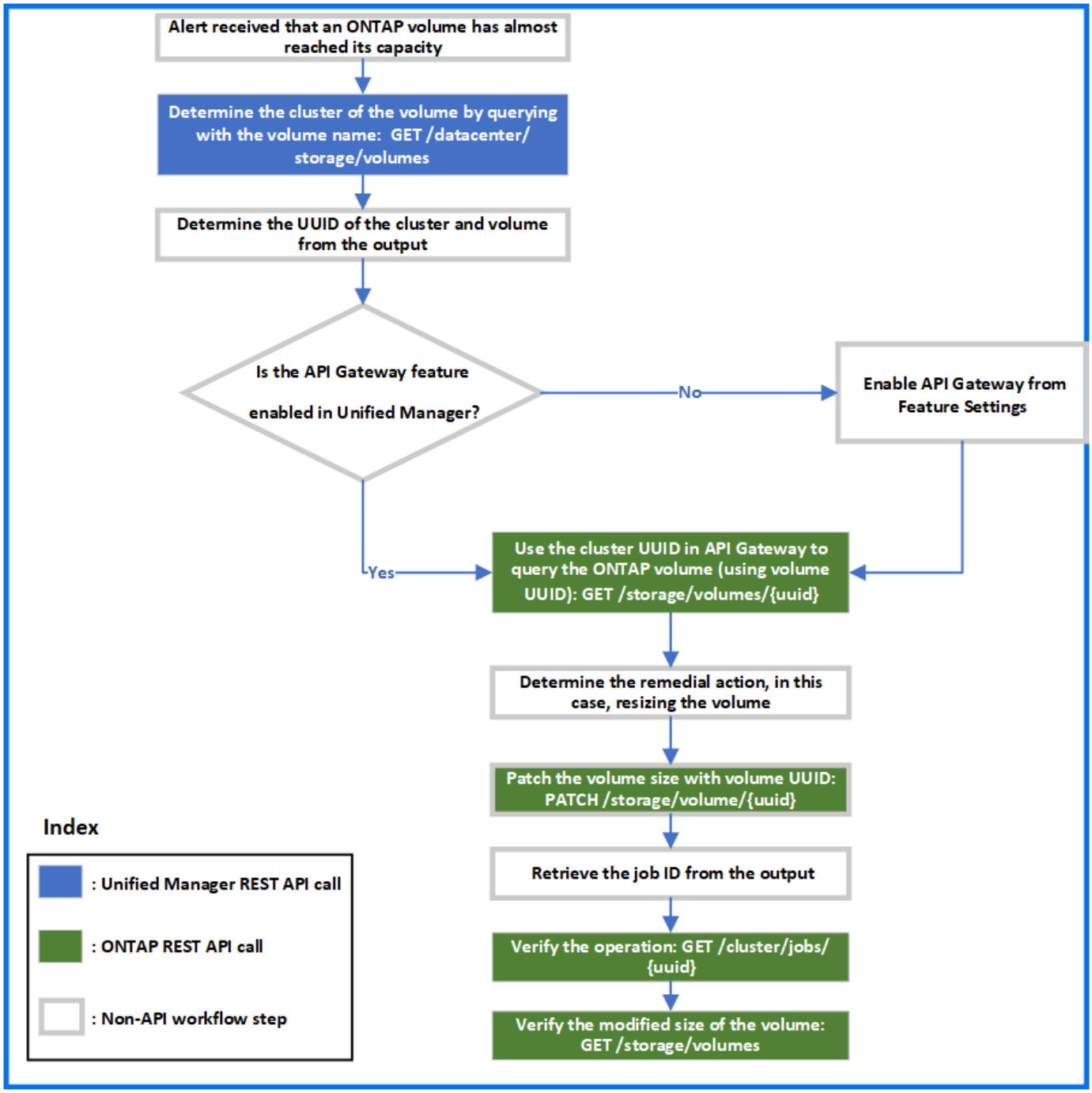
Die Gateway-APIs fungieren als Schnittstelle, um ONTAP-APIs aufzurufen, Informationen über Ihre ONTAP Storage-Objekte abzufragen und Abhilfemaßnahmen zu ergreifen, um die gemeldeten Probleme zu beheben.

Dieser Workflow behandelt einen beispielhaften Anwendungsfall, in dem ein Ereignis ausgelöst wird, wenn ein ONTAP Volume seine Kapazität fast erreicht. Der Workflow zeigt außerdem, wie dieses Problem durch den Aufruf einer Kombination aus Active IQ Unified Manager und ONTAP REST-APIs behoben werden kann.

Vor dem Ausführen der Workflow-Schritte müssen die folgenden Voraussetzungen erfüllt sein:

- Sie kennen die Gateway-APIs und deren Verwendung. Informationen dazu finden Sie unter "Zugriff auf ONTAP APIs über Proxy-Zugriff".
- Sie sind mit der Verwendung von ONTAP REST APIs vertraut. Informationen zur Verwendung von ONTAP REST APIs sind unter "ONTAP Automatisierungsdokumentation" verfügbar.
- Sie sind ein Anwendungsadministrator.
- Auf dem Cluster, auf dem Sie die REST API Vorgänge ausführen möchten, muss ONTAP 9.5 oder höher ausgeführt werden, und der Cluster muss über HTTPS zu Unified Manager hinzugefügt werden.

Das folgende Diagramm veranschaulicht jeden Schritt im Workflow zur Fehlerbehebung bei Problemen mit der Kapazitätsauslastung von ONTAP Volumes.



Der Workflow umfasst die Aufrufpunkte sowohl von Unified Manager als auch der ONTAP REST APIs.

1. Der Volumennamen aus dem Ereignis, das die Kapazitätsauslastung des Volumes meldet, ist zu beachten.
2. Für die Abfrage des Volume mit dem Volumennamen als Wert im Parameter „name“ steht die folgende Unified Manager API zur Verfügung.

Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/storage/volumes`

3. Aus der Ausgabe lassen sich die Cluster-UUID und die Volume-UUID entnehmen.

4. In der Web-Benutzeroberfläche von Unified Manager kann unter **Allgemein** > **Funktionseinstellungen** > **API Gateway** überprüft werden, ob die API Gateway Funktion aktiviert ist. Solange sie nicht aktiviert ist, stehen die APIs der Gateway Kategorie nicht zum Aufrufen zur Verfügung. Falls die Funktion deaktiviert ist, sollte sie aktiviert werden.
5. Die Cluster-UUID ermöglicht das Ausführen der ONTAP API `/storage/volumes/{uuid}` über API gateway. Die Abfrage gibt die Volume-Details zurück, wenn die Volume-UUID als API-Parameter übergeben wird.

   Für die Ausführung der ONTAP APIs über API gateway werden die Unified Manager Anmeldeinformationen intern zur Authentifizierung übergeben, sodass kein zusätzlicher Authentifizierungsschritt für den Zugriff auf einzelne Cluster erforderlich ist.

Kategorie	HTTP-Verb	Pfad

Unified Manager: Gateway
 	
ONTAP: Storage
	GET	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP API:
		`/storage/volumes/{uuid}`

   > In /gateways/{uuid}/{path} muss der Wert für {uuid} durch die Cluster-UUID ersetzt werden, auf der die REST-Operation ausgeführt werden soll. {path} muss durch die ONTAP REST-URL /storage/volumes/{uuid} ersetzt werden.

   Die angehängte URL lautet: `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

   Beim Ausführen der GET-Operation wird folgende URL generiert:
   `GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes/{volume_uuid}`

   Beispiel für einen cURL-Befehl

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

6. Anhand der Ausgabe lassen sich Größe, Nutzung und die zu ergreifende Abhilfemaßnahme bestimmen. In diesem Workflow besteht die ergriffene Abhilfemaßnahme in der Anpassung der Größe des Volume.
7. Für die Größenanpassung des Volumes sind die Cluster UUID und die Ausführung der folgenden ONTAP API über das API Gateway erforderlich. Informationen zu den Eingabeparametern für das Gateway und die ONTAP APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Pfad

Unified Manager: Gateway
 	
ONTAP: Storage
	PATCH	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP API:
		`/storage/volumes/{uuid}`

Neben der Cluster UUID und der Volume UUID muss für die Größenänderung des Volumes ein Wert für den Parameter size eingegeben werden. Wichtig ist, dass der Wert in Byte angegeben wird. Wenn beispielsweise die Größe eines Volumes von 100 GB auf 120 GB erhöht werden soll, wird der Wert für den Parameter size am Ende der Abfrage angegeben: `-d {\"size\": 128849018880}"`

Beispiel für einen cURL-Befehl

```
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}"
```

Die JSON-Ausgabe gibt eine Job-UUID zurück.

8. Anhand der Job-UUID lässt sich überprüfen, ob der Job erfolgreich ausgeführt wurde. Die folgende ONTAP API kann über das API-Gateway mit der Cluster-UUID und der Job-UUID ausgeführt werden. Informationen zu den Eingabeparametern für das Gateway und ONTAP-APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Pfad

Unified Manager: Gateway
 	
ONTAP: Cluster
	GET	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP-API:
		`/cluster/jobs/{uuid}`

Die zurückgegebenen HTTP-Codes entsprechen den HTTP-Statuscodes der ONTAP REST API.

9. Die folgende ONTAP API dient zum Abfragen der Details des vergrößerten Volumes. Informationen zu den Eingabeparametern für das gateway und die ONTAP APIs sind in Schritt 5 enthalten.

Kategorie	HTTP-Verb	Pfad

Unified Manager: Gateway
 	
ONTAP: Storage
	GET	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP API:
		`/storage/volumes/{uuid}`

Die Ausgabe zeigt eine erhöhte Volumengröße von 120 GB an.

Workflows für das Workload-Management

Bereitstellung und Änderung von Speicherworkloads in Active IQ Unified Manager

Mit Active IQ Unified Manager können Sie Storage Workloads (LUNs, NFS-Dateifreigaben und CIFS-Freigaben) provisionieren und modifizieren. Die Provisionierung umfasst mehrere Schritte, von der Erstellung der Storage Virtual Machine (SVM) bis zur

Anwendung von Performance Service Level und Storage Efficiency Policies auf die Storage Workloads. Das Modifizieren von Workloads umfasst die Schritte zum Ändern spezifischer Parameter und zum Aktivieren zusätzlicher Funktionen für diese.

Folgende Arbeitsabläufe werden beschrieben:

- Workflow für die Provisionierung von Storage Virtual Machines (SVMs) in Unified Manager.

  Dieser Workflow muss vor der Provisionierung von LUNs oder Dateifreigaben auf Unified Manager durchgeführt werden.

- Provisionierung von Dateifreigaben.
- Provisionierung von LUNs.
- Ändern von LUNs und Dateifreigaben (anhand des Beispiels zum Aktualisieren des Parameters „Performance Service Level“ für die Storage Workloads).
- Ändern einer NFS-Dateifreigabe zur Unterstützung des CIFS-Protokolls
- Arbeitslasten ändern, um QoS auf AQoS zu aktualisieren

Für jeden Provisionierungsworkflow (LUNs und Dateifreigaben) ist der Abschluss des Workflows zur Überprüfung der SVMs auf den Clustern erforderlich.

Vor der Verwendung der einzelnen APIs in den Workflows ist außerdem die Lektüre der Empfehlungen und Einschränkungen erforderlich. Die entsprechenden Details zu den APIs sind in den jeweiligen Abschnitten der zugehörigen Konzepte und Referenzen verfügbar.

SVMs auf ONTAP Clustern mithilfe der Active IQ Unified Manager APIs überprüfen

Vor der Provisionierung von Dateifreigaben oder LUNs sollte geprüft werden, ob auf den Clustern Storage Virtual Machines (SVMs) erstellt wurden.

Der Workflow setzt voraus, dass ONTAP Cluster zu Unified Manager hinzugefügt wurden und der Clusterschlüssel abgerufen wurde. Die Cluster müssen über die erforderlichen Lizenzen für die Provisionierung von LUNs und Dateifreigaben verfügen.

1. Es ist zu prüfen, ob im Cluster eine SVM erstellt wurde.

Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/svm/svms` `/datacenter/svm/svms/{key}`

Beispiel cURL

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Wenn der SVM-Schlüssel nicht zurückgegeben wird, muss die SVM erstellt werden. Zum Erstellen der

SVMs benötigen Sie den Clusterschlüssel, auf dem Sie die SVM provisionieren. Außerdem müssen Sie den SVM-Namen angeben. Die folgenden Schritte sind auszuführen.

Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/cluster/clusters` `/datacenter/cluster/clusters/{key}`

Ermittlung des Cluster-Schlüssels.

Beispiel cURL

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

3. Der Cluster-Schlüssel aus der Ausgabe dient anschließend als Eingabe für die Erstellung der SVM.

> Beim Erstellen der SVM muss sichergestellt werden, dass sie alle für die Provisionierung von LUNs und Dateifreigaben erforderlichen Protokolle unterstützt, z. B. CIFS, NFS, FCP und iSCSI. Die Provisionierungs-Workflows können fehlschlagen, wenn die SVM die erforderlichen Services nicht unterstützt. Es wird empfohlen, die Services für die jeweiligen Workload-Typen ebenfalls auf der SVM zu aktivieren.

Kategorie	HTTP-Verb	Pfad
Datacenter	POST	`/datacenter/svm/svms`

Beispiel cURL

Die Details des SVM-Objekts sind als Eingabeparameter anzugeben.

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Content-Type: application/json" -H "Authorization:
Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": {},
\"key\": \"1cd8a442-86d1,type=objecttype,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\",
\"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-
00a0986138f7\" } ],
\"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\":
\"string\",
\"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" },
\"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-
123478563412,type=object type,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\" },
\"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ],
```

```
\"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] },
\"fcp\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true,
\"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" },
\"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\":
\"dataLif1\" } ], \"ipspace\": { \"name\": \"exchange\" },
\"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\",
\"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\",
\"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ]
},
\"name\": \"svm1\", \"nfs\": { \"enabled\": true },
\"nis\": { \"domain\": \"string\", \"enabled\": true,
\"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true },
\"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\",
\"netmask\": \"24\" }, \"gateway\": \"string\" } ],
\"snapshot_policy\": { \"name\": \"default\" },
\"state\": \"running\", \"subtype\": \"default\"}"
```

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie die von Ihnen erstellte SVM überprüfen können.

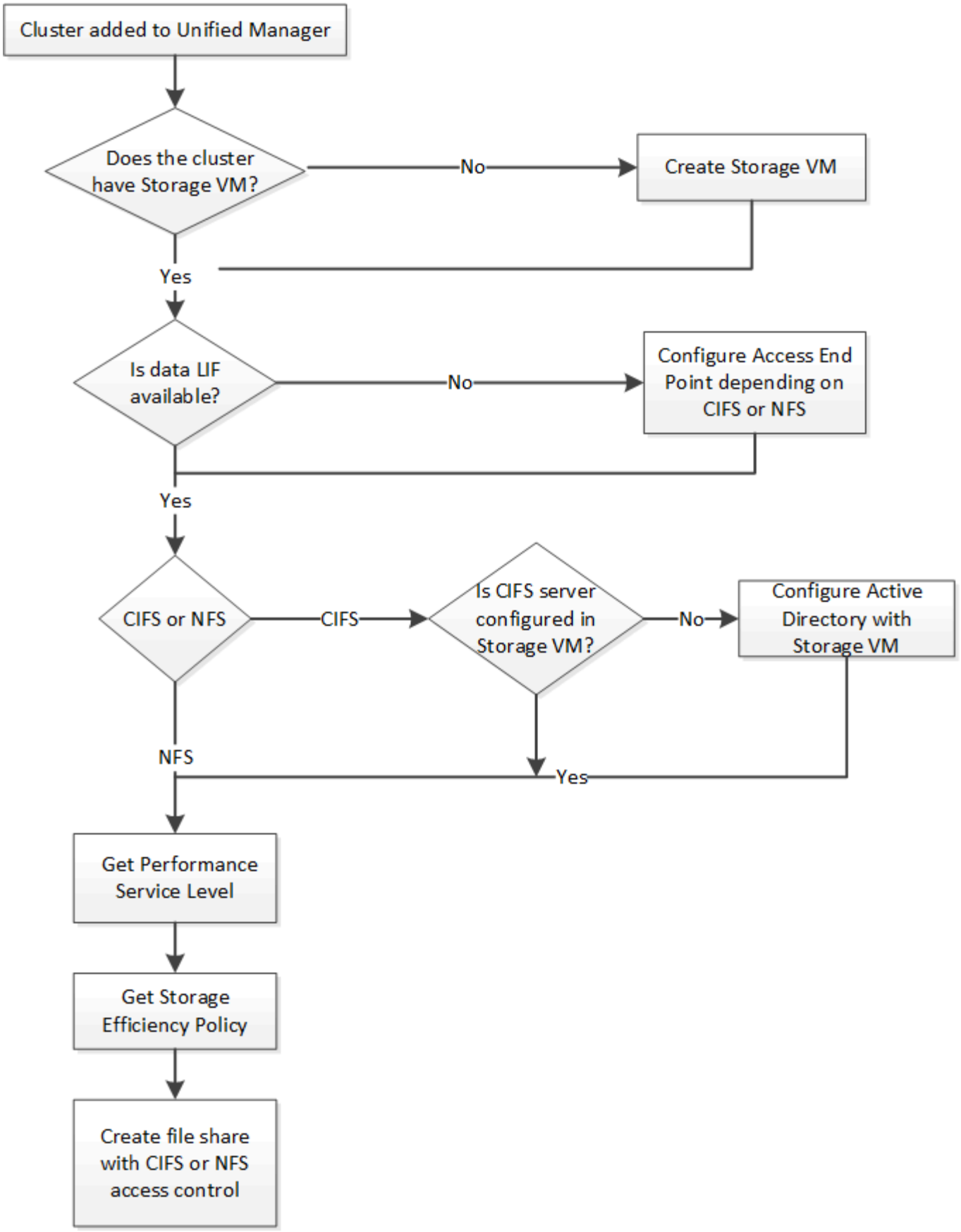
4. Die Überprüfung der SVM-Erstellung erfolgt mithilfe des Jobobjektschlüssels für die Abfrage. Bei erfolgreicher Erstellung der SVM wird der SVM-Schlüssel in der Antwort zurückgegeben.

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	`/management-server/jobs/{key}`

Bereitstellung von CIFS- und NFS-Dateifreigaben mithilfe von Active IQ Unified Manager APIs

Sie können CIFS-Freigaben und NFS-Dateifreigaben auf Ihren Storage Virtual Machines (SVMs) mithilfe der Provisionierungs-APIs provisionieren, die als Teil von Active IQ Unified Manager bereitgestellt werden. Dieser Provisionierungs-Workflow beschreibt die Schritte zum Abrufen der Schlüssel der SVMs, der Performance Service Levels und der Storage Efficiency Policies vor dem Erstellen der Dateifreigaben.

Das folgende Diagramm veranschaulicht jeden Schritt in einem Workflow zur Provisionierung von Dateifreigaben. Es umfasst die Provisionierung sowohl von CIFS-Freigaben als auch von NFS-Dateifreigaben.



Stellen Sie Folgendes sicher:

- ONTAP Cluster wurden zu Unified Manager hinzugefügt, und der Clusterschlüssel wurde abgerufen.
- Auf den Clustern wurden SVMs erstellt.
- Die SVMs unterstützen CIFS- und NFS-Services. Die Provisionierung von Dateifreigaben kann fehlschlagen, wenn die SVMs die erforderlichen Services nicht unterstützen.
- Der FCP-Port ist für die Port-Provisionierung online.

1. Es ist festzustellen, ob auf der SVM, auf der die CIFS-Freigabe erstellt werden soll, Data LIFs oder Zugriffs-Endpunkte verfügbar sind. Die Liste der auf der SVM verfügbaren Zugriffs-Endpunkte:

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/access-endpoints` `/storage-provider/access-endpoints/{key}`

Beispiel 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. Sofern Ihr Zugriffsendpunkt in der Liste verfügbar ist, erfolgt der Abruf des Schlüssels des Zugriffsendpunkts, andernfalls die Erstellung des Zugriffsendpunkts.

Es muss sichergestellt werden, dass Zugriffs-Endpunkte erstellt werden, auf denen das CIFS-Protokoll aktiviert ist. Die Provisionierung von CIFS-Freigaben schlägt fehl, wenn kein Zugriffs-Endpunkt mit aktiviertem CIFS-Protokoll erstellt wurde.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/access-endpoints`

Beispiel cURL

Sie müssen die Details des Zugriffsendpunkts, den Sie erstellen möchten, als Eingabeparameter eingeben.

```
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}"
```

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie den von Ihnen erstellten Zugriffs-Endpunkt überprüfen können.

3. Überprüfung des Zugriffs-Endpunkts:

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	`/management-server/jobs/{key}`

4. Es ist zu ermitteln, ob eine CIFS-Freigabe oder eine NFS-Dateifreigabe erstellt werden muss. Für die Erstellung von CIFS-Freigaben gelten die folgenden Unterschritte:

   a. Es ist festzustellen, ob der CIFS-Server auf Ihrer SVM konfiguriert ist, das heißt, ob auf der SVM eine Active Directory-Zuordnung eingerichtet ist.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/active-directories-mappings`

   b. Wenn die Active Directory-Zuordnung erstellt wurde, ist der Schlüssel zu verwenden, andernfalls ist die Active Directory-Zuordnung auf der SVM zu erstellen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/active-directories-mappings`

Beispiel cURL

Als Eingabeparameter sind die Details zum Erstellen der Active Directory Zuordnung anzugeben.

```
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\"}"
```

+
Dies ist ein synchroner Aufruf, und die Erstellung der Active Directory-Zuordnung lässt sich in der Ausgabe überprüfen. Im Fehlerfall wird eine Fehlermeldung angezeigt, anhand derer sich das Problem beheben und die Anfrage erneut ausführen lässt.

5. Die Ermittlung des SVM-Schlüssels für die SVM, auf der die CIFS-Freigabe oder die NFS-Dateifreigabe erstellt werden soll, erfolgt wie im Workflow-Thema *Verifying SVMs on clusters* beschrieben.
6. Den Schlüssel für das Performance Service Level erhalten Sie, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie den `system_defined` Eingabeparameter auf `true` „true“ setzen. In der Ausgabe befindet sich der Schlüssel des Performance Service Levels, das Sie auf die Dateifreigabe anwenden möchten.

7. Optional können Sie den Schlüssel der Storage Efficiency Policy, die Sie auf die Dateifreigabe anwenden möchten, abrufen, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort extrahieren.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/storage-efficiency-policies`

8. Erstellung der Dateifreigabe. Sie können eine Dateifreigabe erstellen, die sowohl CIFS als auch NFS unterstützt, indem Sie die Zugriffssteuerungsliste und die Exportrichtlinie angeben. Die folgenden Teilschritte enthalten Informationen, wenn Sie eine Dateifreigabe erstellen möchten, die auf dem Volume nur eines der Protokolle unterstützt. Sie können eine NFS-Dateifreigabe auch aktualisieren, um die Zugriffssteuerungsliste einzuschließen, nachdem Sie die NFS-Freigabe erstellt haben. Informationen dazu enthält das Thema *Modifying storage workloads*.

   a. Für die Erstellung nur einer CIFS-Freigabe werden die Informationen zur Zugriffssteuerungsliste (ACL) benötigt. Für die Erstellung der CIFS-Freigabe sind für die folgenden Eingabeparameter gültige Werte anzugeben. Für jede Benutzergruppe, die zugewiesen wird, wird beim Provisionieren einer CIFS/SMB-Freigabe eine ACL erstellt. Anhand der für ACL und Active Directory-Zuordnung eingegebenen Werte werden Zugriffskontrolle und Zuordnung für die CIFS-Freigabe bei ihrer Erstellung festgelegt.

      Ein cURL-Befehl mit Beispielwerten

```
{
  "access_control": {
```

```
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    },
```

b. Für die Erstellung nur einer NFS-Dateifreigabe sind die Informationen zur Exportrichtlinie erforderlich. Für die Erstellung der NFS-Dateifreigabe sind für die folgenden Eingabeparameter gültige Werte erforderlich. Anhand dieser Werte wird die Exportrichtlinie bei der Erstellung mit der NFS-Dateifreigabe verknüpft.

> Bei der Provisionierung der NFS-Freigabe können Sie entweder eine Exportrichtlinie erstellen, indem Sie alle erforderlichen Werte angeben, oder den Exportrichtlinienschlüssel angeben und eine bestehende Exportrichtlinie wiederverwenden. Wenn Sie eine Exportrichtlinie für die Storage VM wiederverwenden möchten, müssen Sie den Exportrichtlinienschlüssel hinzufügen. Falls Sie den Schlüssel nicht kennen, können Sie den Exportrichtlinienschlüssel über die `/datacenter/protocols/nfs/export-policies` API abrufen. Zum Erstellen einer neuen Richtlinie müssen Sie die Regeln wie im folgenden Beispiel gezeigt eingeben. Anhand der eingegebenen Regeln versucht die API, eine bestehende Exportrichtlinie zu finden, indem sie Host, Storage VM und Regeln abgleicht. Wenn bereits eine Exportrichtlinie vorhanden ist, wird sie verwendet. Andernfalls wird eine neue Exportrichtlinie erstellt.

Ein cURL-Befehl mit Beispielwerten

```
"export_policy": {
      "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
      "name_tag": "ExportPolicyNameTag",
      "rules": [
        {
          "clients": [
            {
              "match": "0.0.0.0/0"
            }
```

Nach der Konfiguration der Zugriffssteuerungsliste und der Exportrichtlinie sind die gültigen Werte für die obligatorischen Eingabeparameter sowohl für CIFS- als auch für NFS-Dateifreigaben anzugeben:

> Storage Efficiency Policy ist ein optionaler Parameter für die Erstellung von Dateifreigaben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/file-shares`

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem sich die erstellte Dateifreigabe überprüfen lässt . Die Erstellung der Dateifreigabe lässt sich mithilfe des Job-Objektschlüssels überprüfen, der bei der Abfrage des Jobs zurückgegeben wird:

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	`/management-server/jobs/{key}`

Am Ende der Antwort sehen Sie den Schlüssel der erstellten Dateifreigabe.

```
    ],
    "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. Zur Überprüfung der Erstellung der Dateifreigabe wird die folgende API mit dem zurückgegebenen Schlüssel ausgeführt:

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/file-shares/{key}`

   Beispielhafte JSON-Ausgabe

   Es ist ersichtlich, dass die POST-Methode `/storage-provider/file-shares`intern alle für die einzelnen Funktionen erforderlichen APIs aufruft und das Objekt erstellt. Beispielsweise ruft sie die `/storage-provider/performance-service-levels/`API auf, um das Performance Service Level der Dateifreigabe zuzuweisen.

   ```
   {
       "key": "7d5a59b3-953a-11e8-8857-
   ```

```
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
    "name": "FileShare_377",
    "cluster": {
        "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
        "name": "AFFA300-206-68-70-72-74",
        "_links": {
            "self": {
                "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-
00a098dcc959"
            }
        }
    },
    "svm": {
        "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
        "name": "RRT_ritu_vs1",
        "_links": {
            "self": {
                "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-
8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-
00a098dcc959"
            }
        }
    },
    "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
        }
    },
    "recommended_performance_service_level": {
        "key": null,
        "name": "Idle",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
```

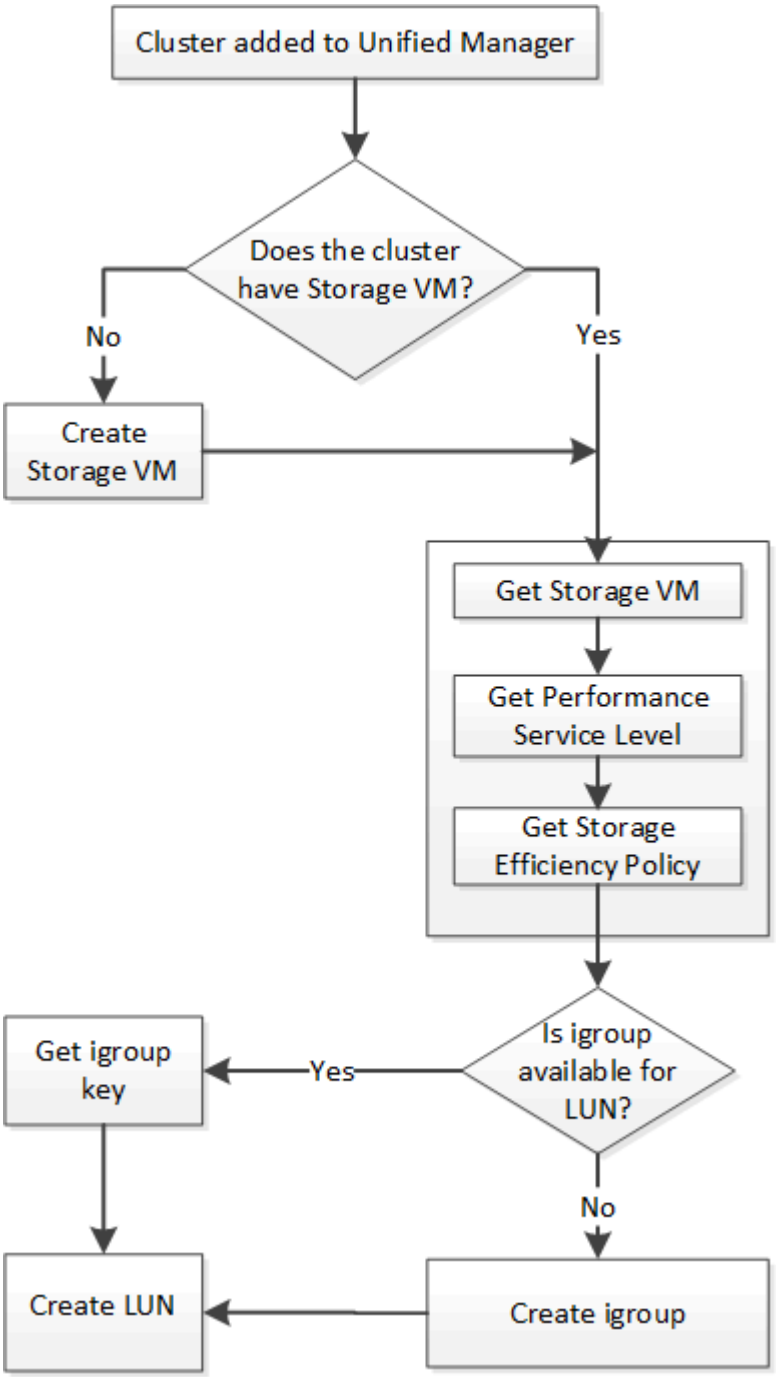
```
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 1,
                    "protocols": [
                        "nfs3",
                        "nfs4"
                    ],
                    "ro_rule": [
                        "sys"
                    ],
                    "rw_rule": [
                        "sys"
                    ],
                    "superuser": [
                        "none"
                    ]
                },
                {
                    "anonymous_user": "65534",
```

```
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 2,
                    "protocols": [
                        "cifs"
                    ],
                    "ro_rule": [
                        "ntlm"
                    ],
                    "rw_rule": [
                        "ntlm"
                    ],
                    "superuser": [
                        "none"
                    ]
                }
            ],
            "_links": {
                "self": {
                    "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
                }
            }
        }
    },
    "_links": {
        "self": {
            "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
        }
    }
}
```


Bereitstellung von LUNs mithilfe der Active IQ Unified Manager APIs

Sie können LUNs auf Ihren Storage Virtual Machines (SVMs) mithilfe der als Teil von Active IQ Unified Manager bereitgestellten Provisionierungs-APIs provisionieren. Dieser Provisionierungs-Workflow beschreibt die Schritte zum Abrufen der Schlüssel der SVMs, der Performance Service Levels und der Storage Efficiency Policies vor dem Erstellen der LUN.

Das folgende Diagramm veranschaulicht die Schritte in einem LUN-Provisionierungs-Workflow.



Dieser Workflow setzt voraus, dass die ONTAP Cluster zu Unified Manager hinzugefügt wurden und der Clusterschlüssel abgerufen wurde. Der Workflow setzt außerdem voraus, dass die SVMs bereits auf den Clustern erstellt wurden.

1. Den SVM-Schlüssel für die SVM, auf der die LUN erstellt werden soll, finden Sie im Workflow-Thema *Verifying SVMs on clusters*.
2. Den Schlüssel für das Performance Service Level erhalten Sie, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie den `system_defined` Eingabeparameter auf `true` setzen. Aus der Ausgabe kann der Schlüssel des Performance Service Levels ermittelt werden, das Sie auf die LUN anwenden möchten.

3. Optional können Sie den Schlüssel für die Storage Efficiency Policy abrufen, die Sie auf die LUN anwenden möchten, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/storage-efficiency-policies`

4. Stellen Sie fest, ob Initiatorgruppen (igroups) erstellt wurden, um Zugriff auf das LUN-Ziel zu gewähren, das Sie erstellen möchten.

Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/protocols/san/igroups` `/datacenter/protocols/san/igroups/{key}`

Erforderlich ist die Eingabe des Parameterwerts, der die SVM angibt, für die die Initiatorgruppe autorisierten Zugriff hat. Wenn außerdem eine bestimmte Initiatorgruppe abgefragt werden soll, ist der Name der Initiatorgruppe (Schlüssel) als Eingabeparameter anzugeben.

5. Wenn sich in der Ausgabe die Initiatorgruppe finden lässt, der Sie Zugriff gewähren möchten, können Sie den Schlüssel abrufen. Andernfalls kann die Initiatorgruppe erstellt werden.

Kategorie	HTTP-Verb	Pfad
Datacenter	POST	`/datacenter/protocols/san/igroups`

Als Eingabeparameter sind die Details der Initiatorgruppe anzugeben, die erstellt werden soll. Dies ist ein synchroner Aufruf, und die Erstellung der Initiatorgruppe kann in der Ausgabe überprüft werden. Im Fehlerfall erscheint eine Meldung, die bei der Fehlerbehebung und beim erneuten Ausführen der API unterstützt.

6. Die LUN wird erstellt.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/luns`

Beim Erstellen der LUN ist sicherzustellen, dass die abgerufenen Werte als obligatorische Eingabeparameter hinzugefügt wurden.

Die Speichereffizienzrichtlinie ist ein optionaler Parameter für die Erstellung von LUNs.

Beispiel cURL

Sie müssen alle Details der LUN, die Sie erstellen möchten, als Eingabeparameter angeben.

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie die von Ihnen erstellte LUN überprüfen können.

7. Die Überprüfung der LUN-Erstellung erfolgt mithilfe des Job-Objektschlüssels, der bei der Abfrage des Jobs zurückgegeben wird:

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	`/management-server/jobs/{key}`

Am Ende der Antwort ist der Schlüssel der erstellten LUN sichtbar.

8. Die Erstellung der LUN kann überprüft werden, indem die folgende API mit dem zurückgegebenen Schlüssel ausgeführt wird:

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/luns/{key}`

Beispielhafte JSON-Ausgabe

Es zeigt sich, dass die POST-Methode `/storage-provider/luns`intern alle für die einzelnen Funktionen erforderlichen APIs aufruft und das Objekt erstellt. Beispielsweise ruft sie die `/storage-provider/performance-service-levels/` API zum Zuweisen des Performance Service Level auf der LUN auf.

== Schritte zur Fehlerbehebung bei Fehlern in der LUN-Erstellung oder -Zuordnung

Nach Abschluss dieses Workflows kann es dennoch zu einem Fehler bei der LUN-Erstellung kommen. Selbst wenn die LUN erfolgreich erstellt wurde, kann die Zuordnung der LUN zur Initiatorgruppe aufgrund einer nicht verfügbaren SAN-LIF oder eines Zugriffsendpunkts auf dem Knoten, auf dem die LUN erstellt wird, fehlschlagen. Im Fehlerfall wird die folgende Meldung angezeigt:

```
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.
```

Die folgenden Schritte zur Fehlerbehebung dienen dazu, diesen Fehler zu umgehen.

1. Erforderlich ist ein Zugriffsendpunkt auf der SVM, auf der Sie versucht haben, die LUN zu erstellen, der das ISCSI/FCP-Protokoll unterstützt.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/access-endpoints`

Beispiel cURL

Sie müssen die Details des Zugriffs-Endpunkts, den Sie erstellen möchten, als Eingabeparameter eingeben.

> Stellen Sie sicher, dass Sie im Eingabeparameter die Adresse hinzugefügt haben, um den Home-Node der LUN anzugeben, sowie die ha_address, um den Partner-Node des Home-Node anzugeben. Bei der Ausführung dieses Vorgangs werden Zugriffsendpunkte sowohl auf dem Home-Node als auch auf dem Partner-Node erstellt.

2. Anhand des im JSON-Output zurückgegebenen Job-Objektschlüssels lässt sich überprüfen, dass der Job erfolgreich ausgeführt wurde, um die Zugriffs-Endpunkte auf der SVM hinzuzufügen, und dass die iSCSI/FCP Services auf der SVM aktiviert wurden.

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	`/management-server/jobs/{key}`

Beispielhafte JSON-Ausgabe

Am Ende der Ausgabe ist der Schlüssel der erstellten Zugriffs-Endpunkte zu sehen. In der folgenden Ausgabe gibt der Wert "name": "accessEndpointKey" den Zugriffs-Endpunkt an, der auf dem Home-Knoten der LUN erstellt wurde und dessen Schlüssel 9c964258-14ef-11ea-95e2-00a098e32c28 lautet. Der Wert "name": "accessEndpointHAKey" gibt den Zugriffs-Endpunkt an, der auf dem Partnerknoten des Home-Knotens erstellt wurde und dessen Schlüssel 9d347006-14ef-11ea-8760-00a098e3215f lautet.

3. Die LUN wird geändert, um die Zuordnung der Initiatorgruppe zu aktualisieren. Weitere Informationen zur Workflow-Änderung finden Sie unter „`Modifying storage workloads`“.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/lun/{key}`

Die Eingabe umfasst den Initiatorgruppe-Schlüssel, mit dem die LUN-Zuordnung aktualisiert werden soll, sowie den LUN-Schlüssel.

Beispiel cURL

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie überprüfen können, ob die Zuordnung erfolgreich war.

4. Die LUN-Zuordnung lässt sich durch eine Abfrage mit dem LUN-Schlüssel überprüfen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/luns/{key}`

Beispielhafte JSON-Ausgabe

In der Ausgabe können Sie sehen, dass die LUN erfolgreich der Initiatorgruppe (Schlüssel d19ec2fa-fec7-11e8-b23d-00a098e32c28) zugeordnet wurde, mit der sie ursprünglich provisioniert wurde.

Storage Workloads modifizieren

Das Ändern von Speicherworkloads mithilfe von APIs in Active IQ Unified Manager

Das Ändern von Storage-Workloads umfasst das Aktualisieren von LUNs oder Dateifreigaben mit fehlenden Parametern oder das Ändern der vorhandenen Parameter.

Dieser Workflow verwendet das Beispiel der Aktualisierung von Performance Service Levels für LUNs und Dateifreigaben.

Der Workflow setzt voraus, dass die LUN oder die Dateifreigabe mit Performance Service Levels provisioniert wurde.

Dateifreigaben ändern

Beim Bearbeiten einer Dateifreigabe können Sie die folgenden Parameter aktualisieren:

- Kapazität oder Größe.
- Online- oder Offline-Einstellung.
- Richtlinie zur Speichereffizienz.
- Performance-Service-Level.
- Einstellungen der Zugriffssteuerungsliste (ACL).
- Exportrichtlinieneinstellungen. Sie können auch Exportrichtlinienparameter löschen und die standardmäßigen (leeren) Exportrichtlinienregeln für die Dateifreigabe wiederherstellen.

Bei einem einzelnen API-Lauf kann nur ein Parameter aktualisiert werden.

Dieses Verfahren beschreibt das Hinzufügen eines Performance Service Level zu einer Dateifreigabe. Dasselbe Verfahren kann auch zum Aktualisieren jeder anderen Eigenschaft einer Dateifreigabe verwendet werden.

1. Der CIFS- oder NFS-Dateifreigabeschlüssel der Dateifreigabe, die Sie aktualisieren möchten, muss ermittelt werden. Mit dieser API werden alle Dateifreigaben in Ihrem Datacenter abgefragt. Dieser Schritt kann übersprungen werden, wenn Ihnen der Dateifreigabeschlüssel bereits bekannt ist.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/file-shares`

2. Die Details der Dateifreigabe können Sie anzeigen, indem Sie die folgende API mit dem Dateifreigabeschlüssel ausführen, den Sie erhalten haben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/file-shares/{key}`

In der Ausgabe sind die Details der Dateifreigabe zu sehen.

```
"assigned_performance_service_level": {
        "key": null,
        "name": "Unassigned",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
      },
```

3. Benötigt wird der Schlüssel für die Performance Service Level, die dieser Dateifreigabe zugewiesen werden soll. Derzeit ist ihr keine Richtlinie zugewiesen.

Kategorie	HTTP-Verb	Pfad
Performance-Servicelevels	GET	`/storage-provider/performance-service-levels`

> Die Details der systemdefinierten Performance Service Levels können durch Setzen des `system_defined` Eingabeparameters auf `true` abgerufen werden. Der Ausgabe ist der Schlüssel des Performance Service Level zu entnehmen, der auf die Dateifreigabe angewendet werden soll.

4. Performance Service Level auf die Dateifreigabe anwenden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/file-shares/{key}`

In der Eingabe müssen Sie nur den Parameter angeben, den Sie aktualisieren möchten, zusammen mit dem Dateifreigabeschlüssel. In diesem Fall handelt es sich um den Schlüssel des Performance Service Level.

Beispiel 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\" },
```

```
}"
```

Die JSON-Ausgabe zeigt ein Job-Objekt an, mit dem überprüft werden kann, ob die Zugriffsendpunkte auf den Home- und Partnerknoten erfolgreich erstellt wurden.

5. Anhand des in Ihrer Ausgabe angezeigten Jobobjektschlüssels lässt sich überprüfen, ob der Dateifreigabe das Leistungsdienstniveau hinzugefügt wurde.

Kategorie	HTTP-Verb	Pfad
Verwaltungsserver	GET	`/management-server/jobs/{key}`

Bei einer Abfrage über die ID des Job-Objekts ist erkennbar, ob die Dateifreigabe erfolgreich aktualisiert wurde. Im Fehlerfall empfiehlt sich eine Fehlerbehebung mit anschließender erneuter Ausführung der API. Nach erfolgreicher Erstellung lässt sich die Dateifreigabe abfragen, um das geänderte Objekt anzuzeigen:

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/file-shares/{key}`

In der Ausgabe sind die Details der Dateifreigabe zu sehen.

```
"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"
            }
        }
```

Aktualisierung von LUNs

Beim Aktualisieren einer LUN können Sie die folgenden Parameter ändern:

- Kapazität oder Größe
- Online- oder Offline-Einstellung
- Richtlinie zur Storage-Effizienz
- Performance-Service-Level
- LUN erfassen

Bei einem einzelnen API-Lauf kann nur ein Parameter aktualisiert werden.

Dieses Verfahren beschreibt das Hinzufügen eines Performance Service Level zu einer LUN. Dasselbe Verfahren kann auch für die Aktualisierung jeder anderen LUN-Eigenschaft verwendet werden.

1. Der LUN-Schlüssel der LUN, die aktualisiert werden soll, ist zu ermitteln. Diese API liefert Details zu allen LUNs in Ihrem Datacenter. Dieser Schritt kann übersprungen werden, wenn der LUN-Schlüssel bereits bekannt ist.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/luns`

2. Die Details der LUN können Sie anzeigen, indem Sie die folgende API mit dem erhaltenen LUN-Schlüssel ausführen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/luns/{key}`

   Die Details der LUN können Sie in der Ausgabe einsehen. Sie sehen, dass dieser LUN kein Performance Service Level zugewiesen ist.

   Beispielhafte JSON-Ausgabe

```
"assigned_performance_service_level": {
      "key": null,
      "name": "Unassigned",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
```

3. Benötigt wird der Schlüssel für das Performance Service Level, das der LUN zugewiesen werden soll.

Kategorie	HTTP-Verb	Pfad
Performance-Servicelevels	GET	`/storage-provider/performance-service-levels`

   Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie den `system_defined` Eingabeparameter auf `true` setzen. Aus der Ausgabe kann der Schlüssel des Performance Service Levels ermittelt werden, das Sie auf die LUN anwenden möchten.

4. Das Performance Service Level auf die LUN anwenden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/lun/{key}`

In der Eingabe müssen Sie lediglich den zu aktualisierenden Parameter sowie den LUN-Schlüssel angeben. In diesem Fall handelt es sich um den Schlüssel des Performance Service Level.

Beispiel 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\" }"
```

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie die aktualisierte LUN überprüfen können.

5. Die Details der LUN können Sie anzeigen, indem Sie die folgende API mit dem erhaltenen LUN-Schlüssel ausführen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/luns/{key}`

Die Details der LUN können Sie in der Ausgabe einsehen. Dort sehen Sie, dass dieser LUN das Performance Service Level zugewiesen ist.

Beispielhafte JSON-Ausgabe

```
     "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"
            }
```

Ändern einer NFS Dateifreigabe zur Unterstützung von CIFS mithilfe der Active IQ Unified Manager APIs

Sie können eine NFS-Dateifreigabe ändern, damit sie das CIFS-Protokoll unterstützt. Bei der Erstellung der Dateifreigabe können sowohl Parameter der Zugriffssteuerungsliste (ACL) als auch Exportrichtlinienregeln für dieselbe Dateifreigabe angegeben werden. Wenn Sie CIFS jedoch auf demselben Volume aktivieren möchten, auf dem Sie eine NFS-Dateifreigabe erstellt haben, können Sie die ACL-Parameter dieser Dateifreigabe aktualisieren, damit sie CIFS unterstützt.

Bevor Sie beginnen

1. Eine NFS-Dateifreigabe muss bereits nur mit den Exportrichtliniendetails erstellt worden sein. Informationen dazu enthalten *Managing file shares* und *Modifying storage workloads*.
2. Für diesen Vorgang benötigen Sie den Dateifreigabeschlüssel. Informationen zum Anzeigen von Dateifreigabedetails und zum Abrufen des Dateifreigabeschlüssels mithilfe der Job ID finden Sie unter „Bereitstellen von CIFS- und NFS-Dateifreigaben“.

Dies gilt für eine NFS-Dateifreigabe, die Sie erstellt haben, indem Sie nur Exportrichtlinienregeln und keine ACL-Parameter hinzugefügt haben. Sie ändern die NFS-Dateifreigabe, sodass die ACL-Parameter einbezogen werden.

Schritte

1. Auf der NFS-Dateifreigabe erfolgt ein `PATCH`Vorgang mit den ACL-Details, um CIFS-Zugriff zuzulassen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/file-shares`

Beispiel cURL

Basierend auf den Zugriffsrechten, die Sie der Benutzergruppe zuweisen, wird, wie im folgenden Beispiel dargestellt, eine ACL erstellt und der Dateifreigabe zugewiesen.

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
```

Beispielhafte JSON-Ausgabe

Die Operation gibt die Job-ID des Jobs zurück, der das Update ausführt.

2. Ob die Parameter korrekt hinzugefügt wurden, lässt sich durch Abfrage der Details der Dateifreigabe für dieselbe Dateifreigabe verifizieren.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/file-shares/{key}`

Beispielhafte JSON-Ausgabe

```
"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"
        }
    }
```

Sie können die ACL zusammen mit der Exportrichtlinie für dieselbe Dateifreigabe sehen.

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtsvermerke, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp Trademarks-Seite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp owned patents finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

Informationen zu Urheberrechten und Lizenzen Dritter, die in diesem Produkt verwendet werden.

"Hinweis für Active IQ Unified Manager 9.18"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.