Active IQ Unified Manager Dokumentation

Active IQ Unified Manager

NetApp
October 15, 2025

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

Inhalt

Active IQ Unified Manager Dokumentation . . . 1
Versionshinweise . . . 2
Erste Schritte . . . 3
- Schnellstartanleitung für VMware-Installationen . . . 3
  - Systemanforderungen . . . 3
  - Installieren Sie Active IQ Unified Manager . . . 3
- Schnellstartanleitung für Linux-Installationen . . . 4
  - Systemanforderungen . . . 4
  - Installieren Sie Active IQ Unified Manager . . . 4
- Schnellstartanleitung für Windows-Installationen . . . 5
  - Systemanforderungen . . . 5
  - Installieren Sie Active IQ Unified Manager . . . 6

Installieren Sie Unified Manager auf VMware vSphere-Systemen . . . 7
- Einführung in Active IQ Unified Manager . . . 7
  - Was der Unified Manager-Server macht . . . 7
  - Übersicht über den Installationsablauf . . . 7
- Voraussetzungen für die Installation von Unified Manager . . . 8
  - Anforderungen an die virtuelle Infrastruktur und das Hardwaresystem . . . 8
  - VMware-Software- und Installationsanforderungen . . . 10
  - Unterstützte Browser . . . 10
  - Protokoll- und Portanforderungen . . . 11
  - Füllen Sie das Arbeitsblatt aus . . . 15
- Installieren, aktualisieren und entfernen Sie die Unified Manager-Software . . . 17
  - Übersicht über den Bereitstellungsprozess . . . 17
  - Unified Manager bereitstellen . . . 18
  - Upgrade von Unified Manager . . . 22
  - Starten Sie die virtuelle Unified Manager-Maschine neu . . . 25
  - Unified Manager entfernen . . . 25

Installieren Sie Unified Manager auf Linux-Systemen . . . 27
- Einführung in Active IQ Unified Manager . . . 27
  - Was der Unified Manager-Server macht . . . 27
  - Übersicht über den Installationsablauf . . . 27
- Voraussetzungen für die Installation von Unified Manager . . . 28
  - Anforderungen an die virtuelle Infrastruktur und das Hardwaresystem . . . 28
  - Linux-Software und Installationsanforderungen . . . 30
  - Unterstützte Browser . . . 33
  - Protokoll- und Portanforderungen . . . 33
  - Füllen Sie das Arbeitsblatt aus . . . 37
- Installieren, aktualisieren und entfernen Sie die Unified Manager-Software . . . 39
  - Übersicht über den Installationsprozess . . . 39
  - Einrichten der erforderlichen Software-Repositorys . . . 39
  - SELinux-Anforderungen an NFS- und CIFS-Freigaben . . . 41
  - Installieren Sie Unified Manager auf Linux-Systemen . . . 44

Upgrade von Unified Manager auf Red Hat Enterprise Linux . . . 51
Aktualisieren Sie Produkte von Drittanbietern nach der Installation von Unified Manager . . . 57
Unified Manager neu starten . . . 57
Unified Manager entfernen . . . 58
Entfernen Sie den benutzerdefinierten Umadmin-Benutzer und die Wartungsgruppe . . . 59
Installieren Sie Unified Manager auf Windows-Systemen . . . 60
Einführung in Active IQ Unified Manager . . . 60
Was der Unified Manager-Server macht . . . 60
Übersicht über den Installationsablauf . . . 60
Voraussetzungen für die Installation von Unified Manager . . . 61
Anforderungen an die virtuelle Infrastruktur und das Hardwaresystem . . . 61
Windows-Software- und Installationsanforderungen . . . 63
Unterstützte Browser . . . 64
Protokoll- und Portanforderungen . . . 65
Füllen Sie das Arbeitsblatt aus . . . 69
Installieren, aktualisieren und entfernen Sie die Unified Manager-Software . . . 70
Übersicht über den Installationsprozess . . . 71
Installieren Sie Unified Manager unter Windows . . . 71
Ändern des JBoss-Passworts . . . 75
Unterstützter Upgrade-Pfad für Unified Manager-Versionen . . . 76
Upgrade von Unified Manager . . . 76
Upgrade von Produkten von Drittanbietern . . . 78
Deinstallieren Sie Produkte von Drittanbietern . . . 79
Unified Manager neu starten . . . 79
Deinstallieren Sie Unified Manager . . . 80
Durchführen von Konfigurations- und Verwaltungsaufgaben . . . 82
Konfigurieren Sie Active IQ Unified Manager . . . 82
Übersicht über den Konfigurationsablauf . . . 82
Zugriff auf die Unified Manager-Web-Benutzeroberfläche . . . 82
Führen Sie die Ersteinrichtung der Unified Manager-Web-Benutzeroberfläche durch . . . 83
Cluster hinzufügen . . . 84
Konfigurieren Sie Unified Manager zum Senden von Warnbenachrichtigungen . . . 87
Ändern des lokalen Benutzerkennworts . . . 96
Festlegen des Sitzungs-Inaktivitäts-Timeouts . . . 97
Legen Sie das Sitzungs-Timeout über die CLI fest . . . 97
Ändern des Unified Manager-Hostnamens . . . 98
Aktivieren und Deaktivieren der richtlinienbasierten Speicherverwaltung . . . 102
Konfigurieren der Unified Manager-Sicherung . . . 103
Funktionseinstellungen verwalten . . . 103
Aktivieren Sie die richtlinienbasierte Speicherverwaltung . . . 104
API-Gateway aktivieren . . . 104
Inaktivitäts-Timeout angeben . . . 105
Aktivieren von Active IQ Portalereignissen . . . 105
Aktivieren und Deaktivieren von Sicherheitseinstellungen zur Einhaltung der Vorschriften . . . 106
Aktivieren und Deaktivieren des Skript-Uploads . . . 107

Login-Banner hinzufügen . . . 107
Verwenden der Wartungskonsole . . . 107
Welche Funktionalität bietet die Wartungskonsole? . . . 107
Was der Wartungsbenutzer tut . . . 108
Diagnosefunktionen für Benutzer . . . 108
Zugriff auf die Wartungskonsole . . . 108
Greifen Sie über die vSphere VM-Konsole auf die Wartungskonsole zu . . . 109
Menüs der Wartungskonsole . . . 110
Ändern des Wartungsbenutzerkennworts unter Windows . . . 115
Ändern des Umadmin-Passworts auf Linux-Systemen . . . 116
Ändern Sie die Ports, die Unified Manager für HTTP- und HTTPS-Protokolle verwendet . . . 116
Netzwerkschnittstellen hinzufügen . . . 117
Fügen Sie dem Unified Manager-Datenbankverzeichnis Speicherplatz hinzu . . . 118
Verwalten des Benutzerzugriffs . . . 121
Benutzer hinzufügen . . . 121
Bearbeiten der Benutzereinstellungen . . . 123
Benutzer anzeigen . . . 123
Löschen von Benutzern oder Gruppen . . . 124
Was ist RBAC? . . . 124
Was rollenbasierte Zugriffskontrolle bewirkt . . . 124
Definitionen von Benutzertypen . . . 124
Definitionen von Benutzerrollen . . . 125
Unified Manager-Benutzerrollen und -Funktionen . . . 126
Verwalten der SAML-Authentifizierungseinstellungen . . . 128
Anforderungen an den Identitätsanbieter . . . 129
Aktivieren der SAML-Authentifizierung . . . 130
Ändern Sie den für die SAML-Authentifizierung verwendeten Identitätsanbieter . . . 131
Aktualisieren Sie die SAML-Authentifizierungseinstellungen nach der Änderung des Unified Manager-Sicherheitszertifikats . . . 132
Deaktivieren der SAML-Authentifizierung . . . 133
Deaktivieren Sie die SAML-Authentifizierung über die Wartungskonsole . . . 134
SAML-Authentifizierungsseite . . . 134
Verwalten der Authentifizierung . . . 135
Authentifizierungsserver bearbeiten . . . 136
Authentifizierungsserver löschen . . . 136
Authentifizierung mit Active Directory oder OpenLDAP . . . 136
Überwachungsprotokollierung . . . 137
Seite „Remote-Authentifizierung“ . . . 140
Sicherheitszertifikate verwalten . . . 143
Zeigen Sie das HTTPS-Sicherheitszertifikat an . . . 143
Laden Sie eine HTTPS-Zertifikatsignieranforderung herunter . . . 144
Installieren Sie ein von einer CA signiertes und zurückgegebenes HTTPS-Zertifikat . . . 144
Installieren Sie ein mit externen Tools generiertes HTTPS-Zertifikat . . . 145
Seitenbeschreibungen zur Zertifikatsverwaltung . . . 148
Überwachen und Verwalten des Speichers . . . 150

Einführung in Active IQ Unified Manager . . . 150
Einführung in die Integritätsüberwachung von Active IQ Unified Manager . . . 150
Einführung in die Leistungsüberwachung von Active IQ Unified Manager . . . 151
Verwenden Sie Unified Manager REST-APIs . . . 152
Was der Unified Manager-Server macht . . . 152
Verstehen Sie die Benutzeroberfläche . . . 153
Typische Fensterlayouts . . . 153
Anpassung des Fensterlayouts . . . 154
Verwenden Sie die Unified Manager-Hilfe . . . 155
Setzen Sie ein Lesezeichen für Ihre bevorzugten Hilfethemen . . . 156
Suche nach Speicherobjekten . . . 156
Speicherdaten als Berichte exportieren . . . 157
Inhalt der Inventarseite filtern . . . 159
Zeigen Sie aktive Ereignisse über die Benachrichtigungsglocke an . . . 160
Überwachen und verwalten Sie Cluster über das Dashboard . . . 160
Dashboard-Seite . . . 161
Verwalten Sie ONTAP -Probleme oder -Funktionen direkt vom Unified Manager . . . 164
Verwalten von Clustern . . . 172
So funktioniert der Cluster-Erkennungsprozess . . . 172
Liste der überwachten Cluster anzeigen . . . 173
Cluster hinzufügen . . . 174
Cluster bearbeiten . . . 176
Cluster entfernen . . . 177
Cluster neu entdecken . . . 177
Überwachen Sie die virtuelle VMware-Infrastruktur . . . 178
Was wird nicht unterstützt? . . . 180
Anzeigen und Hinzufügen von vCenter Server . . . 181
Entfernen von vCenter Server . . . 183
Überwachen virtueller Maschinen . . . 183
Anzeigen der virtuellen Infrastruktur in einem Disaster Recovery-Setup . . . 185
Bereitstellen und Verwalten von Workloads . . . 187
Übersicht über Workloads . . . 188
Leistungsservice-Levels . . . 195
Verwalten von Speichereffizienzrichtlinien . . . 202
Verwalten und Überwachen von MetroCluster -Konfigurationen . . . 204
Lautstärkeverhalten beim Umschalten und Zurückschalten . . . 204
Cluster-Konnektivitätsstatusdefinitionen für die MetroCluster über-FC-Konfiguration . . . 206
Datenspiegelungsstatusdefinitionen für MetroCluster über FC . . . 207
Überwachen Sie MetroCluster -Konfigurationen . . . 207
Überwachen der MetroCluster -Replikation . . . 210
Verwalten von Kontingenten . . . 211
Welche Kontingentgrenzen gibt es . . . 211
Anzeigen von Benutzer- und Benutzergruppenkontingenten . . . 212
Erstellen Sie Regeln zum Generieren von E-Mail-Adressen . . . 212
Erstellen Sie ein E-Mail-Benachrichtigungsformat für Benutzer- und Benutzergruppenkontingente . . . 213

Bearbeiten Sie die E-Mail-Adressen der Benutzer- und Gruppenkontingente . . . 213
Erfahren Sie mehr über Quoten . . . 214
Beschreibung der Kontingentdialogfelder . . . 215
Fehlerbehebung . . . 218
Fügen Sie dem Unified Manager-Datenbankverzeichnis Speicherplatz hinzu . . . 218
Ändern des Erfassungsintervalls für Leistungsstatistiken . . . 222
Ändern Sie die Dauer, für die Unified Manager Ereignis- und Leistungsdaten speichert . . . 223
Unbekannter Authentifizierungsfehler . . . 224
Benutzer nicht gefunden . . . 224
Problem beim Hinzufügen von LDAP mithilfe anderer Authentifizierungsdienste . . . 224
Problem mit der Protokollrotation des NetApp Manageability SDK auf Windows-Systemen . . . 225
Verwalten von Ereignissen und Warnungen . . . 226
Ereignisse verwalten . . . 226
Was sind Active IQ Plattformereignisse? . . . 226
Was sind Event Management System-Ereignisse? . . . 226
Was passiert, wenn ein Ereignis empfangen wird? . . . 232
Anzeigen von Ereignissen und Ereignisdetails . . . 233
Nicht zugewiesene Ereignisse anzeigen . . . 234
Ereignisse bestätigen und beheben . . . 234
Zuweisen von Ereignissen zu bestimmten Benutzern . . . 235
Deaktivieren Sie unerwünschte Ereignisse . . . 236
Beheben Sie Probleme mit der automatischen Korrektur durch Unified Manager . . . 237
Aktivieren und Deaktivieren der Active IQ -Ereignisberichterstattung . . . 238
Laden Sie eine neue Active IQ Regeldatei hoch . . . 238
So werden Active IQ Plattformereignisse generiert . . . 239
Beheben Sie Active IQ Plattformereignisse . . . 239
Konfigurieren der Ereignisaufbewahrungseinstellungen . . . 240
Was ein Unified Manager-Wartungsfenster ist . . . 240
Verwalten von Hostsystemressourcenereignissen . . . 242
Erfahren Sie mehr über Ereignisse . . . 243
Liste der Ereignisse und Schweregrade . . . 249
Beschreibung der Ereignisfenster und Dialogfelder . . . 312
Verwalten von Warnungen . . . 324
Was sind Warnungen . . . 325
Welche Informationen sind in einer Warn-E-Mail enthalten? . . . 325
Benachrichtigungen hinzufügen . . . 325
Hinzufügen von Warnungen für Leistungsereignisse . . . 328
Testwarnungen . . . 329
Aktivieren und Deaktivieren von Warnungen für behobene und veraltete Ereignisse . . . 330
Ausschließen von Disaster Recovery-Zielvolumes von der Generierung von Warnungen . . . 330
Warnungen anzeigen . . . 331
Benachrichtigungen bearbeiten . . . 331
Benachrichtigungen löschen . . . 332
Beschreibung der Warnfenster und Dialogfelder . . . 332
Skripte verwalten . . . 338

So funktionieren Skripte mit Warnungen . . . 339
Skripts hinzufügen . . . 340
Skripte löschen . . . 341
Testskriptausführung . . . 341
Unterstützte Unified Manager CLI-Befehle . . . 342
Beschreibung der Skriptfenster und Dialogfelder . . . 348
Überwachen und Verwalten der Clusterleistung . . . 350
Einführung in die Leistungsüberwachung von Active IQ Unified Manager . . . 350
Leistungsüberwachungsfunktionen von Unified Manager . . . 350
Unified Manager-Schnittstellen zur Verwaltung der Speichersystemleistung . . . 351
Clusterkonfiguration und Leistungsdatenerfassungsaktivität . . . 351
Was ein Datenkontinuitätserfassungszyklus ist . . . 353
Was der Zeitstempel in erfassten Daten und Ereignissen bedeutet . . . 354
Navigieren Sie durch Leistungsworkflows in der Unified Manager-GUI . . . 354
Melden Sie sich bei der Benutzeroberfläche an . . . 354
Grafische Oberfläche und Navigationspfade . . . 355
Suche nach Speicherobjekten . . . 357
Inhalt der Inventarseite filtern . . . 358
Überwachen Sie die Clusterleistung vom Dashboard aus . . . 359
Leistungsbereiche auf dem Dashboard verstehen . . . 360
Leistungsbannernachrichten und -beschreibungen . . . 360
Ändern des Erfassungsintervalls für Leistungsstatistiken . . . 361
Beheben von Workload-Problemen mit dem Workload-Analyzer . . . 362
Welche Daten zeigt der Workload Analyzer an . . . 362
Wann würde ich den Workload-Analyzer verwenden? . . . 364
Verwenden des Workload-Analysators . . . 365
Überwachen Sie die Clusterleistung von der Zielseite des Leistungsclusters aus . . . 365
Die Zielseite des Performance-Clusters verstehen . . . 365
Zielseite des Performance-Clusters . . . 366
Überwachen Sie die Leistung mithilfe der Leistungsinventarseiten . . . 370
Anzeigen der Leistungsinventarseiten für alle Speicherobjekte . . . 371
Verfeinern des Inhalts der Performance-Inventarseite . . . 376
Informieren Sie sich über die Empfehlungen des Unified Managers zur Datenschichtung in der Cloud. 379
Überwachen der Leistung mithilfe der Performance Explorer-Seiten . . . 380
Verstehen Sie das Stammobjekt . . . 381
Wenden Sie Filter an, um die Liste der korrelierten Objekte im Raster zu reduzieren . . . 381
Festlegen eines Zeitbereichs für korrelierte Objekte . . . 381
Definieren Sie die Liste der korrelierten Objekte für die grafische Vergleichsdarstellung . . . 383
Zählerdiagramme verstehen . . . 384
Arten von Leistungsindikatordiagrammen . . . 385
Wählen Sie die anzuzeigenden Leistungsdiagramme aus . . . 388
Erweitern Sie den Bereich „Zählerdiagramme“ . . . 388
Ändern Sie den Fokus der Counter Charts auf einen kürzeren Zeitraum . . . 388
Ereignisdetails in der Ereigniszeitleiste anzeigen . . . 389
Zählerdiagramme Zoomansicht . . . 390

Anzeigen der Volume-Latenz nach Clusterkomponente . . . 392
SVM-IOPS-Verkehr nach Protokoll anzeigen . . . 393
Zeigen Sie Volume- und LUN-Latenzdiagramme an, um die Leistungsgarantie zu überprüfen . . . 393
Leistung aller SAN-Array-Cluster anzeigen . . . 394
Anzeigen von Knoten-IOPS basierend auf Workloads, die sich nur auf dem lokalen Knoten befinden . . . 395
Komponenten der Objekt-Landingpages . . . 395
Verwalten der Leistung mithilfe von QoS-Richtliniengruppeninformationen . . . 401
So kann Speicher-QoS den Workload-Durchsatz steuern . . . 401
Alle auf allen Clustern verfügbaren QoS-Richtliniengruppen anzeigen . . . 402
Anzeigen von Volumes oder LUNs, die sich in derselben QoS-Richtliniengruppe befinden . . . 402
Anzeigen der QoS-Richtliniengruppeneinstellungen, die auf bestimmte Volumes oder LUNs angewendet werden . . . 403
Zeigen Sie Leistungsdiagramme an, um Volumes oder LUNs zu vergleichen, die sich in derselben QoS-Richtliniengruppe befinden . . . 404
So werden verschiedene Arten von QoS-Richtlinien in den Durchsatzdiagrammen angezeigt . . . 405
Anzeigen der minimalen und maximalen QoS-Einstellungen für die Arbeitslast im Performance Explorer . . . 406
Verwalten Sie die Leistung mithilfe von Leistungskapazität und verfügbaren IOPS-Informationen . . . 407
Welche Leistungsfähigkeit wird genutzt . . . 408
Was der Leistungskapazitäts-Gebrauchswert bedeutet . . . 408
Welche IOPS sind verfügbar? . . . 409
Anzeigen der verwendeten Knoten- und aggregierten Leistungskapazitätswerte . . . 410
Knoten anzeigen und verfügbare IOPS-Werte aggregieren . . . 410
Zeigen Sie Leistungskapazitätsindikatordiagramme an, um Probleme zu identifizieren . . . 411
Leistungskapazität genutzte Leistungsschwellenbedingungen . . . 411
Verwenden Sie den Leistungskapazitätszähler, um die Leistung zu verwalten . . . 412
Verstehen und Verwenden der Seite „Knoten-Failover-Planung“ . . . 413
Verwenden Sie die Seite „Knoten-Failover-Planung“, um Korrekturmaßnahmen festzulegen . . . 413
Komponenten der Seite „Knoten-Failover-Planung“ . . . 413
Verwenden einer Schwellenwertrichtlinie mit der Seite „Knoten-Failover-Planung“ . . . 415
Verwenden Sie das Diagramm „Aufschlüsselung der genutzten Leistungskapazität“ für die Failover-Planung . . . 416
Sammeln Sie Daten und überwachen Sie die Workload-Leistung . . . 417
Von Unified Manager überwachte Workloadtypen . . . 417
Messwerte für die Workload-Leistung . . . 418
Was ist der erwartete Leistungsbereich . . . 420
Wie die Latenzprognose in der Leistungsanalyse verwendet wird . . . 421
So nutzt Unified Manager die Workload-Latenz, um Leistungsprobleme zu identifizieren . . . 422
Wie Clustervorgänge die Workload-Latenz beeinflussen können . . . 423
Leistungsüberwachung von MetroCluster -Konfigurationen . . . 424
Leistungsereignisse und Warnungen verstehen . . . 425
Quellen von Leistungsereignissen . . . 425
Schweregradtypen von Leistungsereignissen . . . 426
Von Unified Manager erkannte Konfigurationsänderungen . . . 427
Arten systemdefinierter Richtlinien für Leistungsschwellenwerte . . . 427

Analyse und Benachrichtigung von Leistungsereignissen . . . 430
So ermittelt Unified Manager die Leistungsauswirkungen eines Ereignisses . . . 432
Clusterkomponenten und warum sie kontrovers diskutiert werden können . . . 433
Rollen der an einem Leistungsereignis beteiligten Workloads . . . 435
Leistungsschwellenwerte verwalten . . . 436
Funktionsweise benutzerdefinierter Leistungsschwellenwertrichtlinien . . . 437
Was passiert, wenn eine Leistungsschwellenrichtlinie verletzt wird? . . . 438
Welche Leistungsindikatoren können mithilfe von Schwellenwerten verfolgt werden? . . . 438
Welche Objekte und Zähler können in Kombinationsschwellenwertrichtlinien verwendet werden? . . . 441
Erstellen Sie benutzerdefinierte Richtlinien für Leistungsschwellenwerte . . . 442
Zuweisen von Leistungsschwellenwertrichtlinien zu Speicherobjekten . . . 443
Richtlinien für Leistungsschwellenwerte anzeigen . . . 444
Bearbeiten benutzerdefinierter Richtlinien für Leistungsschwellenwerte . . . 445
Entfernen Sie Leistungsschwellenwertrichtlinien aus Speicherobjekten . . . 445
Was passiert, wenn eine Leistungsschwellenwertrichtlinie geändert wird? . . . 446
Was passiert mit Leistungsschwellenwertrichtlinien, wenn ein Objekt verschoben wird? . . . 447
Analysieren von Leistungsereignissen . . . 448
Informationen zu Leistungsereignissen anzeigen . . . 448
Analysieren Sie Ereignisse anhand benutzerdefinierter Leistungsschwellenwerte . . . 449
Analysieren Sie Ereignisse anhand systemdefinierter Leistungsschwellenwerte . . . 450
Analysieren Sie Ereignisse anhand dynamischer Leistungsschwellenwerte . . . 456
Beheben von Leistungsereignissen . . . 464
Bestätigen Sie, dass die Latenz im erwarteten Bereich liegt . . . 464
Überprüfen Sie die Auswirkungen von Konfigurationsänderungen auf die Workload-Leistung . . . 464
Optionen zur Verbesserung der Workload-Leistung auf der Clientseite . . . 465
Suchen Sie nach Client- oder Netzwerkproblemen . . . 465
Überprüfen Sie, ob andere Volumes in der QoS-Richtliniengruppe ungewöhnlich hohe Aktivität aufweisen . . . 465
Logische Schnittstellen (LIFs) verschieben . . . 466
Führen Sie Speichereffizienzvorgänge in weniger ausgelasteten Zeiten durch . . . 467
Hinzufügen von Datenträgern und Neuzuweisung von Daten . . . 468
So kann die Aktivierung von Flash Cache auf einem Knoten die Workload-Leistung verbessern . . . 468
So kann die Aktivierung von Flash Pool auf einem Speicheraggregat die Workload-Leistung verbessern . . . 469
Integritätsprüfung der MetroCluster -Konfiguration . . . 469
Überprüfung der MetroCluster -Konfiguration . . . 469
Verschieben von Workloads in ein anderes Aggregat . . . 470
Verschieben von Workloads auf einen anderen Knoten . . . 471
Verschieben von Workloads in ein Aggregat auf einem anderen Knoten . . . 473
Verschieben Sie Workloads auf einen Knoten in einem anderen HA-Paar . . . 475
Verschieben Sie Workloads auf einen anderen Knoten in einem anderen HA-Paar . . . 477
Verwenden Sie QoS-Richtlinieneinstellungen, um die Arbeit an diesem Knoten zu priorisieren . . . 478
Entfernen inaktiver Volumes und LUNs . . . 479
Fügen Sie Datenträger hinzu und führen Sie eine Rekonstruktion des Gesamtlayouts durch . . . 480
Einrichten einer Verbindung zwischen einem Unified Manager-Server und einem externen Datenanbieter 480

Leistungsdaten, die an einen externen Server gesendet werden können . . . 480
Richten Sie Graphite ein, um Leistungsdaten von Unified Manager zu erhalten . . . 481
Konfigurieren einer Verbindung von einem Unified Manager-Server zu einem externen Datenanbieter 482
Überwachen und Verwalten der Clusterintegrität . . . 485
Einführung in die Integritätsüberwachung von Active IQ Unified Manager . . . 485
Körperliche und logische Leistungsfähigkeit . . . 485
Kapazitätsmesseinheiten . . . 485
Unified Manager-Funktionen zur Integritätsüberwachung . . . 486
Unified Manager-Schnittstellen zur Verwaltung der Speichersystemintegrität . . . 487
Verwalten und Überwachen der Integrität von Clustern und Clusterobjekten . . . 488
Grundlegendes zur Clusterüberwachung . . . 488
Anzeigen der Clusterliste und Details . . . 490
Überprüfen Sie den Zustand von Clustern in einer MetroCluster -Konfiguration . . . 491
Anzeigen des Integritäts- und Kapazitätsstatus aller SAN-Array-Cluster . . . 493
Anzeigen der Knotenliste und Details . . . 493
Erstellen Sie einen Hardware-Inventarbericht für die Vertragsverlängerung . . . 494
Anzeigen der Storage-VM-Liste und Details . . . 494
Gesamtliste und Details anzeigen . . . 495
Informationen zur FabricPool -Kapazität anzeigen . . . 496
Anzeigen von Speicherpooldetails . . . 497
Anzeigen der Volumeliste und Details . . . 498
Details zu NFS-Freigaben anzeigen . . . 499
Details zu SMB/CIFS-Freigaben anzeigen . . . 499
Liste der Snapshot-Kopien anzeigen . . . 500
Löschen von Snapshot-Kopien . . . 501
Berechnen Sie den wiederherstellbaren Speicherplatz für Snapshot-Kopien . . . 501
Beschreibung der Clusterobjektfenster und Dialogfelder . . . 502
Allgemeine Unified Manager-Integritätsworkflows und -Aufgaben . . . 502
Überwachen und Beheben von Problemen mit der Datenverfügbarkeit . . . 504
Beheben Sie Kapazitätsprobleme . . . 511
Verwalten von Integritätsschwellenwerten . . . 513
Verwalten von Cluster-Sicherheitszielen . . . 518
Verwalten von Sicherungs- und Wiederherstellungsvorgängen . . . 531
Skripte verwalten . . . 547
Verwalten und Überwachen von Gruppen . . . 550
Priorisieren Sie Speicherobjektereignisse mithilfe von Anmerkungen . . . 559
Senden Sie ein Support-Paket über die Web-Benutzeroberfläche und die Wartungskonsole . . . 569
Aufgaben und Informationen zu verschiedenen Arbeitsabläufen . . . 576
Schützen und Wiederherstellen von Daten . . . 636
Erstellen, Überwachen und Beheben von Problemen mit Schutzbeziehungen . . . 636
Arten des SnapMirror Schutzes . . . 636
Einrichten von Schutzbeziehungen im Unified Manager . . . 638
Führen Sie ein Failover und Failback für die Schutzbeziehung durch . . . 640
Beheben eines Schutzauftragsfehlers . . . 644
Beheben von Verzögerungsproblemen . . . 648

Verwalten und Überwachen von Schutzbeziehungen . . . 649
Anzeigen des Volume-Schutzstatus . . . 650
Anzeigen von Volume-Schutzbeziehungen . . . 652
Überwachen von LUNs in einer Konsistenzgruppenbeziehung . . . 652
Erstellen Sie eine SnapVault -Schutzbeziehung aus der Ansicht „Health: Alle Volumes“ . . . 653
Erstellen Sie eine SnapVault -Schutzbeziehung auf der Seite „Volume/Health-Details“ . . . 654
Erstellen Sie eine SnapMirror -Schutzbeziehung aus der Ansicht „Health: All Volumes“ . . . 655
Erstellen Sie eine SnapMirror -Schutzbeziehung auf der Seite „Volume/Health-Details“ . . . 657
Erstellen einer SnapMirror -Beziehung mit versionsflexibler Replikation . . . 658
Erstellen Sie SnapMirror -Beziehungen mit versionsflexibler Replikation mit Backup-Option . . . 659
Konfigurieren der Zieleffizienzeinstellungen . . . 660
Erstellen Sie SnapMirror und SnapVault -Zeitpläne . . . 661
Erstellen Sie Kaskaden- oder Fanout-Beziehungen, um den Schutz einer bestehenden Schutzbeziehung zu erweitern. . . . 661
Bearbeiten Sie Schutzbeziehungen auf der Seite „Volume-Beziehungen“. . . . 662
Bearbeiten Sie Schutzbeziehungen auf der Seite „Volume-/Integritätsdetails“. . . . 663
Erstellen Sie eine SnapMirror -Richtlinie, um die Übertragungseffizienz zu maximieren . . . 663
Erstellen Sie eine SnapVault -Richtlinie, um die Übertragungseffizienz zu maximieren . . . 664
Brechen Sie eine aktive Datenschutzübertragung von der Seite „Volume-Beziehungen“ ab . . . 665
Brechen Sie eine aktive Datensicherungsübertragung von der Seite „Volume-/Integritätsdetails“ ab . . . 665
Quiesce einer Schutzbeziehung auf der Seite „Volume-Beziehungen“ . . . 666
Beenden Sie eine Schutzbeziehung auf der Seite „Volume-/Integritätsdetails“. . . . 667
Brechen Sie eine SnapMirror -Beziehung von der Seite „Volume-Beziehungen“ ab . . . 668
Entfernen einer Schutzbeziehung von der Seite „Volume-Beziehungen“ . . . 668
Fortsetzen geplanter Übertragungen einer stillgelegten Beziehung über die Seite „Volume-Beziehungen“ . . . 669
Fortsetzen geplanter Übertragungen in einer stillgelegten Beziehung von der Seite „Volumen-/Gesundheitsdetails“ . . . 670
Initialisieren oder aktualisieren Sie Schutzbeziehungen auf der Seite „Volume-Beziehungen“. . . . 670
Initialisieren oder aktualisieren Sie Schutzbeziehungen auf der Seite „Volume-/Integritätsdetails“. . . . 671
Synchronisieren Sie Schutzbeziehungen über die Seite „Volume-Beziehungen“ erneut. . . . 672
Umkehren von Schutzbeziehungen auf der Seite „Volume-Beziehungen“ . . . 673
Wiederherstellen von Daten mithilfe der Detailseiten „Volume“ und „Volume/Integrität“ . . . 674
Was sind Ressourcenpools . . . 676
Erstellen von Ressourcenpools . . . 676
Ressourcenpools bearbeiten . . . 677
Anzeigen des Ressourcenpoolbestands . . . 677
Hinzufügen von Ressourcenpoolmitgliedern . . . 677
Entfernen von Aggregaten aus Ressourcenpools . . . 678
Ressourcenpools löschen . . . 678
Überwachen der Schutzbeziehungen für Storage-VM-Disaster-Recovery . . . 679
Grundlegendes zu Storage-VM-Zuordnungen . . . 681
SVM- und Ressourcenpoolanforderungen zur Unterstützung von Speicherdiensten . . . 683
Welche Jobs sind . . . 684
Überwachen von Jobs . . . 684

Jobdetails anzeigen . . . 685
Jobs abbrechen . . . 685
Wiederholen Sie einen fehlgeschlagenen Schutzauftrag . . . 685
Beschreibung der Fenster und Dialogfelder zu Schutzbeziehungen . . . 686
Erstellen Sie benutzerdefinierte Berichte . . . 730
Einheitliche Manager-Berichterstellung . . . 730
Zugriffspunkte zum Erstellen von Berichten . . . 730
Berichte verstehen . . . 732
Verstehen der Ansichts- und Berichtsbeziehung . . . 732
Berichtstypen . . . 733
Berichtseinschränkungen . . . 735
Arbeiten mit Berichten . . . 735
Berichtsworkflow . . . 735
Schnellstart zur Berichterstellung . . . 736
Suchen nach einem geplanten Bericht . . . 738
Berichte anpassen . . . 739
Berichte herunterladen . . . 742
Berichte planen . . . 742
Planen eines Berichts . . . 742
Berichtszeitpläne verwalten . . . 744
Beispiele für benutzerdefinierte Berichte . . . 746
Anpassen von Cluster-Speicherberichten . . . 746
Anpassen aggregierter Kapazitätsberichte . . . 749
Anpassen von Volume-Kapazitätsberichten . . . 752
Passen Sie Qtree-Kapazitätsberichte an . . . 755
Anpassen von NFS-Freigabeberichten . . . 756
Anpassen von Speicher-VM-Berichten . . . 758
Anpassen von Volumenbeziehungsberichten . . . 759
Anpassen von Volume-Leistungsberichten . . . 763
Beispiele für Microsoft Excel-Berichte . . . 764
Erstellen Sie einen Bericht, um eine Tabelle und ein Diagramm zur Gesamtkapazität anzuzeigen . . . 765
Erstellen Sie einen Bericht, um Diagramme mit der Gesamtsumme und der verfügbaren Kapazität anzuzeigen . . . 766
Erstellen Sie einen Bericht, um Diagramme zur verfügbaren Datenträgerkapazität anzuzeigen . . . 768
Erstellen Sie einen Bericht, um Aggregate mit den meisten verfügbaren IOPS anzuzeigen . . . 769
Verwalten des Speichers mithilfe von REST-APIs . . . 772
Erste Schritte mit Active IQ Unified Manager REST-APIs . . . 772
Zielgruppe für diesen Inhalt . . . 772
Active IQ Unified Manager API-Zugriff und Kategorien . . . 772
Im Active IQ Unified Manager angebotene REST-Dienste . . . 774
API-Version im Active IQ Unified Manager . . . 774
Speicherressourcen in ONTAP . . . 775
REST-API-Zugriff und Authentifizierung im Active IQ Unified Manager . . . 776
Authentifizierung . . . 778
Im Active IQ Unified Manager verwendete HTTP-Statuscodes . . . 778

Empfehlungen zur Verwendung der APIs für Active IQ Unified Manager . . . 780
Protokolle zur Fehlerbehebung . . . 780
Jobobjekte asynchrone Prozesse . . . 781
Hallo API-Server . . . 782
Unified Manager REST-APIs . . . 786
Verwalten von Speicherobjekten in einem Rechenzentrum mithilfe von APIs . . . 787
Greifen Sie über Proxy-Zugriff auf ONTAP -APIs zu . . . 794
Ausführen von Verwaltungsaufgaben mithilfe von APIs . . . 797
Verwalten von Benutzern mithilfe von APIs . . . 799
Anzeigen von Leistungsmetriken mithilfe von APIs . . . 800
Anzeigen von Jobs und Systemdetails . . . 811
Verwalten von Ereignissen und Warnungen mithilfe von APIs . . . 812
Verwalten von Workloads mithilfe von APIs . . . 816
Gängige API-Workflows für die Speicherverwaltung . . . 825
Verstehen Sie die in den Workflows verwendeten API-Aufrufe . . . 825
Ermitteln von Platzproblemen in Aggregaten mithilfe von APIs . . . 825
Ermitteln Sie Probleme in Speicherobjekten mithilfe von Ereignis-APIs . . . 827
Fehlerbehebung bei ONTAP -Volumes mithilfe von Gateway-APIs . . . 828
API-Workflows für das Workload-Management . . . 833
Rechtliche Hinweise . . . 860
Copyright . . . 860
Marken . . . 860
Patente . . . 860
Datenschutzrichtlinie . . . 860
Open Source . . . 860

Active IQ Unified Manager Dokumentation

Versionshinweise

Bietet eine Zusammenfassung der neuen Funktionen, Einschränkungen und bekannten Probleme für Active IQ Unified Manager 9.16.

Weitere Informationen finden Sie im "Versionshinweise zu Active IQ Unified Manager" .

Erste Schritte

Schnellstartanleitung für VMware-Installationen

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

Systemanforderungen

- Betriebssystem: VMware ESXi 8.0
- Arbeitsspeicher: 12 GB
- CPU: 9572 MHz gesamt
- Freier Speicherplatz: 5 GB (Thin Provisioning), 152 GB (Thick Provisioning)

Ausführliche Systemanforderungen finden Sie im"Voraussetzungen für die Installation von Unified Manager" Und"Interoperabilitätsmatrix" .

Installieren Sie Active IQ Unified Manager

Laden Sie das Installationsprogramm herunter

1. Laden Sie die `.tar` Datei, die ein Stammzertifikat enthält, ein `README` Datei und eine `OVA` Datei.
2. Speichern Sie die Datei in einem lokalen Verzeichnis oder Netzwerkverzeichnis, auf das Ihr vSphere-Client zugreifen kann.
3. In dem Verzeichnis, in das Sie die `.tar` Datei, geben Sie die `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz` Befehl. + Die erforderlichen `OVA` Datei, ein Stammzertifikat und ein `README` Datei werden in das Zielverzeichnis entpackt.

Integrität überprüfen

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

Unified Manager installieren

1. Klicken Sie im vSphere Client auf **Datei > OVF-Vorlage bereitstellen**.
2. Suchen Sie die OVA-Datei und verwenden Sie den Assistenten, um die virtuelle Appliance auf dem ESXi-Server bereitzustellen.
3. Auf der Seite „Überprüfungsdetails“ im Abschnitt „Herausgeber“ wird die Meldung `Entrust Code Signing - OVCS2 (Trusted certificate)` bestätigt die Integrität der heruntergeladenen `OVA` Datei. Für die Nachricht `Entrust Code Signing - OVCS2 (Invalid certificate)` , aktualisieren Sie den VMware vCenter Server auf Version 7.0U3E oder höher.
4. Füllen Sie auf der Seite „Vorlage anpassen“ auf der Registerkarte „Eigenschaften“ die Felder entsprechend dem von Ihnen durchgeführten Installationstyp aus:
   - Geben Sie für die statische Konfiguration die erforderlichen Informationen in alle Felder ein. Das Hinzufügen von Informationen für das Feld **Sekundärer DNS** ist nicht erforderlich.
   - Geben Sie für DHCP mit IPv4 in keinem Feld Informationen ein.

    - Aktivieren Sie für DHCP mit IPv6 das Kontrollkästchen „Automatische IPv6-Adressierung aktivieren“. Fügen Sie in keinem anderen Feld Informationen hinzu.
5. Schalten Sie die VM ein.
6. Klicken Sie auf die Registerkarte „Konsole“, um den ersten Startvorgang anzuzeigen.
7. Konfigurieren Sie die Zeitzone.
8. Geben Sie einen Unified Manager-Wartungsbenutzernamen und ein Kennwort ein.

Am Ende der Installation werden die Informationen zur Verbindung mit der Unified Manager-Web-Benutzeroberfläche angezeigt.

Schnellstartanleitung für Linux-Installationen

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

Systemanforderungen

- Betriebssystem: Red Hat Enterprise Linux Versionen 8.x und 9.4, basierend auf der x86_64-Architektur, installiert mit der Basisumgebung „Server mit GUI“ aus der Option **Softwareauswahl** des Betriebssysteminstallationsprogramms
- RAM: 12 GB, CPU: 9572 MHz gesamt
- Freier Speicherplatz: 100 GB Speicherplatz im `/opt/netapp/data` Verzeichnis, 50 GB in der Root-Partition. Für separat montierte `/opt` Und `/var/log` Verzeichnisse, stellen Sie sicher, dass `/opt` hat 15 GB, `/var/log` hat 16 GB und `/tmp` hat 10 GB freien Speicherplatz.

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

Installieren Sie Active IQ Unified Manager

Laden Sie das Installationsprogramm herunter

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

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

Integrität überprüfen

Führen Sie die folgenden Befehle aus, um die Integrität des Installationspakets zu überprüfen:

- Laufen `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>` um eine Datei mit dem öffentlichen Schlüssel aus dem Codesignaturzertifikat zu erstellen.
- Laufen `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip` um die Signatur des

Installationspakets zu überprüfen.

Überprüfen der Repository-Konfiguration

Die Verfahren zum Konfigurieren eines Red Hat Enterprise Linux-Repository sind standortspezifisch. Sie können die `pre_install_check.sh` im Installationspaket enthaltenes Skript zum Überprüfen der Konfiguration Ihres Betriebssystems. Wenn Ihr System mit dem Internet verbunden ist, erhalten Sie automatisch Anweisungen zum Einrichten des Red Hat Enterprise Linux-Repository.

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

Unified Manager installieren

Unified Manager verwendet die `yum` Dienstprogramm zum Installieren der Software und aller abhängigen Software. Da es unterschiedliche Images von Red Hat Enterprise Linux gibt, hängen die installierten Pakete von der in den Images vorhandenen Software ab. Der `yum` Das Dienstprogramm ermittelt die abhängigen Softwarepakete für die Installation. Wenn Sie weitere Informationen zu den abhängigen Softwarepaketen benötigen, lesen Sie die"Linux-Software und Installationsanforderungen" .

Um Unified Manager zu installieren, führen Sie den folgenden Befehl entweder als Root-Benutzer oder mit `sudo` , aus dem Verzeichnis, 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 zur Verbindung mit der Unified Manager-Web-Benutzeroberfläche angezeigt. Wenn Sie keine Verbindung zur Web-Benutzeroberfläche herstellen können, lesen Sie die `README` Weitere Informationen zu den Einschränkungen für Port 443 finden Sie in der mit der Software gelieferten Datei.

Schnellstartanleitung für Windows-Installationen

Sie können das Installationspaket herunterladen und Unified Manager installieren, um Probleme mit der Datenspeicherkapazität, Verfügbarkeit, Leistung und dem Schutz zu überwachen und zu beheben.

Systemanforderungen

- Betriebssysteme
  - Microsoft Windows Server 2019 Standard und 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

- Arbeitsspeicher: 12 GB
- CPU: 9572 MHz gesamt
- Freier Speicherplatz: 100 GB Speicherplatz für das Installationsverzeichnis, 50 GB Speicherplatz für das MySQL-Datenverzeichnis

Ausführliche Systemanforderungen finden Sie im"Voraussetzungen für die Installation von Unified Manager" Und"Interoperabilitätsmatrix" .

Installieren Sie Active IQ Unified Manager

Laden Sie das Installationsprogramm herunter

1. Laden Sie die `ActiveIQUnifiedManager-<version>.exe` Installationspaket.
2. Kopieren Sie die Installationsdatei in ein Verzeichnis auf dem Zielsystem.

Unified Manager installieren

Stellen Sie für die Installation von Unified Manager sicher, dass Sie Microsoft .NET 4.5.2 oder eine neuere Version installiert haben. Als Teil des Installationsprozesses installiert Unified Manager bei Bedarf andere Pakete von Drittanbietern. Weitere Informationen zu den abhängigen Softwarepaketen finden Sie im"Windows-Software- und Installationsanforderungen" .

1. Melden Sie sich mit dem standardmäßigen lokalen Administratorkonto bei Windows an.
2. Klicken Sie mit der rechten Maustaste in das Verzeichnis, in das Sie die Installationsdatei heruntergeladen haben, und führen Sie die ausführbare Datei (.exe) von Unified Manager als Administrator aus.
3. Geben Sie bei der entsprechenden Aufforderung den Benutzernamen und das Kennwort ein, um den Unified Manager-Wartungsbenutzer zu erstellen.
4. Geben Sie im Datenbankverbindungsassistenten das MySQL-Root-Passwort ein.
5. Folgen Sie den weiteren Anweisungen, um die Installation abzuschließen.
6. Klicken Sie am Ende der Installation auf **Fertig** und die Unified Manager-Web-Benutzeroberfläche wird angezeigt.

Installieren Sie Unified Manager auf VMware vSphere-Systemen

Einführung in Active IQ Unified Manager

Mit Active IQ Unified Manager (früher OnCommand Unified Manager) können Sie den Zustand und die Leistung Ihrer ONTAP -Speichersysteme über eine einzige Schnittstelle überwachen und verwalten. Sie können Unified Manager auf einem Linux-Server, einem Windows-Server oder als virtuelle Appliance auf einem VMware-Host bereitstellen.

Nachdem Sie die Installation abgeschlossen und die Cluster hinzugefügt haben, die Sie verwalten möchten, bietet Unified Manager eine grafische Benutzeroberfläche, die die Kapazität, Verfügbarkeit, den Schutz und den Leistungsstatus der überwachten Speichersysteme anzeigt.

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Was der Unified Manager-Server macht

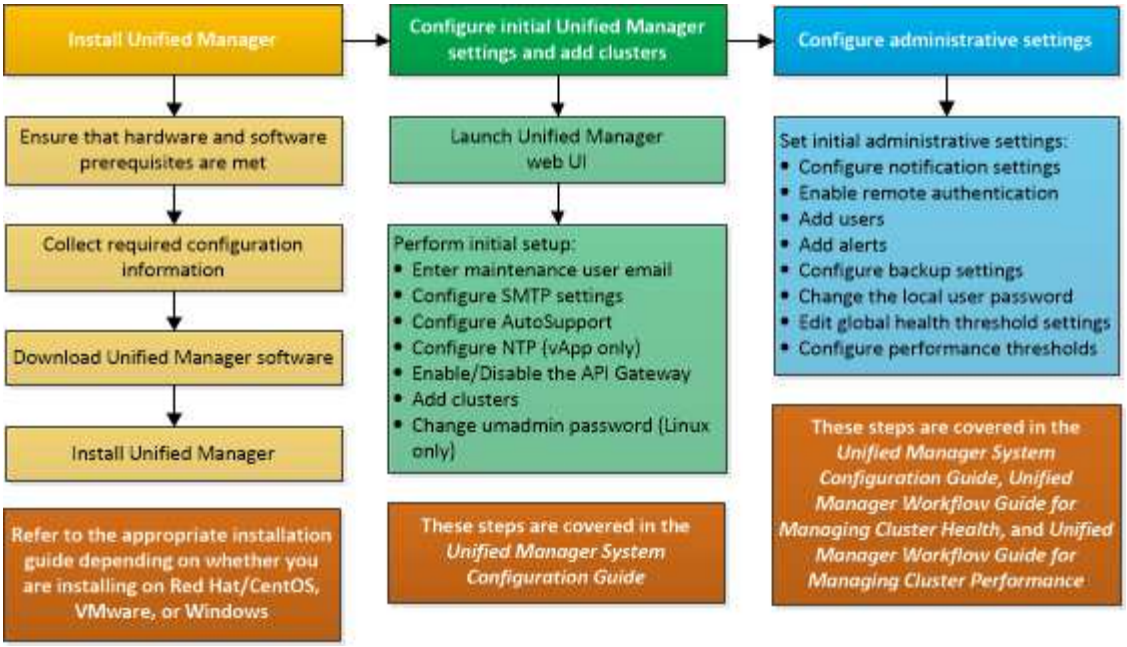
Die Unified Manager-Serverinfrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Anwendungsserver. Es bietet Infrastrukturdienste wie Erkennung, Überwachung, rollenbasierte Zugriffskontrolle (RBAC), Auditing und Protokollierung.

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

Übersicht über den Installationsablauf

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

In diesen Abschnitten werden alle im folgenden Arbeitsablauf angezeigten Elemente beschrieben.



Voraussetzungen für die Installation von Unified Manager

Stellen Sie vor Beginn des Installationsvorgangs sicher, dass der Server, auf dem Sie Unified Manager installieren möchten, die spezifischen Software-, Hardware-, CPU- und Speicheranforderungen erfüllt.

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

Weitere Einzelheiten zum Anwenden von Sicherheitsmaßnahmen auf den Unified Manager-Server finden Sie im 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"

Anforderungen an die virtuelle Infrastruktur und das Hardwaresystem

Die Installation von Unified Manager auf einer virtuellen Infrastruktur oder einem physischen System sollte die Mindestanforderungen an Arbeitsspeicher, CPU und Festplattenspeicher erfüllen.

In der folgenden Tabelle sind die empfohlenen Werte für Arbeitsspeicher-, CPU- und Festplattenspeicherressourcen aufgeführt. Diese Werte wurden qualifiziert, sodass Unified Manager akzeptable Leistungsniveaus erreicht.

Hardwarekonfiguration	Empfohlene Einstellungen
RAM	12 GB (Mindestanforderung 8 GB)
Prozessoren	4 CPUs
CPU-Zykluskapazität	9572 MHz gesamt (Mindestanforderung 9572 MHz)
Freier Speicherplatz	• 5 GB (Thin Provisioning) • 152 GB (Thick Provisioning)

Unified Manager kann auf Systemen mit wenig Arbeitsspeicher installiert werden, die empfohlenen 12 GB RAM stellen jedoch sicher, dass genügend Arbeitsspeicher für eine optimale Leistung zur Verfügung steht und dass das System bei wachsender Konfiguration zusätzliche Cluster und Speicherobjekte aufnehmen kann. Sie sollten auf der VM, auf der Unified Manager bereitgestellt wird, keine Speicherbeschränkungen festlegen und keine Funktionen (z. B. Ballooning) aktivieren, die die Software daran hindern, den zugewiesenen Speicher auf dem System zu nutzen.

Darüber hinaus gibt es eine Begrenzung für die Anzahl der Knoten, die eine einzelne Instanz von Unified Manager überwachen kann, bevor Sie eine zweite Instanz von Unified Manager installieren. Weitere Informationen finden Sie unter "Leitfaden zu Best Practices für Unified Manager".

Das Auslagern von Speicherseiten wirkt sich negativ auf die Leistung des Systems und der Verwaltungsanwendung aus. Der Wettbewerb um CPU-Ressourcen, die aufgrund der Gesamtauslastung des Hosts nicht verfügbar sind, kann die Leistung beeinträchtigen.

Voraussetzung für die dedizierte Nutzung

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, sollte ausschließlich für Unified Manager verwendet und nicht mit anderen Anwendungen geteilt werden. Andere Anwendungen verbrauchen möglicherweise Systemressourcen und können die Leistung von Unified Manager drastisch reduzieren.

Speicherplatzbedarf für Backups

Wenn Sie die Sicherungs- und Wiederherstellungsfunktion von Unified Manager verwenden möchten, weisen Sie zusätzliche Kapazität zu, sodass das Verzeichnis oder die Festplatte „`data`“ über 150 GB Speicherplatz verfügt. Eine Sicherung kann an ein lokales oder ein Remote-Ziel geschrieben werden. Die beste Vorgehensweise besteht darin, einen Remote-Standort außerhalb des Unified Manager-Hostsystems zu identifizieren, der über mindestens 150 GB Speicherplatz verfügt.

Anforderungen für die Hostkonnektivität

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, sollte so konfiguriert sein, dass Sie erfolgreich `ping` der Hostname vom Host selbst. Bei einer IPv6-Konfiguration sollten Sie überprüfen, ob `ping6` zum Hostnamen erfolgreich ist, um sicherzustellen, dass die Installation von Unified Manager erfolgreich ist.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Web-Benutzeroberfläche des Produkts zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie einen Namen für den Netzwerkhost festgelegt. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollten Sie den Hostnamen vom DNS beziehen.

Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen statt über den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse ermöglichen möchten, muss Ihre Netzwerkkonfiguration diesen Kurznamen in einen gültigen FQDN auflösen.

VMware-Software- und Installationsanforderungen

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 führt intern Debian OS 12 (Bookworm) aus. Informationen zu den Versionen der virtuellen Maschinenhardware, die von den unterstützten Versionen von ESXi-Servern unterstützt werden können, finden Sie in der VMware-Dokumentation.

Die folgenden Versionen von vSphere werden unterstützt:

- VMware vCenter Server 7.0 und 8.0

Die vollständige und aktuelle Liste der unterstützten ESXi-Versionen finden Sie in der Interoperabilitätsmatrix.

"mysupport.netapp.com/matrix"

Damit die virtuelle Appliance ordnungsgemäß funktioniert, sollte die Serverzeit von VMware ESXi mit der Serverzeit von NTP übereinstimmen. Durch die Synchronisierung der VMware ESXi-Serverzeit mit der NTP-Serverzeit wird ein Zeitausfall verhindert.

Installationsvoraussetzungen

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

Wenn Sie einen NFS-Datenspeicher auf einem Speichersystem bereitstellen, auf dem ONTAP -Software ausgeführt wird, verwenden Sie das NetApp NFS-Plug-in für VMware VAAI, um Thick Provisioning zu nutzen.

Wenn die Bereitstellung in Ihrer Umgebung mit aktivierter Hochverfügbarkeit aufgrund unzureichender Ressourcen fehlschlägt, müssen Sie möglicherweise die Optionen der virtuellen Maschine für Clusterfunktionen ändern, indem Sie die VM-Neustartpriorität deaktivieren und die Host-Isolationsreaktion eingeschaltet lassen.

> Während der Installation oder Aktualisierung von Unified Manager werden die erforderliche Drittanbietersoftware und Sicherheitspatches automatisch auf einem VMware vSphere-System installiert oder aktualisiert. Da diese Komponenten durch die Installations- und Upgradeprozesse von Unified Manager gesteuert werden, sollten Sie nicht versuchen, eine eigenständige Installation oder ein Upgrade einer Drittanbieterkomponente durchzuführen.

Unterstützte Browser

Verwenden Sie einen unterstützten Browser, um auf die Unified Manager-Web-

Benutzeroberfläche zuzugreifen.

Die Interoperabilitätsmatrix enthält die Liste der unterstützten Browserversionen.

"mysupport.netapp.com/matrix"

Durch die Deaktivierung von Popup-Blockern wird bei allen Browsern sichergestellt, dass 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

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

Verbindungen zum Unified Manager-Server

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

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

Schnittstelle	Protokoll	Hafen	Beschreibung
Unified Manager-Web-Benutzeroberfläche	HTTP	80	Wird für den Zugriff auf die Unified Manager-Web-Benutzeroberfläche verwendet; leitet automatisch zum sicheren Port 443 um.
Unified Manager-Web-UI und Programme mit APIs	HTTPS	443	Wird verwendet, um sicher auf die Unified Manager-Web-Benutzeroberfläche zuzugreifen oder API-Aufrufe zu tätigen; API-Aufrufe können nur über HTTPS erfolgen.
Wartungskonsole	SSH/SFTP	22	Wird verwendet, um auf die Wartungskonsole zuzugreifen und Supportpakete abzurufen.

Schnittstelle	Protokoll	Hafen	Beschreibung
Linux-Befehlszeile	SSH/SFTP	22	Wird verwendet, um auf die Red Hat Enterprise Linux-Befehlszeile zuzugreifen und Support-Pakete abzurufen.
Syslog	UDP	514	Wird verwendet, um auf abonnementbasierte EMS-Nachrichten von ONTAP Systemen zuzugreifen und auf der Grundlage der Nachrichten Ereignisse zu erstellen.
AUSRUHEN	HTTPS	9443	Wird verwendet, um auf REST-API-basierte EMS-Ereignisse in Echtzeit von authentifizierten ONTAP Systemen zuzugreifen.
MySQL-Datenbank	MySQL	3306	Wird verwendet, um den Zugriff auf Unified Manager OnCommand Workflow Automation und OnCommand API Services zu ermöglichen.
AMQP QPID-Broker	TCP/IP	56072	Wird für die interne Nachrichtenkommunikation verwendet.
AMQP QPID-Broker	WebSocket über TCP	56080	Wird verwendet, um auf diesem Port auf von ONTAP (Cloud-Agent) empfangene Nachrichten zu lauschen.
AMQP QPID-Broker	WebSocket über TCP	56443	Wird verwendet, um auf diesem Port auf von ONTAP (Cloud-Agent) empfangene Nachrichten zu lauschen. Die Kommunikation über diesen Port unterstützt die Verschlüsselung durch TLS oder SSL.

Der Standardport für MySQL, 3306, ist bei der Installation von Unified Manager auf VMware vSphere-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 anderen Hosts zur Verfügung gestellt werden, indem man den `Control access to MySQL port 3306` Option auf der Wartungskonsole. Weitere Informationen finden Sie unter"Zusätzliche Menüoptionen" . Die für die HTTP- und HTTPS-Kommunikation verwendeten Ports (Ports 80 und 443) können über die Wartungskonsole von Unified Manager geändert werden. Weitere Informationen finden Sie unter "Menüs der Wartungskonsole".

Verbindungen vom Unified Manager-Server

Sie sollten Ihre Firewall so konfigurieren, dass Ports geöffnet werden, die die Kommunikation zwischen dem Unified Manager-Server und verwalteten Speichersystemen, Servern und anderen Komponenten ermöglichen. Wenn ein Port nicht geöffnet ist, schlägt die Kommunikation fehl.

Abhängig von Ihrer Umgebung können Sie die vom Unified Manager-Server zum Herstellen einer Verbindung mit bestimmten Zielen verwendeten Ports und Protokolle ändern.

Der Unified Manager-Server stellt über die folgenden Protokolle und Ports eine Verbindung zu den verwalteten Speichersystemen, Servern und anderen Komponenten her:

Ziel	Protokoll	Hafen	Beschreibung
Speichersystem	HTTPS	443/TCP	Wird zur Überwachung und Verwaltung von Speichersystemen verwendet. Wenn Sie diesen oder einen anderen Port verwenden, um eine Verbindung zum VMware vCenter Server oder ESXi-Server herzustellen, stellen Sie sicher, 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	Wird zum Senden von AutoSupport -Informationen verwendet. Für die Ausführung dieser Funktion ist ein Internetzugang erforderlich.

Ziel	Protokoll	Hafen	Beschreibung
Authentifizierungsserver	LDAP	389	Wird verwendet, um Authentifizierungsanfragen sowie Benutzer- und Gruppensuchanfragen zu stellen.
LDAPS	636	Wird für die sichere LDAP-Kommunikation verwendet.	Mailserver
SMTP	25	Wird zum Senden von E-Mail-Benachrichtigungen verwendet.	SNMP-Trap-Sender
SNMPv1 oder SNMPv3	162/UDP	Wird zum Senden von SNMP-Traps für Warnbenachrichtigungen verwendet.	Externer Datenanbieterserver
TCP	2003	Wird verwendet, um Leistungsdaten an einen externen Datenanbieter wie Graphite zu senden.	NTP-Server
NTP	123/UDP	Wird verwendet, um die Zeit auf dem Unified Manager-Server mit einem externen NTP-Zeitserver zu synchronisieren. (Nur VMware-Systeme)	Syslog

Füllen Sie das Arbeitsblatt aus

Bevor Sie Unified Manager installieren und konfigurieren, sollten Sie bestimmte Informationen zu Ihrer Umgebung zur Hand haben. Sie können die Informationen im Arbeitsblatt festhalten.

Unified Manager-Installationsinformationen

Die zur Installation von Unified Manager erforderlichen Details.

System, auf dem die Software bereitgestellt wird	Ihr Wert
IP-Adresse des ESXi-Servers	
Vollqualifizierter Domänenname des Hosts	

System, auf dem die Software bereitgestellt wird	Ihr Wert
Host-IP-Adresse	
Netzwerkmaske	
Gateway-IP-Adresse	
Primäre DNS-Adresse	
Sekundäre DNS-Adresse	
Suchdomänen	
Wartungsbenutzername	
Wartungsbenutzerkennwort	

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	
Hostname oder IP-Adresse des SMTP-Servers	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Port	25 (Standardwert)
E-Mail, von der Warnbenachrichtigungen gesendet werden	
Hostname oder IP-Adresse des Authentifizierungsservers	
Active Directory-Administratorname oder LDAP-Bind-Distinguished Name	

Einstellung	Ihr Wert
Active Directory-Passwort oder LDAP-Bind-Passwort	
Basis-Distinguished Name des Authentifizierungsservers	
URL des Identitätsanbieters (IdP)	
Metadaten des Identitätsanbieters (IdP)	
IP-Adressen des SNMP-Trap-Zielhosts	
SNMP-Port	

Cluster-Informationen

Die Details für die Speichersysteme, die Sie mit Unified Manager verwalten.

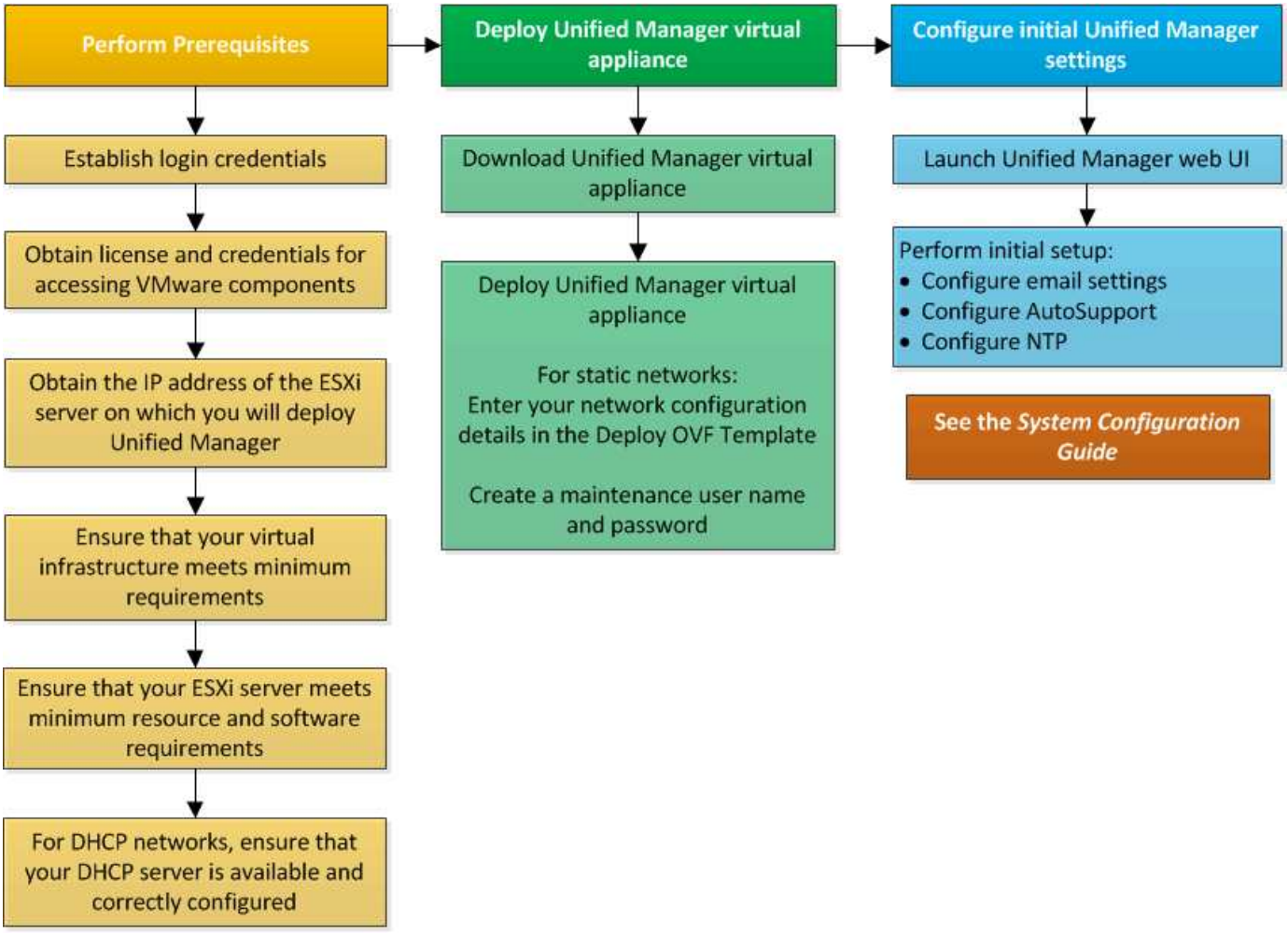
Cluster 1 von N	Ihr Wert
Hostname oder IP-Adresse zur Clusterverwaltung	
ONTAP -Administratorbenutzername Dem Administrator muss die Rolle „`admin`“ zugewiesen worden sein.	
ONTAP -Administratorkennwort	
Protokoll	HTTPS

Installieren, aktualisieren und entfernen Sie die Unified Manager-Software

Auf VMware vSphere-Systemen können Sie Unified Manager installieren, auf eine neuere Version der Software aktualisieren oder die virtuelle Appliance (vApp) von Unified Manager entfernen.

Übersicht über den Bereitstellungsprozess

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



Unified Manager bereitstellen

Die Bereitstellung von Unified Manager umfasst das Herunterladen von Software, die Bereitstellung der virtuellen Appliance, das Erstellen eines Wartungsbenutzernamens und -kennworts und die Durchführung der Ersteinrichtung in der Web-Benutzeroberfläche.

Bevor Sie beginnen

- Sie sollten die Systemanforderungen für die Bereitstellung überprüfen und erfüllen.

  Sehen"Systemanforderungen" .

- Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen:
  - Anmeldeinformationen 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 Rechenzentrum, wie Speicherplatz im Datastore und Speicherbedarf
  - Wenn Sie die IPv6-Adressierung verwenden möchten, sollte IPv6 auf dem Host aktiviert sein.

Sie können Unified Manager als virtuelle Appliance auf einem VMware ESXi-Server bereitstellen.

Sie sollten über die VMware-Konsole und nicht über SSH auf die Wartungskonsole zugreifen.

Ab Unified Manager 9.8 wurden VMware Tools durch Open VM Tools ersetzt `open-vm-tools`). Sie müssen VMware Tools nicht mehr als Teil der Installation installieren, da `open-vm-tools` ist im Unified Manager-Installationspaket enthalten.

Nach Abschluss der Bereitstellung und Ersteinrichtung können Sie entweder Cluster hinzufügen oder zusätzliche Netzwerkeinstellungen in der Wartungskonsole konfigurieren und dann auf die Web-Benutzeroberfläche zugreifen.

Schritte

1. Befolgen Sie die Schritte in"Unified Manager herunterladen" .
2. Befolgen Sie außerdem die Schritte in"Bereitstellen der virtuellen Unified Manager-Appliance" .

Laden Sie die Unified Manager-Installationsdatei herunter

Laden Sie die Installationsdatei für Unified Manager von der NetApp Support-Site herunter, um Unified Manager als virtuelle Appliance bereitzustellen.

Bevor Sie beginnen

Sie sollten über die Anmeldeinformationen für die NetApp Support-Site verfügen.

Die Installationsdatei ist eine `.tar` Datei, die ein Stammzertifikat enthält, ein `README` Datei und eine `OVA` Datei mit der für eine virtuelle Appliance konfigurierten Unified Manager-Software.

Schritte

1. Melden Sie sich bei der NetApp Support-Site an und navigieren Sie zur Download-Seite für Unified Manager:

   "NetApp Support Site"

2. Wählen Sie die erforderliche Version von Unified Manager aus und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA).
3. Laden Sie die `.tar` Datei für die VMware vSphere-Installation in ein lokales Verzeichnis oder Netzwerkverzeichnis, auf das Ihr vSphere-Client zugreifen kann.
4. Überprüfen Sie die Prüfsumme, um sicherzustellen, dass die Software korrekt heruntergeladen wurde.
5. Navigieren Sie zu dem Verzeichnis, in das Sie die `.tar` Datei und geben Sie den folgenden Befehl in Ihr Terminalfenster ein, um das Unified Manager-Paket zu erweitern:

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

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

6. Überprüfen Sie die Integrität der `OVA` Datei, indem Sie die Schritte in der `README` Datei.

Bereitstellen der virtuellen Unified Manager-Appliance

Nachdem Sie die Installationsdatei heruntergeladen haben, stellen Sie Unified Manager als virtuelle Appliance bereit. Verwenden Sie den vSphere Web Client, um die virtuelle

Appliance auf einem ESXi-Server bereitzustellen. Wenn Sie die virtuelle Appliance bereitstellen, wird eine virtuelle Maschine erstellt.

Bevor Sie beginnen

Sie sollten die Systemanforderungen überprüfen. Nehmen Sie die erforderlichen Änderungen vor, bevor Sie die virtuelle Unified Manager-Appliance bereitstellen.

Sehen"Anforderungen an die virtuelle Infrastruktur" .

Sehen"VMware-Software- und Installationsanforderungen" .

Wenn Sie das Dynamic Host Configuration Protocol (DHCP) verwenden, stellen Sie sicher, dass der DHCP-Server verfügbar ist und dass die DHCP- und VM-Netzwerkadapterkonfigurationen korrekt sind. DHCP ist standardmäßig konfiguriert.

Wenn Sie eine statische Netzwerkkonfiguration verwenden, stellen Sie sicher, dass die IP-Adresse nicht im selben Subnetz dupliziert wird und dass die entsprechenden DNS-Servereinträge konfiguriert wurden.

Besorgen Sie sich vor der Bereitstellung der virtuellen Appliance die folgenden Informationen:

- 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 Rechenzentrum, wie beispielsweise die Verfügbarkeit von Speicherplatz
- Wenn Sie DHCP nicht verwenden, ermitteln Sie die IPv4- oder IPv6-Adressen für die Netzwerkgeräte, zu denen Sie eine Verbindung herstellen möchten:
  - Vollqualifizierter Domänenname (FQDN) des Hosts
  - IP-Adresse des Hosts
  - Netzwerkmaske
  - IP-Adresse des Standard-Gateways
  - Primäre und sekundäre DNS-Adressen
  - Suchdomänen

Ab Unified Manager 9.8 wurden VMware Tools durch Open VM Tools ersetzt `open-vm-tools`). Sie müssen VMware Tools nicht als Teil des Installationsprozesses installieren, da `open-vm-tools` ist im Unified Manager-Installationspaket enthalten.

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

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

Schritte

1. Klicken Sie im vSphere Client auf **Datei** > **OVF-Vorlage bereitstellen**.
2. Schließen Sie den Assistenten „OVF-Vorlage bereitstellen“ ab, um die virtuelle Unified Manager-Appliance bereitzustellen.

   Auf der Seite „Bewertungsdetails“:

- Überprüfen Sie die Details im Abschnitt „Herausgeber“. Die Meldung **Entrust Code Signing - OVCS2 (Trusted certificate)** bestätigt die Integrität des heruntergeladenen `OVA` Datei. + Wenn die Meldung **Entrust Code Signing – OVCS2 (Ungültiges Zertifikat)** angezeigt wird, aktualisieren Sie den VMware vCenter Server auf Version 7.0U3E oder höher.

  Auf der Seite „Vorlage anpassen“:

- Lassen Sie alle Felder leer, wenn Sie DHCP- und IPv4-Adressierung verwenden.
- Aktivieren Sie das Kontrollkästchen „Automatische IPv6-Adressierung aktivieren“ und lassen Sie alle anderen Felder leer, wenn Sie DHCP- und IPv6-Adressierung verwenden.
- Wenn Sie eine statische Netzwerkkonfiguration verwenden möchten, können Sie die Felder auf dieser Seite ausfüllen und diese Einstellungen werden während der Bereitstellung angewendet. Stellen Sie sicher, dass die IP-Adresse für den Host, auf dem sie bereitgestellt wird, eindeutig ist, dass sie nicht bereits verwendet wird und dass sie über einen gültigen DNS-Eintrag verfügt.

3. Nachdem die virtuelle Unified Manager-Appliance auf dem ESXi-Server bereitgestellt wurde, schalten Sie die VM ein, indem Sie mit der rechten Maustaste auf die VM klicken und dann **Einschalten** auswählen.

   Wenn der Einschaltvorgang aufgrund unzureichender Ressourcen fehlschlägt, fügen Sie Ressourcen hinzu und wiederholen Sie die Installation.

4. Klicken Sie auf die Registerkarte **Konsole**.

   Der erste Startvorgang dauert einige Minuten.

5. Um Ihre Zeitzone zu konfigurieren, geben Sie Ihr geografisches Gebiet und Ihre Stadt oder Region ein, wie im VM-Konsolenfenster aufgefordert.

   Alle angezeigten Datumsinformationen verwenden die für Unified Manager konfigurierte Zeitzone, unabhängig von der Zeitzoneneinstellung auf Ihren verwalteten Geräten. Wenn Ihre Speichersysteme und der Verwaltungsserver mit demselben NTP-Server konfiguriert sind, beziehen sie sich auf denselben Zeitpunkt, auch wenn sie unterschiedlich erscheinen. Wenn Sie beispielsweise eine Snapshot-Kopie mit einem Gerät erstellen, das mit einer anderen Zeitzone als der des Verwaltungsservers konfiguriert ist, entspricht der Zeitstempel der Zeit des Verwaltungsservers.

6. Wenn keine DHCP-Dienste verfügbar sind oder ein Fehler in den Angaben zur statischen Netzwerkkonfiguration vorliegt, wählen Sie eine der folgenden Optionen:

Wenn Sie verwenden…	Dann tun Sie Folgendes …
DHCP	Wählen Sie **DHCP erneut versuchen**. Wenn Sie DHCP verwenden möchten, sollten Sie sicherstellen, dass es richtig konfiguriert ist. Wenn Sie ein DHCP-fähiges Netzwerk verwenden, werden die FQDN- und DNS-Servereinträge automatisch an die virtuelle Appliance vergeben. Wenn DHCP nicht richtig mit DNS konfiguriert ist, wird der Hostname „UnifiedManager“ automatisch zugewiesen und mit dem Sicherheitszertifikat verknüpft. Wenn Sie kein DHCP-fähiges Netzwerk eingerichtet haben, sollten Sie die Netzwerkkonfigurationsinformationen manuell eingeben.
Eine statische Netzwerkkonfiguration	a. Wählen Sie **Geben Sie die Details für die statische Netzwerkkonfiguration ein**. Der Konfigurationsvorgang dauert einige Minuten. b. Bestätigen Sie die eingegebenen Werte und wählen Sie **Y**.

7. Geben Sie bei der Eingabeaufforderung einen Wartungsbenutzernamen ein und klicken Sie dann auf **Eingabe**.

   Der Wartungsbenutzername sollte mit einem Buchstaben von a bis z beginnen, gefolgt von einer beliebigen Kombination aus -, a bis z oder 0 bis 9.

8. Geben Sie bei der Eingabeaufforderung ein Kennwort ein und klicken Sie dann auf **Eingabe**.

   Die VM-Konsole zeigt die URL für die Unified Manager-Web-Benutzeroberfläche an.

Sie können auf die Web-Benutzeroberfläche zugreifen, um die Ersteinrichtung von Unified Manager durchzuführen, wie im Abschnitt"Konfigurieren von Active IQ Unified Manager" .

Upgrade von Unified Manager

Sie können Active IQ Unified Manager nur von Version 9.13 oder 9.14 auf Version 9.16 aktualisieren.

Während des Upgrade-Vorgangs ist Unified Manager nicht verfügbar. Sie sollten alle laufenden Vorgänge abschließen, bevor Sie Unified Manager aktualisieren.

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 der Durchführung der Upgrades eine neue Workflow Automation-Verbindung einrichten. Wenn Sie ein Upgrade nur für eines der Produkte durchführen, sollten Sie sich nach dem Upgrade bei Workflow Automation anmelden und überprüfen, ob weiterhin Daten vom Unified Manager abgerufen werden.

Schritte

1. Befolgen Sie die Schritte in"Laden Sie das ISO-Image von Unified Manager herunter" .
2. Befolgen Sie außerdem die Schritte in"Upgrade von Unified Manager" .

Unterstützter Upgrade-Pfad für Unified Manager-Versionen

Active IQ Unified Manager unterstützt für jede Version einen bestimmten Upgradepfad.

Nicht alle Versionen von Unified Manager können ein direktes Upgrade auf neuere Versionen durchführen. Die Unified Manager-Upgrades sind auf ein N-2-Modell beschränkt, d. h. ein Upgrade kann auf allen Plattformen nur innerhalb der nächsten zwei Versionen durchgeführt werden. Sie können beispielsweise nur von Unified Manager 9.13 und 9.14 ein Upgrade auf Unified Manager 9.16 durchführen.

Wenn Sie eine Version ausführen, die älter ist als die unterstützten Versionen, muss Ihre Unified Manager-Instanz zuerst auf eine der unterstützten Versionen und dann auf die aktuelle Version aktualisiert werden.

Wenn Sie beispielsweise die Version Unified Manager 9.9 installiert haben und auf Unified Manager 9.14 aktualisieren möchten, befolgen Sie eine Upgrade-Reihenfolge.

Beispielhafter Upgradepfad:

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

Weitere Informationen zur Upgrade-Pfadmatrix finden Sie hier "Wissensdatenbankartikel (KB)" .

Laden Sie die Unified Manager-Upgradedatei herunter

Laden Sie vor dem Upgrade von Unified Manager die Upgrade-Datei für Unified Manager von der NetApp Support-Site herunter.

Bevor Sie beginnen

Sie sollten über Anmeldeinformationen für die NetApp Support-Site verfügen.

Schritte

1. Melden Sie sich bei der NetApp Support-Site an:

   "NetApp Support Site"

2. Navigieren Sie zur Download-Seite, um Unified Manager auf VMware vSphere zu aktualisieren.
3. Laden Sie die `.iso` Image für das Upgrade und speichern Sie es in einem lokalen Verzeichnis oder Netzwerkverzeichnis, auf das Ihr vSphere-Client zugreifen kann.
4. Überprüfen Sie die Prüfsumme, um sicherzustellen, dass die Software korrekt heruntergeladen wurde.

Aktualisieren Sie die virtuelle Unified Manager-Appliance

Sie können die virtuelle Appliance Active IQ Unified Manager von den Versionen 9.13 oder 9.14 auf 9.16 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, erfüllt die System- und Softwareanforderungen.

  Sehen"Anforderungen an die virtuelle Infrastruktur" .

  Sehen"VMware-Software- und Installationsanforderungen" .

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

Während des Upgrade-Vorgangs ist Unified Manager nicht verfügbar. Sie sollten alle laufenden Vorgänge abschließen, bevor Sie Unified Manager aktualisieren.

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

Schritte

1. Klicken Sie im vSphere-Client auf **Home** > **Inventar** > **VMs und Vorlagen**.
2. Wählen Sie die virtuelle Maschine (VM) aus, auf der die virtuelle Unified Manager-Appliance installiert ist.
3. Wenn die Unified Manager-VM ausgeführt wird, navigieren Sie zu **Zusammenfassung** > **Befehle** > **Gast herunterfahren**.
4. Erstellen Sie eine Sicherungskopie, z. B. einen Snapshot oder einen Klon, der Unified Manager-VM, um eine anwendungskonsistente Sicherung zu erstellen.
5. Schalten Sie die Unified Manager-VM vom vSphere-Client aus ein.
6. Starten Sie die VMware Remote Console.
7. Klicken Sie auf das Symbol **CD-ROM** und wählen Sie **Mit Disk-Image-Datei (.iso) verbinden**.
8. Wählen Sie die `ActiveIQUnifiedManager-<version>-virtual-update.iso` Datei und klicken Sie auf **Öffnen**.
9. Klicken Sie auf die Registerkarte **Konsole**.
10. Melden Sie sich bei der Wartungskonsole von Unified Manager an.
11. Wählen Sie im Hauptmenü **Upgrade**.

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

12. Typ `y` , um fortzufahren.

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

13. Typ `y` , um fortzufahren.

    Der Upgrade-Vorgang und der Neustart der Unified Manager-Dienste können mehrere Minuten dauern.

14. Drücken Sie eine beliebige Taste, um fortzufahren.

    Sie werden automatisch von der Wartungskonsole abgemeldet.

15. **Optional:** Melden Sie sich bei der Wartungskonsole an und überprüfen Sie die Version von Unified Manager.

Sie können die Web-Benutzeroberfläche in einem neuen Fenster eines unterstützten Webbrowsers starten und sich anmelden, um die aktualisierte Version von Unified Manager zu verwenden. Beachten Sie, dass Sie warten müssen, bis der Erkennungsprozess abgeschlossen ist, bevor Sie eine Aufgabe in der Benutzeroberfläche ausführen.

Starten Sie die virtuelle Unified Manager-Maschine neu

Sie können die virtuelle Maschine (VM) von Unified Manager über die Wartungskonsole neu starten. Sie sollten die VM neu starten, nachdem Sie ein neues Sicherheitszertifikat generiert haben oder wenn ein Problem mit der VM vorliegt.

Bevor Sie beginnen

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

Sie können die virtuelle Maschine auch von vSphere aus neu starten, indem Sie die VMware-Option „Gast neu starten“ verwenden. Siehe "das Cmdlet „Restart-VMGuest“ in der VMware vSphere PowerCLI CMDLET-Referenz von Broadcom."

Schritte

1. Wählen Sie in der Wartungskonsole **Systemkonfiguration** > **Virtuelle Maschine neu starten**.
2. Starten Sie die Unified Manager-Web-Benutzeroberfläche in Ihrem Browser und melden Sie sich an.

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 sollten über Anmeldeinformationen für den Zugriff auf VMware vCenter Server und vSphere Web Client verfügen.
- Jede aktive Verbindung des Unified Manager-Servers zu einem Workflow Automation-Server sollte geschlossen werden.
- Alle Cluster (Datenquellen) sollten vom Unified Manager-Server entfernt werden, bevor Sie die virtuelle Maschine (VM) entfernen.

Schritte

1. Verwenden Sie die Unified Manager-Wartungskonsole, um zu überprüfen, dass der Unified Manager-Server keine aktive Verbindung zu einem externen Datenanbieter hat.
2. Klicken Sie im vSphere-Client auf **Home** > **Inventar** > **VMs und Vorlagen**.
3. Wählen Sie die VM aus, die Sie entfernen möchten, und klicken Sie auf die Registerkarte **Zusammenfassung**.
4. Wenn die VM ausgeführt wird, klicken Sie auf **Power** > **Gast herunterfahren**.
5. Klicken Sie mit der rechten Maustaste auf die VM, die Sie entfernen möchten, und klicken Sie auf **Von Festplatte löschen**.

Installieren Sie Unified Manager auf Linux-Systemen

Einführung in Active IQ Unified Manager

Mit Active IQ Unified Manager (früher OnCommand Unified Manager) können Sie den Zustand und die Leistung Ihrer ONTAP -Speichersysteme über eine einzige Schnittstelle überwachen und verwalten. Sie können Unified Manager auf einem Linux-Server, einem Windows-Server oder als virtuelle Appliance (vApp) auf einem VMware-Host bereitstellen.

Nachdem Sie die Installation abgeschlossen und die Cluster hinzugefügt haben, die Sie verwalten möchten, bietet Unified Manager eine grafische Benutzeroberfläche, die die Kapazität, Verfügbarkeit, den Schutz und den Leistungsstatus der überwachten Speichersysteme anzeigt.

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Was der Unified Manager-Server macht

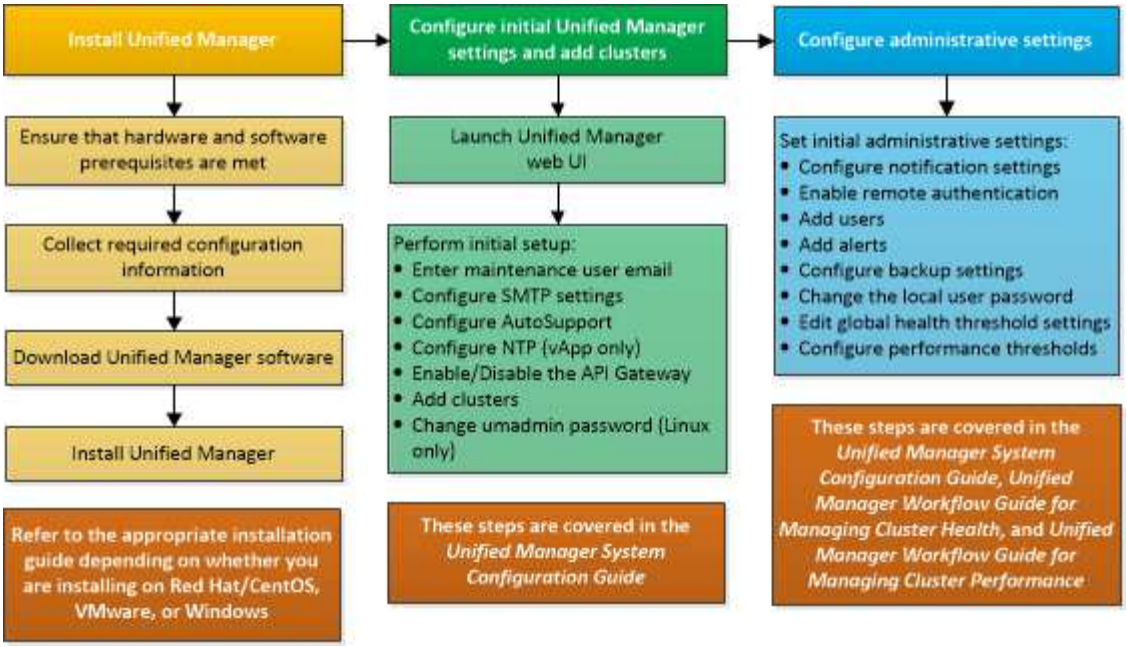
Die Unified Manager-Serverinfrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Anwendungsserver. Es bietet Infrastrukturdienste wie Erkennung, Überwachung, rollenbasierte Zugriffskontrolle (RBAC), Auditing und Protokollierung.

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

Übersicht über den Installationsablauf

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

In diesen Abschnitten werden alle im folgenden Arbeitsablauf angezeigten Elemente beschrieben.



Voraussetzungen für die Installation von Unified Manager

Stellen Sie vor Beginn des Installationsvorgangs sicher, dass der Server, auf dem Sie Unified Manager installieren möchten, die spezifischen Software-, Hardware-, CPU- und Speicheranforderungen erfüllt.

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

Weitere Einzelheiten zum Anwenden von Sicherheitsmaßnahmen auf den Unified Manager-Server finden Sie im Knowledge Base-Artikel.

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

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Anforderungen an die virtuelle Infrastruktur und das Hardwaresystem

Die Installation von Unified Manager auf einer virtuellen Infrastruktur oder einem physischen System sollte die Mindestanforderungen an Arbeitsspeicher, CPU und Festplattenspeicher erfüllen.

In der folgenden Tabelle sind die empfohlenen Werte für Arbeitsspeicher-, CPU- und Festplattenspeicherressourcen aufgeführt. Diese Werte wurden qualifiziert, sodass Unified Manager akzeptable Leistungsniveaus erreicht.

Hardwarekonfiguration	Empfohlene Einstellungen
RAM	12 GB (Mindestanforderung 8 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 • 100 GB freier Speicherplatz für die `/opt/netapp/data` Verzeichnis, das auf einem LVM-Laufwerk oder einer separaten lokalen Festplatte gemountet ist, die an das Zielsystem angeschlossen ist Für separat montierte `/opt` Und `/var/log` Verzeichnisse, stellen Sie sicher, dass `/opt` verfügt über 15 GB und `/var/log` hat 16 GB freien Speicherplatz. Der `/tmp` Das Verzeichnis sollte mindestens 10 GB freien Speicherplatz haben.

Unified Manager kann auf Systemen mit wenig Arbeitsspeicher installiert werden, die empfohlenen 12 GB RAM stellen jedoch sicher, dass genügend Arbeitsspeicher für eine optimale Leistung zur Verfügung steht und dass das System bei wachsender Konfiguration zusätzliche Cluster und Speicherobjekte aufnehmen kann. Sie sollten auf der VM, auf der Unified Manager bereitgestellt wird, keine Speicherbeschränkungen festlegen und keine Funktionen (z. B. Ballooning) aktivieren, die die Software daran hindern, den zugewiesenen Speicher auf dem System zu nutzen.

Darüber hinaus gibt es eine Begrenzung für die Anzahl der Knoten, die eine einzelne Instanz von Unified Manager überwachen kann, bevor Sie eine zweite Instanz von Unified Manager installieren. Weitere Informationen finden Sie im *Best Practices Guide*.

"Technischer Bericht 4621: Leitfaden zu Best Practices für Unified Manager"

Das Auslagern von Speicherseiten wirkt sich negativ auf die Leistung des Systems und der Verwaltungsanwendung aus. Der Wettbewerb um CPU-Ressourcen, die aufgrund der Gesamtauslastung des Hosts nicht verfügbar sind, kann die Leistung beeinträchtigen.

Voraussetzung für die dedizierte Nutzung

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, sollte ausschließlich für Unified Manager verwendet und nicht mit anderen Anwendungen geteilt werden. Andere Anwendungen verbrauchen möglicherweise Systemressourcen und können die Leistung von Unified Manager drastisch reduzieren.

Speicherplatzbedarf für Backups

Wenn Sie die Sicherungs- und Wiederherstellungsfunktion von Unified Manager verwenden möchten, weisen

Sie zusätzliche Kapazität zu, sodass das Verzeichnis oder die Festplatte „`data`“ über 150 GB Speicherplatz verfügt. Eine Sicherung kann an ein lokales oder ein Remote-Ziel geschrieben werden. Die beste Vorgehensweise besteht darin, einen Remote-Standort außerhalb des Unified Manager-Hostsystems zu identifizieren, der über mindestens 150 GB Speicherplatz verfügt.

Anforderungen für die Hostkonnektivität

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, sollte so konfiguriert sein, dass Sie erfolgreich `ping` der Hostname vom Host selbst. Bei einer IPv6-Konfiguration sollten Sie überprüfen, ob `ping6` zum Hostnamen erfolgreich ist, um sicherzustellen, dass die Installation von Unified Manager erfolgreich ist.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Web-Benutzeroberfläche des Produkts zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie einen Namen für den Netzwerkhost festgelegt. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollten Sie den Hostnamen vom DNS beziehen.

Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen statt über den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse ermöglichen möchten, muss Ihre Netzwerkkonfiguration diesen Kurznamen in einen gültigen FQDN auflösen.

Linux-Software und Installationsanforderungen

Das Linux-System, auf dem Sie Unified Manager installieren, erfordert bestimmte Versionen des Betriebssystems und der unterstützenden Software.

Betriebssystemsoftware

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

- Red Hat Enterprise Linux Versionen 8.x und 9.4, basierend auf der x86_64-Architektur.

Die vollständige und aktuelle Liste der unterstützten Red Hat Enterprise Linux-Versionen finden Sie in der Interoperabilitätsmatrix.

"mysupport.netapp.com/matrix"

Der Server sollte ausschließlich für die Ausführung von Unified Manager vorgesehen sein. Auf dem Server sollten keine anderen Anwendungen installiert sein. Es ist möglich, dass aufgrund von Unternehmensvorschriften ein Schwachstellenscanner wie Qualys auf Ihrem Linux-System installiert ist. Sie sollten den Schwachstellenscanner vor der Installation von Unified Manager deaktivieren, um zu verhindern, dass die Installation fehlschlägt.

Schwachstellenscanner (wie Qualys) können zu einer hohen CPU-Auslastung führen, wenn die virtuelle 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) gescannt wird. Dieses Problem führt häufig dazu, dass die VM nicht mehr reagiert und beeinträchtigt die Unified Manager-Dienste. Daher empfiehlt NetApp , den Schwachstellenscanner in der VM zu deaktivieren, auf der Unified Manager installiert ist. Wenn das Deaktivieren des Scanners keine Option ist, scannen Sie die VM außerhalb der Geschäftszeiten und starten Sie die Dienste nach Abschluss des Scans neu.

Software von Drittanbietern

Unified Manager wird auf einem WildFly-Webserver bereitgestellt. WildFly 26.1.3 ist mit Unified Manager gebündelt und konfiguriert.

Die folgenden Pakete von Drittanbietern sind erforderlich, aber nicht in Unified Manager enthalten. Diese Pakete werden automatisch vom `yum` Installer während der Installation, vorausgesetzt, Sie haben die Repositorys wie in den folgenden Abschnitten beschrieben konfiguriert.

- MySQL Community Edition Version 8.4.4 (aus dem MySQL-Repository)
- OpenJDK Version 11.0.25 (aus dem Red Hat Extra Enterprise Linux Server-Repository)
- Python 3.9.x (aus dem Red Hat Extra Enterprise Linux Server-Repository)
- p7zip Version 16.02 oder höher (aus dem Red Hat Extra Packages for Enterprise Linux-Repository)

Sie müssen eine laufende Instanz von Unified Manager herunterfahren, bevor Sie Software von Drittanbietern aktualisieren. Nachdem die Installation der Drittanbietersoftware abgeschlossen ist, können Sie Unified Manager neu starten.

Anforderungen an die Benutzerautorisierung

Die Installation von Unified Manager auf einem Linux-System kann vom Root-Benutzer oder von Nicht-Root-Benutzern mithilfe des `sudo` Befehl.

Darüber hinaus 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 diesen Inhalt aufgrund von Sicherheitsrichtlinien oder aufgrund eines Sicherheitsüberwachungstools aus Ihrer Umgebung entfernen, müssen Sie ihn wieder hinzufügen. Sie müssen die Sudoers-Konfiguration beibehalten, da einige Unified Manager-Vorgänge diese Sudo-Berechtigungen erfordern.

Installationsvoraussetzungen

Nachfolgend sind die Best Practices für die Installation von Red Hat Enterprise Linux und den zugehörigen Repositories auf Ihrem System aufgeführt. Bei Systemen, die anders installiert oder konfiguriert sind oder außerhalb des Unternehmens (in der Cloud) bereitgestellt werden, sind möglicherweise zusätzliche Schritte erforderlich, und Unified Manager wird bei solchen Bereitstellungen möglicherweise nicht ordnungsgemäß ausgeführt.

- Sie müssen Red Hat Enterprise Linux gemäß den Best Practices von Red Hat installieren und die folgenden Standardoptionen auswählen. Dazu müssen Sie die Basisumgebung „Server mit GUI“ auswählen.

- Während 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.
- Für die `yum` Um mit dem Installationsprogramm abhängige Software in den Red Hat Enterprise Linux-Repositorys zu finden, müssen Sie das System während der Red Hat Enterprise Linux-Installation oder danach mithilfe eines gültigen Red Hat-Abonnements registriert haben.

  Informationen zum Red Hat Subscription Manager finden Sie in der Red Hat-Dokumentation.

- Sie müssen das Repository „Extra Packages for Enterprise Linux“ (EPEL) aktivieren, um die erforderlichen Dienstprogramme von Drittanbietern erfolgreich auf Ihrem System zu installieren.

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

  Sehen"Manuelles Konfigurieren des EPEL-Repositorys" .

- Wenn nicht die richtige MySQL-Version installiert ist, müssen Sie das MySQL-Repository aktivieren, um die MySQL-Software erfolgreich auf Ihrem System zu installieren.

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

  Sehen"Manuelles Konfigurieren des MySQL-Repositorys" .

- Sie dürfen nur eine Version von Java auf Ihrem Unified Manager-Host installieren, da das System sonst möglicherweise nicht feststellen kann, welche Version verwendet werden soll. Sehen "Nach der Aktualisierung von Java auf dem Active IQ Unified Manager Host werden die Dienste nicht gestartet" .

Wenn Ihr System keinen Internetzugang hat und die Repositorys nicht von einem mit dem Internet verbundenen System auf das nicht verbundene System gespiegelt werden, sollten Sie die Installationsanweisungen befolgen, um die externen Softwareabhängigkeiten Ihres Systems zu ermitteln. Anschließend können Sie die benötigte Software auf das mit dem Internet verbundene System herunterladen und die `.rpm` Dateien auf das System, auf dem Sie Unified Manager installieren möchten. Um die Artefakte und Pakete herunterzuladen, müssen Sie die `yum install` Befehl. Sie müssen sicherstellen, dass auf den beiden Systemen dieselbe Betriebssystemversion ausgeführt wird und dass die Abonnementlizenz für das entsprechende Red Hat Enterprise Linux gilt.

> Sie dürfen die erforderliche Drittanbietersoftware nicht aus anderen als den hier aufgeführten Repositorys installieren. Aus den Red Hat-Repositorys installierte Software ist ausdrücklich für Red Hat Enterprise Linux konzipiert und entspricht den Best Practices von Red Hat (Verzeichnislayouts, Berechtigungen usw.). Software von anderen Standorten befolgt diese Richtlinien möglicherweise nicht, was dazu führen kann, dass die Installation von Unified Manager fehlschlägt oder bei zukünftigen Upgrades Probleme auftreten.

Port 443-Anforderung

Generische Images von Red Hat Enterprise Linux blockieren möglicherweise den externen Zugriff auf Port 443. Aufgrund dieser Einschränkung können Sie nach der Installation von Unified Manager möglicherweise keine Verbindung zur Administrator-Web-Benutzeroberfläche herstellen. Durch Ausführen des folgenden Befehls wird allen externen Benutzern und Anwendungen auf einem generischen Red Hat Enterprise Linux der Zugriff auf Port 443 ermöglicht.

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

```
--reload
```

Sie müssen Red Hat Enterprise Linux mit der Basisumgebung „Server mit GUI“ installieren. Es enthält die in den Installationsanweisungen von Unified Manager verwendeten Befehle. In anderen Basisumgebungen müssen Sie möglicherweise zusätzliche Befehle installieren, um die Installation zu validieren oder abzuschließen. Wenn die `firewall-cmd` auf Ihrem System nicht verfügbar ist, müssen Sie es durch Ausführen des folgenden Befehls installieren:

```
# sudo yum install firewalld
```

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

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

Unterstützte Browser

Verwenden Sie einen unterstützten Browser, um auf die Unified Manager-Web-Benutzeroberfläche zuzugreifen.

Die Interoperabilitätsmatrix enthält die Liste der unterstützten Browserversionen.

"mysupport.netapp.com/matrix"

Durch die Deaktivierung von Popup-Blockern wird bei allen Browsern sichergestellt, dass 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

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

Verbindungen zum Unified Manager-Server

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

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

Schnittstelle	Protokoll	Hafen	Beschreibung
Unified Manager-Web-Benutzeroberfläche	HTTP	80	Wird für den Zugriff auf die Unified Manager-Web-Benutzeroberfläche verwendet; leitet automatisch zum sicheren Port 443 um.
Unified Manager-Web-UI und Programme mit APIs	HTTPS	443	Wird verwendet, um sicher auf die Unified Manager-Web-Benutzeroberfläche zuzugreifen oder API-Aufrufe zu tätigen; API-Aufrufe können nur über HTTPS erfolgen.
Wartungskonsole	SSH/SFTP	22	Wird verwendet, um auf die Wartungskonsole zuzugreifen und Supportpakete abzurufen.
Linux-Befehlszeile	SSH/SFTP	22	Wird verwendet, um auf die Red Hat Enterprise Linux-Befehlszeile zuzugreifen und Support-Pakete abzurufen.
MySQL-Datenbank	MySQL	3306	Wird verwendet, um den Zugriff auf Unified Manager OnCommand Workflow Automation und OnCommand API Services zu ermöglichen.
Syslog	UDP	514	Wird verwendet, um auf abonnementbasierte EMS-Nachrichten von ONTAP Systemen zuzugreifen und auf der Grundlage der Nachrichten Ereignisse zu erstellen.
AUSRUHEN	HTTPS	9443	Wird verwendet, um auf REST-API-basierte EMS-Ereignisse in Echtzeit von authentifizierten ONTAP Systemen zuzugreifen.

Schnittstelle	Protokoll	Hafen	Beschreibung
MySQL-Datenbank	MySQL	3306	Wird verwendet, um den Zugriff auf Unified Manager OnCommand Workflow Automation und OnCommand API Services zu ermöglichen.
AMQP QPID-Broker	TCP/IP	56072	Wird für die interne Nachrichtenkommunikation verwendet.
AMQP QPID-Broker	WebSocket über TCP	56080	Wird verwendet, um auf diesem Port auf von ONTAP (Cloud-Agent) empfangene Nachrichten zu lauschen.
AMQP QPID-Broker	WebSocket über TCP	56443	Wird verwendet, um auf diesem Port auf von ONTAP (Cloud-Agent) empfangene Nachrichten zu lauschen. Die Kommunikation über diesen Port unterstützt die Verschlüsselung durch 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 anderen Hosts zur Verfügung gestellt werden, indem man den `Control access to MySQL port 3306` Option auf der Wartungskonsole. Weitere Informationen finden Sie unter"Zusätzliche Menüoptionen" . Die für die HTTP- und HTTPS-Kommunikation verwendeten Ports (Ports 80 und 443) können über die Wartungskonsole von Unified Manager geändert werden. Weitere Informationen finden Sie unter "Menüs der Wartungskonsole".

Verbindungen vom Unified Manager-Server

Sie sollten Ihre Firewall so konfigurieren, dass Ports geöffnet werden, die die Kommunikation zwischen dem Unified Manager-Server und verwalteten Speichersystemen, Servern und anderen Komponenten ermöglichen. Wenn ein Port nicht geöffnet ist, schlägt die Kommunikation fehl.

Abhängig von Ihrer Umgebung können Sie die vom Unified Manager-Server zum Herstellen einer Verbindung mit bestimmten Zielen verwendeten Ports und Protokolle ändern.

Der Unified Manager-Server stellt über die folgenden Protokolle und Ports eine Verbindung zu den verwalteten Speichersystemen, Servern und anderen Komponenten her:

Ziel	Protokoll	Hafen	Beschreibung
Speichersystem	HTTPS	443/TCP	Wird zur Überwachung und Verwaltung von Speichersystemen verwendet.
Speichersystem	NDMP	10000/TCP	Wird für bestimmte Snapshot-Wiederherstellungsvorgänge verwendet.
AutoSupport -Server	HTTPS	443	Wird zum Senden von AutoSupport -Informationen verwendet. Für die Ausführung dieser Funktion ist ein Internetzugang erforderlich.
Authentifizierungsserver	LDAP	389	Wird verwendet, um Authentifizierungsanfragen sowie Benutzer- und Gruppensuchanfragen zu stellen.
LDAPS	636	Wird für die sichere LDAP-Kommunikation verwendet.	Mailserver
SMTP	25	Wird zum Senden von E-Mail-Benachrichtigungen verwendet.	SNMP-Trap-Sender
SNMPv1 oder SNMPv3	162/UDP	Wird zum Senden von SNMP-Traps für Warnbenachrichtigungen verwendet.	Externer Datenanbieterserver
TCP	2003	Wird verwendet, um Leistungsdaten an einen externen Datenanbieter wie Graphite zu senden.	NTP-Server

Ziel	Protokoll	Hafen	Beschreibung
NTP	123/UDP	Wird verwendet, um die Zeit auf dem Unified Manager-Server mit einem externen NTP-Zeitserver zu synchronisieren. (Nur VMware-Systeme)	Syslog

Füllen Sie das Arbeitsblatt aus

Bevor Sie Unified Manager installieren und konfigurieren, sollten Sie bestimmte Informationen zu Ihrer Umgebung zur Hand haben. Sie können die Informationen im Arbeitsblatt festhalten.

Unified Manager-Installationsinformationen

Die zur Installation von Unified Manager erforderlichen Details.

System, auf dem die Software bereitgestellt wird	Ihr Wert
Vollqualifizierter Domänenname des Hosts	
Host-IP-Adresse	
Netzwerkmaske	
Gateway-IP-Adresse	
Primäre DNS-Adresse	
Sekundäre DNS-Adresse	
Suchdomänen	
Wartungsbenutzername	
Wartungsbenutzerkennwort	

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	
Hostname oder IP-Adresse des SMTP-Servers	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Port	25 (Standardwert)
E-Mail, von der Warnbenachrichtigungen gesendet werden	
Hostname oder IP-Adresse des Authentifizierungsservers	
Active Directory-Administratorname oder LDAP-Bind-Distinguished Name	
Active Directory-Passwort oder LDAP-Bind-Passwort	
Basis-Distinguished Name des Authentifizierungsservers	
URL des Identitätsanbieters (IdP)	
Metadaten des Identitätsanbieters (IdP)	
IP-Adressen des SNMP-Trap-Zielhosts	
SNMP-Port	

Cluster-Informationen

Die Details für die Speichersysteme, die Sie mit Unified Manager verwalten.

Cluster 1 von N	Ihr Wert
Hostname oder IP-Adresse zur Clusterverwaltung	
ONTAP -Administratorbenutzername Dem Administrator muss die Rolle „`admin`“ zugewiesen worden sein.	

Cluster 1 von N	Ihr Wert
ONTAP -Administratorkennwort	
Protokoll	HTTPS

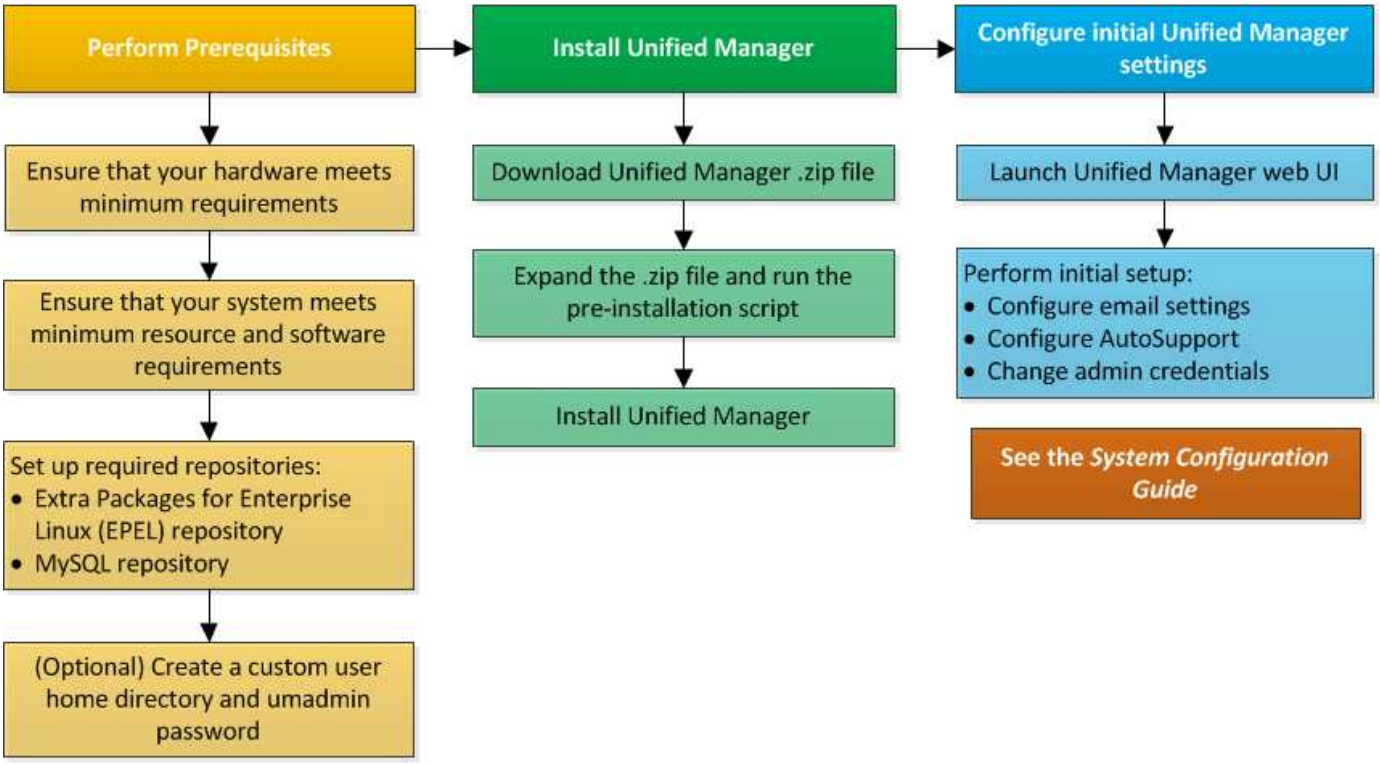
Installieren, aktualisieren und entfernen Sie die Unified Manager-Software

Auf Linux-Systemen können Sie die Unified Manager-Software installieren, auf eine neuere Softwareversion 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 einer physischen Maschine oder auf einer virtuellen Maschine ausgeführt werden, die auf VMware ESXi, Microsoft Hyper-V oder Citrix XenServer läuft.

Übersicht über den Installationsprozess

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



Einrichten der erforderlichen Software-Repositorys

Das System muss Zugriff auf bestimmte Repositorys haben, damit das Installationsprogramm auf alle erforderlichen Softwareabhängigkeiten zugreifen und diese installieren kann.

Manuelles Konfigurieren des EPEL-Repositorys

Wenn das System, auf dem Sie Unified Manager installieren, keinen Zugriff auf das Extra Packages for Enterprise Linux (EPEL)-Repository hat, müssen Sie das Repository für eine erfolgreiche Installation manuell herunterladen und konfigurieren.

Das EPEL-Repository bietet Zugriff auf die erforderlichen Dienstprogramme von Drittanbietern, 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. Laden Sie das EPEL-Repository für Ihre Installation herunter. Laden Sie Version 8 herunter von:

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

   Laden Sie Version 9 herunter von:

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

2. Konfigurieren Sie das EPEL-Repository:

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

Wenn Sie für Red Hat Enterprise Linux 8-Systeme beispielsweise interne Repositories mit modularen RPM-Paketen haben, *javapackages-filesystem-<version>.module.rpm* Stellen Sie sicher, dass die Metadaten für die modularen Pakete auch im selben Repository verfügbar sind.

Manuelles Konfigurieren des MySQL-Repositorys

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

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. Lesen Sie die MySQL-Dokumentation, wenn das System, auf dem Sie Unified Manager installieren, keinen Internetzugang hat.

Schritte

1. Laden Sie das entsprechende MySQL-Repository für Ihre Installation herunter. Laden Sie Version 8 herunter von:

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

   Laden Sie Version 9 herunter von:

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

2. Konfigurieren Sie das MySQL-Repository:

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

Wenn Sie für das Red Hat Enterprise Linux 8-System interne Repositorys mit Java-11-OpenJDK, P7Zip und anderen vom AppStream-Repository bereitgestellten Softwarepaketen haben, müssen Sie Ihr AppStream-Repository deaktivieren und MySQL Community Server installieren. Führen Sie den folgenden Befehl aus:

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

Wenn Sie eine Fehlermeldung über einen fehlenden oder nicht übereinstimmenden Schlüssel erhalten und Ihre Installation fehlschlägt, versuchen Sie Folgendes:

- Importieren Sie auf einem verbundenen System den aktualisierten MySQL-Schlüssel, indem Sie den folgenden Befehl ausführen:

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

for example:

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

- Aktualisieren Sie auf einem System ohne Internetverbindung Ihre MySQL-Repo-Datei und deaktivieren Sie `gpgcheck` durch Markierung `gpgcheck=0` .

SELinux-Anforderungen an NFS- und CIFS-Freigaben

Wenn Sie planen, `/opt/netapp` oder `/opt/netapp/data` auf einem NAS- oder SAN-Gerät und wenn Sie SELinux aktiviert haben, müssen Sie einige Überlegungen beachten.

Wenn Sie planen, `/opt/netapp` oder `/opt/netapp/data` von einem anderen Ort als dem Root-Dateisystem aus und wenn Sie SELinux in Ihrer Umgebung aktiviert haben, sollten Sie den richtigen Kontext für die gemounteten Verzeichnisse festlegen. Befolgen Sie für das entsprechende Szenario in Ihrer Umgebung diese Schritte zum Einrichten und Bestätigen des richtigen SELinux-Kontexts.

Konfigurieren Sie den SELinux-Kontext, wenn `/opt/netapp/data` ist montiert

Wenn Sie montiert haben `/opt/netapp/data` in Ihrem System und SELinux ist eingestellt auf `Enforcing` , stellen Sie sicher, dass der SELinux-Kontexttyp für `/opt/netapp/data` ist eingestellt auf `mysqld_db_t` , das Standardkontextelement für den Speicherort der Datenbankdateien.

1. Führen Sie diesen Befehl aus, um den Kontext zu überprüfen:

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

   Eine Beispielausgabe:

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

> In dieser Ausgabe ist der Kontext `default_t` . Sie sollten diesen Kontext ändern in `mysqld_db_t` .

2. Führen Sie diese Schritte aus, um den Kontext basierend auf der Art und Weise festzulegen, wie Sie `/opt/netapp/data` .
   a. Führen Sie die folgenden Befehle aus, um den Kontext auf `mysqld_db_t` :
      `semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"`
      `` `restorecon -R -v /opt/netapp/data ``
   b. Wenn Sie konfiguriert haben `/opt/netapp/data` In `/etc/fstab` , sollten Sie die `/etc/fstab` Datei. Für die `/opt/netapp/data/` Fügen Sie bei der Mount-Option das MySQL-Label wie folgt hinzu:

      `context=system_u:object_r:mysqld_db_t:s0`
   c. Aushängen und erneutes Einhängen `/opt/netapp/data/` zum Aktivieren des Kontexts.
   d. Wenn Sie über eine direkte NFS-Einbindung verfügen, führen Sie den folgenden Befehl aus, um den Kontext auf `mysqld_db_t` :

      `mount <nfsshare>:/<mountpoint> /opt/netapp/data -o context=system_u:object_r:mysqld_db_t:s0`
3. Überprüfen Sie, ob der Kontext richtig eingestellt ist:

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

Eine Beispielausgabe:

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

Konfigurieren Sie den SELinux-Kontext, wenn `/opt/netapp` montiert ist und `/opt/netapp/data/` wird auch separat montiert

In diesem Szenario sollten Sie zunächst den Kontext für `/opt/netapp/data/` wie im vorherigen Abschnitt beschrieben. Nachdem Sie den richtigen Kontext für `/opt/netapp/data/` , stellen Sie sicher, dass das übergeordnete Verzeichnis `/opt/netapp` hat den SELinux-Kontext nicht auf `file_t` .

Schritte

1. Führen Sie diesen Befehl aus, um den Kontext zu überprüfen:

   `ls -dZ /opt/netapp`

   Eine Beispielausgabe:

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

In dieser Ausgabe ist der Kontext `file_t` sollte geändert werden. Die folgenden Befehle setzen den Kontext auf `usr_t` . Sie können den Kontext auf einen beliebigen Wert außer `file_t` basierend auf Ihren Sicherheitsanforderungen.

2. Führen Sie diese Schritte aus, um den Kontext basierend auf der Art und Weise festzulegen, wie Sie `/opt/netapp` .
   a. Führen Sie die folgenden Befehle aus, um den Kontext festzulegen:

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

1. Wenn Sie konfiguriert haben `/opt/netapp` In `/etc/fstab` , sollten Sie die `/etc/fstab` Datei. Für die `/opt/netapp` Fügen Sie bei der Mount-Option das MySQL-Label wie folgt hinzu:

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

2. Aushängen und dann wieder einhängen `/opt/netapp` zum Aktivieren des Kontexts.
3. Wenn Sie über eine direkte NFS-Einbindung verfügen, führen Sie den folgenden Befehl aus, um den Kontext festzulegen:

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

   a. Überprüfen Sie, ob der Kontext richtig eingestellt ist:

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

   Eine Beispielausgabe

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

Konfigurieren Sie den SELinux-Kontext, wenn `/opt/netapp` montiert ist und `/opt/netapp/data/` wird nicht separat montiert

Wenn Sie montiert haben `/opt/netapp` in Ihrem System und SELinux ist eingestellt auf `Enforcing` , stellen Sie sicher, dass der SELinux-Kontexttyp für `/opt/netapp` ist eingestellt auf `mysqld_db_t` , das Standardkontextelement für den Speicherort der Datenbankdateien.

Schritte

1. Führen Sie diesen Befehl aus, um den Kontext zu überprüfen:

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

   Eine Beispielausgabe:

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

In dieser Ausgabe ist der Kontext `default_t` . Sie sollten diesen Kontext ändern in `mysqld_db_t` .

2. Führen Sie die folgenden Schritte aus, um den Kontext basierend auf der Art und Weise festzulegen, wie Sie ihn gemountet haben `/opt/netapp` .
   a. Führen Sie die folgenden Befehle aus, um den Kontext auf `mysqld_db_t` :
   `semanage fcontext -a -t mysqld_db_t "/opt/netapp"`
   `` `restorecon -R -v /opt/netapp ``
   b. Wenn Sie konfiguriert haben `/opt/netapp` In `/etc/fstab` , bearbeiten Sie die `/etc/fstab` Datei. Für die `/opt/netapp/` Fügen Sie bei der Mount-Option das MySQL-Label wie folgt hinzu:
   `context=system_u:object_r:mysqld_db_t:s0`
   c. Aushängen und dann wieder einhängen `/opt/netapp/` zum Aktivieren des Kontexts.
   d. Wenn Sie über eine direkte NFS-Einbindung verfügen, führen Sie den folgenden Befehl aus, um den Kontext auf `mysqld_db_t` :
   `mount <nfsshare>:/<mountpoint> /opt/netapp -o`
   `context=system_u:object_r:mysqld_db_t:s0`
3. Überprüfen Sie, ob der Kontext richtig eingestellt ist:

`ls -dZ /opt/netapp/`

Eine Beispielausgabe:

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

Installieren Sie Unified Manager auf Linux-Systemen

Es ist wichtig, dass Sie verstehen, dass die Reihenfolge der Schritte zum Herunterladen und Installieren von Unified Manager je nach Ihrem Installationsszenario variiert.

Erstellen Sie vor der Installation ein benutzerdefiniertes Benutzer-Home-Verzeichnis und ein Umadmin-Passwort

Sie können vor der Installation von Unified Manager ein benutzerdefiniertes Home-Verzeichnis erstellen und Ihr eigenes Umadmin-Benutzerkennwort festlegen. Diese Aufgabe ist optional, einige Sites benötigen jedoch möglicherweise die Flexibilität, die Standardeinstellungen der Unified Manager-Installation zu überschreiben.

Bevor Sie beginnen

- Das System muss die in"Hardware-Systemanforderungen" .
- Sie müssen sich als Root-Benutzer beim Red Hat Enterprise Linux-System anmelden können.

Die Standardinstallation von Unified Manager führt die folgenden Aufgaben aus:

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

Da einige Installationsumgebungen den Zugriff auf `/home` , schlägt die Installation fehl. Sie müssen das Home-Verzeichnis an einem anderen Ort erstellen. Darüber hinaus können auf manchen Websites Regeln zur Kennwortkomplexität gelten oder es kann erforderlich sein, dass Kennwörter von lokalen Administratoren und nicht vom Installationsprogramm festgelegt werden.

Wenn Ihre Installationsumgebung erfordert, dass Sie diese Standardinstallationseinstellungen überschreiben, führen Sie diese Schritte aus, um ein benutzerdefiniertes Home-Verzeichnis zu erstellen und das Kennwort des Umadmin-Benutzers festzulegen.

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

Darüber hinaus 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 diesen Inhalt aufgrund von Sicherheitsrichtlinien oder aufgrund eines Sicherheitsüberwachungstools aus Ihrer Umgebung entfernen, müssen Sie ihn wieder hinzufügen. Sie müssen die Sudoers-Konfiguration beibehalten, da einige Unified Manager-Vorgänge diese Sudo-Berechtigungen erfordern.

Die Sicherheitsrichtlinien in Ihrer Umgebung dürfen die Sudo-Berechtigungen für den Unified Manager-Wartungsbenutzer nicht einschränken. Einige Unified Manager-Vorgänge können fehlschlagen, wenn die Berechtigungen eingeschränkt sind. Überprüfen Sie, ob Sie nach erfolgreicher Installation den folgenden Sudo-Befehl ausführen können, wenn Sie als Umadmin-Benutzer angemeldet sind.

```
sudo systemctl status ocie
```

Dieser Befehl sollte den entsprechenden Status des Ocie-Dienstes ohne Fehler zurückgeben.

Schritte

1. Melden Sie sich als Root-Benutzer beim Server an.
2. Erstellen Sie das umadmin-Gruppenkonto mit dem Namen „maintenance“:

   ```
   groupadd maintenance
   ```

3. Erstellen Sie das Benutzerkonto „`umadmin`“ in der Wartungsgruppe unter einem Home-Verzeichnis Ihrer Wahl:

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

4. Definieren Sie das Umadmin-Passwort:

   ```
   passwd umadmin
   ```

   Das System fordert Sie auf, eine neue Kennwortzeichenfolge für den Benutzer „umadmin“ einzugeben.

Nachdem Sie Unified Manager installiert haben, müssen Sie die Benutzeranmeldeshell umadmin angeben.

Unified Manager herunterladen

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

Bevor Sie beginnen

Sie müssen über Anmeldeinformationen für die NetApp Support-Site verfügen.

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

Schritte

1. Melden Sie sich bei der NetApp Support-Site an und navigieren Sie zur Download-Seite für Unified Manager:

   "NetApp Support Site"

2. Wählen Sie die erforderliche Version von Unified Manager aus und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA).
3. Laden Sie die Unified Manager-Installationsdatei für Linux herunter und speichern Sie die `.zip` Datei in ein Verzeichnis auf dem Zielsystem.

   - Stellen Sie sicher, dass Sie die richtige Version der Installationsdatei für Ihr Red Hat Enterprise Linux-System herunterladen. Je nachdem, ob Sie Red Hat Enterprise Linux 8 oder 9 installiert haben, stellen Sie sicher, dass Sie die entsprechende Version des Unified Manager herunterladen `.zip` Datei.
   - NetApp empfiehlt, dass Sie das Code Signing-Zertifikat herunterladen(`.pem`) und digitale Signatur(`.sig`) zusammen mit dem `.zip` Datei.

4. Überprüfen Sie die Prüfsumme auf Integrität der heruntergeladenen Software.
5. Wenn Sie das Codesignaturzertifikat und die digitale Signatur heruntergeladen haben, können Sie die Integrität der Installationsdatei überprüfen. Mit den folgenden Befehlen können Sie die Integrität der Installationsdatei überprüfen:
   - Dieser Befehl erstellt eine Datei mit dem öffentlichen Schlüssel aus dem Codesignaturzertifikat:

     ```
     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
     ```

     Die Nachricht ähnelt `Verified Ok` bestätigt, dass die Installationsdatei sicher verwendet werden kann.

Unified Manager installieren

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.

  Sehen"Hardware-Systemanforderungen" .

  Sehen"Linux-Software und Installationsanforderungen" .

- Sie müssen den Unified Manager heruntergeladen haben `.zip` Datei von der NetApp Support Site auf das Zielsystem.
- Sie sollten die Integrität der heruntergeladenen `.zip` Datei.
- Sie müssen über einen unterstützten Webbrowser verfügen.
- In Ihrer Terminalemulationssoftware muss Scrollback aktiviert sein.

Auf dem Red Hat Enterprise Linux-System sind möglicherweise alle erforderlichen Versionen der erforderlichen unterstützenden Software (Java, MySQL, zusätzliche Dienstprogramme) installiert, nur ein Teil der erforderlichen Software ist installiert oder es handelt sich möglicherweise um ein neu installiertes System, auf dem keine der erforderlichen Software installiert ist.

Schritte

1. Melden Sie sich beim Server an, auf dem Sie Unified Manager installieren.
2. Geben Sie die entsprechenden Befehle ein, um zu ermitteln, welche Software möglicherweise auf dem Zielsystem installiert oder aktualisiert werden muss, um die Installation zu unterstützen:

Erforderliche Software und Mindestversion	Befehl zum Überprüfen von Software und Version
OpenJDK Version 11.0.25	`java -version`
MySQL 8.4.4 Community Edition	`rpm -qa
grep -i mysql`	p7zip 16.02
`rpm -qa	grep p7zip`

3. Wenn die installierte MySQL-Version älter als MySQL 8.4.4 Community Edition ist, geben Sie den folgenden Befehl ein, um sie zu deinstallieren:

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

   Wenn Sie Abhängigkeitsfehler erhalten, müssen Sie die `--nodeps` Option zum Deinstallieren der Komponente.

4. Navigieren Sie zu dem Verzeichnis, in das Sie die Installation heruntergeladen haben `.zip` Datei und erweitern Sie das Unified Manager-Paket:

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

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

5. Stellen Sie sicher, dass das folgende Modul im Verzeichnis verfügbar ist:

```
ls *.rpm

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

6. Führen Sie das Vorinstallationsskript aus, um sicherzustellen, dass keine Systemkonfigurationseinstellungen oder installierte Software vorhanden sind, die mit der Installation von Unified Manager in Konflikt geraten könnten:

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

Das Vorinstallationsskript überprüft, ob das System über ein gültiges Red Hat Enterprise Linux-Abonnement verfügt und Zugriff auf die erforderlichen Software-Repositorys hat. Wenn das Skript Probleme erkennt, müssen Sie diese vor der Installation von Unified Manager beheben.

Wenn Sie für das Red Hat Enterprise Linux 8-System interne Repositories mit JDK 11 – OpenJDK, p7zip und anderen vom AppStream-Repository bereitgestellten Softwarepaketen haben, müssen Sie Ihr AppStream-Repository deaktivieren und MySQL Community Server installieren. Führen Sie den folgenden Befehl aus:

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

7. **Optional:** Sie müssen Schritt 7 nur ausführen, wenn Ihr System nicht mit dem Internet verbunden ist und Sie die für Ihre Installation erforderlichen Pakete manuell herunterladen müssen. Wenn Ihr System über Internetzugang verfügt und alle erforderlichen Pakete verfügbar sind, fahren Sie mit Schritt 8 fort. Führen Sie für Systeme, die nicht mit dem Internet verbunden sind oder die Red Hat Enterprise Linux-Repositorys nicht verwenden, die folgenden Schritte aus, um festzustellen, ob erforderliche Pakete fehlen, und laden Sie diese Pakete dann herunter:

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

   Die Elemente im Abschnitt „Installieren:“ sind die Pakete, die im aktuellen Verzeichnis verfügbar sind, und die Elemente im Abschnitt „Installieren für Abhängigkeiten:“ sind die Pakete, die auf Ihrem System fehlen.

   b. Laden Sie auf einem System mit Internetzugang die fehlenden Pakete herunter:

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

> Da das Plug-in „yum-plugin-downloadonly“ auf Red Hat Enterprise Linux-Systemen nicht immer aktiviert ist, müssen Sie möglicherweise die Funktion zum Herunterladen eines Pakets aktivieren, ohne es zu installieren:
> `yum install yum-plugin-downloadonly`

a. Kopieren Sie die fehlenden Pakete vom mit dem Internet verbundenen System auf Ihr Installationssystem.

8. Als Root-Benutzer oder mit `sudo` führen Sie den folgenden Befehl aus, um die Software zu installieren:

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

   Dieser Befehl installiert die .rpm-Pakete, alle anderen erforderlichen unterstützenden Softwareprogramme und die Unified Manager-Software.

   Wenn die Installation mit dem GPG NOKEY-Fehler fehlschlägt, verwenden Sie `rpm --import` So importieren Sie die Schlüssel von einer URL:

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

   > Versuchen Sie nicht, die Installation mit alternativen Befehlen durchzuführen (wie etwa `rpm -ivh`). Eine erfolgreiche Installation von Unified Manager auf einem Red Hat Enterprise Linux-System erfordert, dass alle Unified Manager-Dateien und zugehörigen Dateien in einer bestimmten Reihenfolge in einer bestimmten Verzeichnisstruktur installiert werden, die automatisch durch die `yum install netapp-um<version>.x86_64.rpm` Befehl.

9. Ignorieren Sie die E-Mail-Benachrichtigung, die unmittelbar nach den Installationsmeldungen angezeigt wird.

   Die E-Mail benachrichtigt den Root-Benutzer über einen anfänglichen Cron-Job-Fehler, der keine negativen Auswirkungen auf die Installation hat.

10. Nachdem die Installationsmeldungen abgeschlossen sind, scrollen Sie durch die Meldungen zurück, bis Sie die Meldung sehen, in der das System eine IP-Adresse oder URL für die Unified Manager-Web-Benutzeroberfläche, den Wartungsbenutzernamen (umadmin) und ein Standardkennwort anzeigt.

    Die Meldung 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. Notieren Sie die IP-Adresse oder URL, den zugewiesenen Benutzernamen (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 umadmin-Benutzeranmeldeshell angeben:

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

Greifen Sie auf die Web-Benutzeroberfläche zu, um das Standardkennwort des umadmin-Benutzers zu ändern, und führen Sie die Ersteinrichtung von Unified Manager durch, wie in beschrieben"Konfigurieren von Active IQ Unified Manager" . Es ist zwingend erforderlich, das Standardkennwort des Umadmin-Benutzers zu ändern.

Während der Installation von Unified Manager erstellte Benutzer

Wenn Sie Unified Manager auf Red Hat Enterprise Linux installieren, werden die folgenden Benutzer von Unified Manager und Dienstprogrammen von Drittanbietern erstellt: umadmin, jboss und mysql.

- **umadmin**

  Wird für die erste Anmeldung bei Unified Manager verwendet. Diesem Benutzer wird die Benutzerrolle „Anwendungsadministrator“ zugewiesen und er ist als Typ „Wartungsbenutzer“ konfiguriert. Dieser Benutzer wird von Unified Manager erstellt.

- **jboss**

  Wird zum Ausführen von Unified Manager-Diensten im Zusammenhang mit dem JBoss-Dienstprogramm verwendet. Dieser Benutzer wird von Unified Manager erstellt.

- **mysql**

  Wird zum Ausführen von MySQL-Datenbankabfragen von Unified Manager verwendet. Dieser Benutzer wird vom MySQL-Dienstprogramm eines Drittanbieters erstellt.

Zusätzlich zu diesen Benutzern erstellt Unified Manager auch entsprechende Gruppen: Wartung, JBoss und MySQL. Die Wartungs- und JBoss-Gruppen werden von Unified Manager erstellt, während die MySQL-Gruppe von einem Dienstprogramm eines Drittanbieters erstellt wird.

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

Ändern des JBoss-Passworts

Sie können das instanzspezifische JBoss-Passwort zurücksetzen, das während der Installation festgelegt wurde. Sie können das Kennwort optional zurücksetzen, falls Ihre Site diese Sicherheitsfunktion benötigt, um die Installationseinstellung des Unified Managers zu überschreiben. Dieser Vorgang ändert auch das Kennwort, das JBoss für den Zugriff auf MySQL verwendet.

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

Schritte

1. Melden Sie sich als Root-Benutzer am System an.
2. Stoppen Sie die Unified Manager-Dienste, indem Sie die folgenden Befehle in der angezeigten Reihenfolge eingeben:

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

   Beenden Sie die zugehörige MySQL-Software nicht.

3. Geben Sie den folgenden Befehl ein, um den Vorgang zur Kennwortänderung zu starten:

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

4. Geben Sie bei entsprechender Aufforderung das neue JBoss-Passwort ein und geben Sie es zur Bestätigung ein zweites Mal ein.

   Beachten Sie, dass das Passwort zwischen 8 und 16 Zeichen lang sein sollte und mindestens eine Ziffer, einen Großbuchstaben, einen Kleinbuchstaben und mindestens eines dieser Sonderzeichen enthalten muss:

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

5. Wenn das Skript abgeschlossen ist, starten Sie die Unified Manager-Dienste, indem Sie die folgenden Befehle in der angezeigten Reihenfolge eingeben:

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

6. Nachdem alle Dienste gestartet wurden, können Sie sich bei der Unified Manager-Benutzeroberfläche anmelden.

Upgrade von Unified Manager auf Red Hat Enterprise Linux

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

Patch-Versionen der Unified Manager-Software werden, sofern sie von NetApp bereitgestellt werden, mit demselben Verfahren wie neue Versionen installiert.

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 der Durchführung der Upgrades eine neue Workflow Automation-Verbindung einrichten. Wenn Sie ein Upgrade nur für eines der Produkte durchführen, sollten Sie sich nach dem Upgrade bei Workflow Automation anmelden und überprüfen, ob weiterhin Daten vom Unified Manager abgerufen werden.

Unterstützter Upgrade-Pfad für Unified Manager-Versionen

Active IQ Unified Manager unterstützt für jede Version einen bestimmten Upgradepfad.

Nicht alle Versionen von Unified Manager können ein direktes Upgrade auf neuere Versionen durchführen. Die Unified Manager-Upgrades sind auf ein N-2-Modell beschränkt, d. h. ein Upgrade kann auf allen Plattformen nur innerhalb der nächsten zwei Versionen durchgeführt werden. Sie können beispielsweise nur von Unified

Manager 9.13 und 9.14 ein Upgrade auf Unified Manager 9.16 durchführen.

Wenn Sie eine Version ausführen, die älter ist als die unterstützten Versionen, muss Ihre Unified Manager-Instanz zuerst auf eine der unterstützten Versionen und dann auf die aktuelle Version aktualisiert werden.

Wenn Sie beispielsweise die Version Unified Manager 9.9 installiert haben und auf Unified Manager 9.14 aktualisieren möchten, befolgen Sie eine Upgrade-Reihenfolge.

Beispielhafter Upgradepfad:

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

Weitere Informationen zur Upgrade-Pfadmatrix finden Sie hier "Wissensdatenbankartikel (KB)" .

Upgrade von Unified Manager

Sie können ein Upgrade von Unified Manager 9.13 oder 9.14 auf 9.16 durchführen, 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.

  Sehen"Hardware-Systemanforderungen" .

  Sehen"Linux-Software und Installationsanforderungen" .

- Sie müssen über ein Abonnement für den Red Hat Enterprise Linux Subscription Manager verfügen.
- Sie müssen die richtige Version von OpenJDK installieren oder auf diese aktualisieren, bevor Sie Unified Manager aktualisieren.

  Sehen"Aktualisieren von JRE unter Linux" .

- Um Datenverlust zu vermeiden, müssen Sie eine Sicherungskopie der Unified Manager-Datenbank erstellt haben, für den Fall, dass während des Upgrades ein Problem auftritt. NetApp empfiehlt, die Sicherungsdatei vom `/opt/netapp/data` Verzeichnis an einen externen Speicherort.
- Während des Upgrades werden Sie möglicherweise aufgefordert zu bestätigen, ob Sie die vorherigen Standardeinstellungen für die Aufbewahrung der Leistungsdaten für 13 Monate beibehalten oder auf 6 Monate ändern möchten. Nach der Bestätigung werden die historischen Leistungsdaten nach 6 Monaten gelöscht.
- Sie sollten alle laufenden Vorgänge abgeschlossen haben, da Unified Manager während des Upgrade-Vorgangs nicht verfügbar ist.
- MySQL Community Edition wird während des Unified Manager-Upgrades automatisch aktualisiert. Wenn die auf Ihrem System installierte MySQL-Version älter als 8.4.4 ist, aktualisiert der Upgrade-Prozess von Unified Manager MySQL automatisch auf 8.4.4.

Schritte

1. Melden Sie sich beim Zielserver von Red Hat Enterprise Linux an.

2. Laden Sie das Unified Manager-Paket auf den Server herunter.

   Sehen"Unified Manager für Linux herunterladen" .

3. Navigieren Sie zum Zielverzeichnis und erweitern Sie das Unified Manager-Paket:

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

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

4. Stellen Sie sicher, dass das folgende Modul im Verzeichnis verfügbar ist:

   ```
   ls *.rpm
   ```

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

5. Führen Sie das Vorinstallationsskript aus, um sicherzustellen, dass keine Systemkonfigurationseinstellungen oder installierte Software vorhanden sind, die mit dem Upgrade in Konflikt geraten könnten:

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

   Das Vorinstallationsskript überprüft, ob das System über ein gültiges Red Hat Enterprise Linux-Abonnement verfügt und Zugriff auf die erforderlichen Software-Repositorys hat. Wenn das Skript Probleme erkennt, müssen Sie diese beheben und mit dem Upgrade fortfahren.

   Wenn fehlende Pakete erkannt werden, führen Sie die in"Zusätzliche Schritte bei fehlenden Paketen" . Wenn keine Pakete fehlen, fahren Sie mit den nächsten Schritten fort.

6. Aktualisieren Sie Unified Manager mit dem folgenden Skript:

   ```
   upgrade.sh
   ```

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

7. Nachdem das Upgrade abgeschlossen ist, scrollen Sie durch die Nachrichten zurück, bis Sie die Nachricht mit einer IP-Adresse oder URL für die Unified Manager-Web-Benutzeroberfläche, dem Wartungsbenutzernamen (umadmin) und dem Standardkennwort sehen.

   Die Meldung 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/
```

Geben Sie die angegebene IP-Adresse oder URL in ein neues Fenster eines unterstützten Webbrowsers ein, um die Unified Manager-Web-Benutzeroberfläche zu starten, und melden Sie sich dann mit demselben Wartungsbenutzernamen (umadmin) und Kennwort an, das Sie zuvor festgelegt haben.

Zusätzliche Schritte bei fehlenden Paketen

Wenn während des Upgrades fehlende Pakete auf Ihrer Site erkannt werden oder wenn Ihr System nicht mit dem Internet verbunden ist oder Sie die Red Hat Enterprise Linux-Repositorys nicht verwenden, führen Sie die folgenden Schritte aus, um festzustellen, ob erforderliche Pakete fehlen, und laden Sie diese Pakete herunter.

Diese Schritte müssen nach Schritt *5* des Hauptverfahrens ausgeführt werden. Mit diesem Verfahren wird Unified Manager aktualisiert. Sie müssen für die Aktualisierung keine weiteren Schritte ausführen.

1. Sehen Sie sich die Liste der verfügbaren und nicht verfügbaren Pakete an:

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

   Die Elemente im Abschnitt „Installieren:“ sind die Pakete, die im aktuellen Verzeichnis verfügbar sind, und die Elemente im Abschnitt „Installieren für Abhängigkeiten:“ sind die Pakete, die auf Ihrem System fehlen.

2. Führen Sie auf einem anderen System mit Internetzugang den folgenden Befehl aus, um die fehlenden Pakete herunterzuladen.

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

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

   Da das Plug-in „yum-plugin-downloadonly“ auf Red Hat Enterprise Linux-Systemen nicht immer aktiviert ist, müssen Sie möglicherweise die Funktion zum Herunterladen eines Pakets aktivieren, ohne es zu installieren:

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

3. Kopieren Sie die heruntergeladenen Pakete in das Verzeichnis, in dem Sie das Unified Manager-Paket auf dem Installationssystem entpackt haben.
4. Wechseln Sie in dieses Verzeichnis und führen Sie den folgenden Befehl aus, um die fehlenden Pakete zusammen mit ihren Abhängigkeiten zu installieren.

   ```
   yum install *.rpm
   ```

5. Starten Sie den Unified Manager-Server. Führen Sie diese Befehle aus:

```
systemctl start ocie

systemctl start ocieau
```

Dieser Vorgang schließt den Upgrade-Prozess von Unified Manager ab. Geben Sie die angegebene IP-Adresse oder URL in ein neues Fenster eines unterstützten Webbrowsers ein, um die Unified Manager-Web-Benutzeroberfläche zu starten, und melden Sie sich dann mit demselben Wartungsbenutzernamen (umadmin) und Kennwort an, das Sie zuvor festgelegt haben.

Aktualisieren Sie das Host-Betriebssystem von Red Hat Enterprise Linux 7.x auf 8.x

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, müssen Sie eines der in diesem Thema aufgeführten Verfahren befolgen. In beiden Fällen müssen Sie eine Sicherungskopie von Unified Manager auf dem Red Hat Enterprise Linux 7.x-System erstellen und die Sicherungskopie dann auf einem Red Hat Enterprise Linux 8.x-System wiederherstellen. Beachten Sie, dass die unterstützten Versionen von Red Hat Enterprise Linux von 8.0 bis 8.10 reichen.

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

Da Sie für diese Aufgabe eine Sicherungskopie von Unified Manager auf dem Red Hat Enterprise Linux 7.x-System erstellen müssen, sollten Sie die Sicherungskopie nur erstellen, wenn Sie bereit sind, den gesamten Upgrade-Prozess abzuschließen, damit Unified Manager für den kürzesten Zeitraum offline ist. In der Unified Manager-Benutzeroberfläche treten Lücken in den erfassten Daten für den Zeitraum auf, in dem das Red Hat Enterprise Linux 7.x-System heruntergefahren ist und bevor das neue Red Hat Enterprise Linux 8.x gestartet wird.

Sehen"Verwalten von Sicherungs- und Wiederherstellungsvorgängen" wenn Sie detaillierte Anweisungen für die Sicherungs- und Wiederherstellungsprozesse lesen müssen.

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

1. Installieren und konfigurieren Sie einen neuen Server mit der Software Red Hat Enterprise Linux 8.x.

   Sehen"Linux-Software und Installationsanforderungen" .

2. Installieren Sie auf dem Red Hat Enterprise Linux 8.x-System dieselbe Version der Unified Manager-Software, die Sie auf dem vorhandenen Red Hat Enterprise Linux 7.x-System haben.

   Sehen"Unified Manager unter Linux installieren" .

   Starten Sie die Benutzeroberfläche nicht und konfigurieren Sie keine Cluster, Benutzer oder Authentifizierungseinstellungen, wenn die Installation abgeschlossen ist. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsvorgangs.

3. Erstellen Sie auf dem Red Hat Enterprise Linux 7.x-System über das Administrationsmenü in der Web-Benutzeroberfläche ein Unified Manager-Backup und kopieren Sie anschließend die Backup-Datei(`.7z` Datei) und den Inhalt des Datenbank-Repository-Verzeichnisses(`/database-dumps-repo`

Unterverzeichnis) an einen externen Speicherort.

4. Fahren Sie Unified Manager auf dem Red Hat Enterprise Linux 7.x-System herunter.
5. Kopieren Sie auf dem Red Hat Enterprise Linux 8.x-System die Sicherungsdatei(`.7z` Datei) vom externen Speicherort in `/opt/netapp/data/ocum-backup/` und die Datenbank-Repository-Dateien in die `/database-dumps-repo` Unterverzeichnis unter dem `/ocum-backup` Verzeichnis.
6. Geben Sie den folgenden Befehl ein, um die Unified Manager-Datenbank aus der Sicherungsdatei wiederherzustellen:

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

7. Geben Sie die IP-Adresse oder URL in Ihren Webbrowser ein, um die Unified Manager-Web-Benutzeroberfläche zu starten, und melden Sie sich dann beim System an.

Nachdem Sie überprüft haben, dass das System ordnungsgemäß funktioniert, können Sie Unified Manager vom Red Hat Enterprise Linux 7.x-System entfernen.

Aktualisieren des Host-Betriebssystems auf demselben Server

Befolgen Sie diese Schritte, wenn Sie kein Ersatzsystem haben, auf dem Sie die Red Hat Enterprise Linux 8.x-Software installieren können.

1. Erstellen Sie im Administrationsmenü der Web-Benutzeroberfläche ein Unified Manager-Backup und kopieren Sie anschließend die Backup-Datei(`.7z` Datei) und den Inhalt des Datenbank-Repository-Verzeichnisses(`/database-dumps-repo` Unterverzeichnis) an einen externen Speicherort.
2. Entfernen Sie das Red Hat Enterprise Linux 7.x-Image vom System und löschen Sie das System vollständig.
3. Installieren und konfigurieren Sie die Red Hat Enterprise Linux 8.x-Software auf demselben System.

   Sehen"Linux-Software und Installationsanforderungen" .

4. Installieren Sie auf dem Red Hat Enterprise Linux 8.x-System dieselbe Version der Unified Manager-Software, die Sie auf dem Red Hat Enterprise Linux 7.x-System hatten.

   Sehen"Unified Manager unter Linux installieren" .

   Starten Sie die Benutzeroberfläche nicht und konfigurieren Sie keine Cluster, Benutzer oder Authentifizierungseinstellungen, wenn die Installation abgeschlossen ist. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsvorgangs.

5. Kopieren Sie die Sicherungsdatei(`.7z` Datei) vom externen Speicherort in `/opt/netapp/data/ocum-backup/` und die Datenbank-Repository-Dateien in die `/database-dumps-repo` Unterverzeichnis unter dem `/ocum-backup` Verzeichnis.
6. Geben Sie den folgenden Befehl ein, um die Unified Manager-Datenbank aus der Sicherungsdatei wiederherzustellen:

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

7. Geben Sie die IP-Adresse oder URL in Ihren Webbrowser ein, um die Unified Manager-Web-Benutzeroberfläche zu starten, und melden Sie sich dann beim System an.

Aktualisieren Sie Produkte von Drittanbietern nach der Installation von Unified Manager

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

Die Unternehmen, die diese Produkte von Drittanbietern entwickeln, melden regelmäßig Sicherheitslücken. Sie können nach Ihrem eigenen Zeitplan auf neuere Versionen dieser Software aktualisieren.

Aktualisieren Sie OpenJDK unter Linux

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

Bevor Sie beginnen

Sie müssen über Root-Berechtigungen für das Linux-System verfügen, auf dem Unified Manager installiert ist.

Sie können OpenJDK-Versionen innerhalb von Versionsfamilien aktualisieren. Sie können beispielsweise ein Upgrade von OpenJDK 11.0.14 auf OpenJDK 11.0.17 durchführen, aber nicht direkt von OpenJDK 11 auf OpenJDK 12.

Schritte

1. Melden Sie sich als Root-Benutzer auf dem Unified Manager-Hostcomputer an.
2. Laden Sie die entsprechende Version von OpenJDK (64-Bit) auf das Zielsystem herunter.
3. Stoppen Sie die Unified Manager-Dienste:

```
systemctl stop ocieau

systemctl stop ocie
```

4. Installieren Sie das neueste OpenJDK auf dem System.
5. Starten Sie die Unified Manager-Dienste:

```
systemctl start ocie

systemctl start ocieau
```

Unified Manager neu starten

Möglicherweise müssen Sie Unified Manager neu starten, nachdem Sie Konfigurationsänderungen vorgenommen haben.

Bevor Sie beginnen

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

Schritte

1. Melden Sie sich als Root-Benutzer bei dem Server an, auf dem Sie den Unified Manager-Dienst neu starten möchten.

2. Stoppen Sie den Unified Manager-Dienst und den zugehörigen MySQL-Dienst in dieser Reihenfolge:

```
systemctl stop ocieau

systemctl stop ocie

systemctl stop mysqld
```

3. Starten Sie die MySQL- und Unified Manager-Dienste 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 erforderlich ist.

Unified Manager entfernen

Sie können Unified Manager mit einem einzigen Befehl vom Red Hat Enterprise Linux-Host stoppen und deinstallieren.

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. Ändern Sie den SELinux-Laufzeitmodus auf „Permissive“, indem Sie `setenforce 0` Befehl.
- Alle Cluster (Datenquellen) müssen vom Unified Manager-Server entfernt werden, bevor die Software entfernt wird.
- Sie sollten die Firewall-Regeln, die zum Zulassen oder Blockieren des MySQL-Ports 3306 erstellt wurden, manuell löschen. Die Firewall-Regeln werden nicht automatisch gelöscht.

Schritte

1. Melden Sie sich als Root-Benutzer bei dem Server an, von dem Sie Unified Manager entfernen möchten.
2. Stoppen und entfernen Sie Unified Manager vom Server:

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

   Dieser Schritt entfernt alle zugehörigen NetApp RPM-Pakete. Die erforderlichen Softwaremodule wie Java, MySQL und p7zip werden nicht entfernt.

3. **Optional:** Entfernen Sie gegebenenfalls die unterstützenden Softwaremodule wie Java, MySQL und p7zip:

   ```
   rpm -e p7zip 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 der `/opt/netapp/data` Das

Verzeichnis wird verschoben in das `/opt/netapp/data/BACKUP` Ordner nach der Deinstallation. Durch die Deinstallation von Unified Manager werden auch die Java- und MySQL-Pakete entfernt, es sei denn, die Pakete werden von einer anderen Anwendung auf dem System benötigt und verwendet. MySQL-Daten werden jedoch nicht gelöscht.

Entfernen Sie den benutzerdefinierten Umadmin-Benutzer und die Wartungsgruppe

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 benutzerdefinierte Umadmin-Benutzer und Wartungskonten nicht entfernt. Sie müssen diese Elemente manuell löschen.

Schritte

1. Melden Sie sich als Root-Benutzer beim Red Hat Enterprise Linux-Server an.
2. Löschen Sie den umadmin-Benutzer:

   ```
   userdel umadmin
   ```

3. Löschen Sie die Wartungsgruppe:

   ```
   groupdel maintenance
   ```

Installieren Sie Unified Manager auf Windows-Systemen

Einführung in Active IQ Unified Manager

Mit Active IQ Unified Manager (früher OnCommand Unified Manager) können Sie den Zustand und die Leistung Ihrer ONTAP -Speichersysteme über eine einzige Schnittstelle überwachen und verwalten. Sie können Unified Manager auf einem Linux-Server, einem Windows-Server oder als virtuelle Appliance auf einem VMware-Host bereitstellen.

Nachdem Sie die Installation abgeschlossen und die Cluster hinzugefügt haben, die Sie verwalten möchten, bietet Unified Manager eine grafische Benutzeroberfläche, die die Kapazität, Verfügbarkeit, den Schutz und den Leistungsstatus der überwachten Speichersysteme anzeigt.

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Was der Unified Manager-Server macht

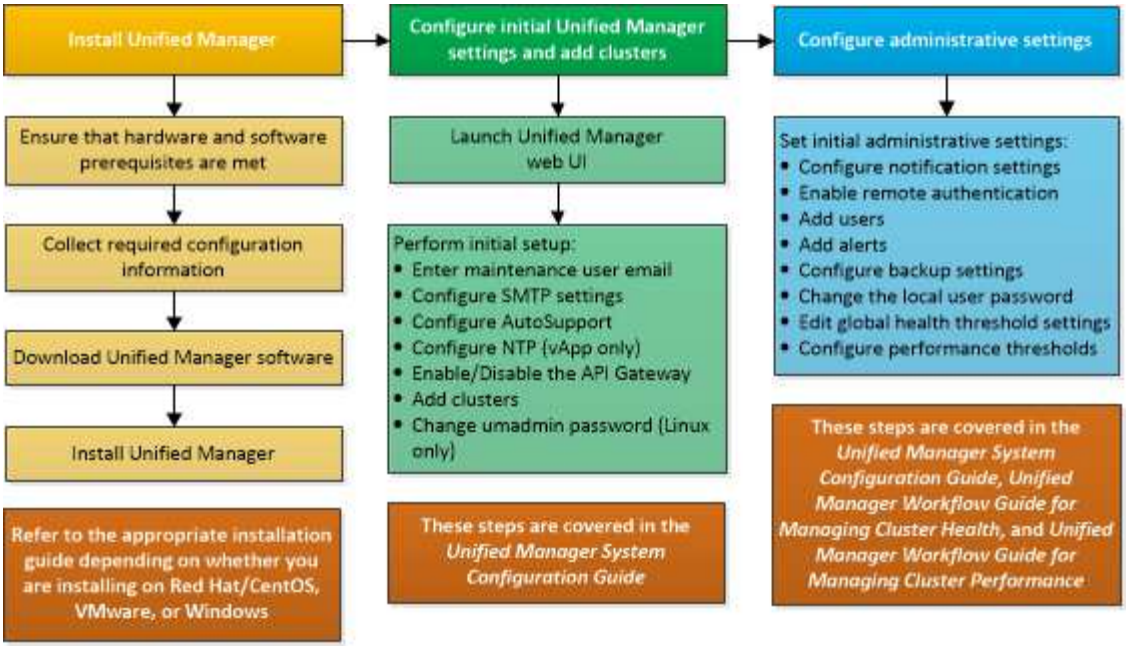
Die Unified Manager-Serverinfrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Anwendungsserver. Es bietet Infrastrukturdienste wie Erkennung, Überwachung, rollenbasierte Zugriffskontrolle (RBAC), Auditing und Protokollierung.

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

Übersicht über den Installationsablauf

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

In diesen Abschnitten werden alle im folgenden Arbeitsablauf angezeigten Elemente beschrieben.



Voraussetzungen für die Installation von Unified Manager

Stellen Sie vor Beginn des Installationsvorgangs sicher, dass der Server, auf dem Sie Unified Manager installieren möchten, die spezifischen Software-, Hardware-, CPU- und Speicheranforderungen erfüllt.

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

Weitere Einzelheiten zum Anwenden von Sicherheitsmaßnahmen auf den Unified Manager-Server finden Sie im Knowledge Base-Artikel.

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

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

Anforderungen an die virtuelle Infrastruktur und das Hardwaresystem

Die Installation von Unified Manager auf einer virtuellen Infrastruktur oder einem physischen System sollte die Mindestanforderungen an Arbeitsspeicher, CPU und Festplattenspeicher erfüllen.

In der folgenden Tabelle sind die empfohlenen Werte für Arbeitsspeicher-, CPU- und Festplattenspeicherressourcen aufgeführt. Diese Werte wurden qualifiziert, sodass Unified Manager akzeptable Leistungsniveaus erreicht.

Hardwarekonfiguration	Empfohlene Einstellungen
RAM	12 GB (Mindestanforderung 8 GB)
Prozessoren	4 CPUs
CPU-Zykluskapazität	9572 MHz gesamt (Mindestanforderung 9572 MHz)
Freier Speicherplatz	150 GB, wobei die Kapazität wie folgt aufgeteilt ist: • 100 GB Speicherplatz für das Installationsverzeichnis • 50 GB Speicherplatz für das MySQL-Datenverzeichnis

Unified Manager kann auf Systemen mit wenig Arbeitsspeicher installiert werden, die empfohlenen 12 GB RAM stellen jedoch sicher, dass genügend Arbeitsspeicher für eine optimale Leistung zur Verfügung steht und dass das System bei wachsender Konfiguration zusätzliche Cluster und Speicherobjekte aufnehmen kann. Sie sollten auf der VM, auf der Unified Manager bereitgestellt wird, keine Speicherbeschränkungen festlegen und keine Funktionen (z. B. Ballooning) aktivieren, die die Software daran hindern, den zugewiesenen Speicher auf dem System zu nutzen.

Darüber hinaus gibt es eine Begrenzung für die Anzahl der Knoten, die eine einzelne Instanz von Unified Manager überwachen kann, bevor Sie eine zweite Instanz von Unified Manager installieren. Weitere Informationen finden Sie im *Best Practices Guide*.

"Technischer Bericht 4621: Leitfaden zu Best Practices für Unified Manager"

Das Auslagern von Speicherseiten wirkt sich negativ auf die Leistung des Systems und der Verwaltungsanwendung aus. Der Wettbewerb um CPU-Ressourcen, die aufgrund der Gesamtauslastung des Hosts nicht verfügbar sind, kann die Leistung beeinträchtigen.

Voraussetzung für die dedizierte Nutzung

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, sollte ausschließlich für Unified Manager verwendet und nicht mit anderen Anwendungen geteilt werden. Andere Anwendungen verbrauchen möglicherweise Systemressourcen und können die Leistung von Unified Manager drastisch reduzieren.

Speicherplatzbedarf für Backups

Wenn Sie die Sicherungs- und Wiederherstellungsfunktion von Unified Manager verwenden möchten, weisen Sie zusätzliche Kapazität zu, sodass das Verzeichnis oder die Festplatte „`data`“ über 150 GB Speicherplatz verfügt. Eine Sicherung kann an ein lokales oder ein Remote-Ziel geschrieben werden. Die beste Vorgehensweise besteht darin, einen Remote-Standort außerhalb des Unified Manager-Hostsystems zu identifizieren, der über mindestens 150 GB Speicherplatz verfügt.

Anforderungen für die Hostkonnektivität

Das physische oder virtuelle System, auf dem Sie Unified Manager installieren, sollte so konfiguriert sein, dass Sie erfolgreich `ping` der Hostname vom Host selbst. Bei einer IPv6-Konfiguration sollten Sie überprüfen, ob `ping6` zum Hostnamen erfolgreich ist, um sicherzustellen, dass die Installation von Unified Manager erfolgreich ist.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Web-Benutzeroberfläche des Produkts zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie einen Namen für den Netzwerkhost festgelegt. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollten Sie den Hostnamen vom DNS beziehen.

Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen statt über den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse ermöglichen möchten, muss Ihre Netzwerkkonfiguration diesen Kurznamen in einen gültigen FQDN auflösen.

Windows-Software- und Installationsanforderungen

Für die erfolgreiche Installation von Unified Manager unter Windows sollten Sie sicherstellen, dass das System, auf dem Unified Manager installiert wird, die Softwareanforderungen erfüllt.

Betriebssystemsoftware

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

- Microsoft Windows Server 2019 Standard und 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 aktuelle Liste der unterstützten Windows-Versionen finden Sie in der Interoperabilitätsmatrix.

"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 die Ausführung von Unified Manager vorgesehen sein. Auf dem Server sollten keine anderen Anwendungen installiert sein. Möglicherweise ist aufgrund von Unternehmensvorschriften eine aktive Antivirensoftware auf Ihrem Windows-System installiert. Sie sollten die Antivirensoftware vor der Installation von Unified Manager deaktivieren, um zu verhindern, dass die Installation fehlschlägt.

Software von Drittanbietern

Die folgenden Pakete von Drittanbietern sind im Unified Manager enthalten. Wenn diese Drittanbieterpakete nicht auf Ihrem System installiert sind, installiert Unified Manager sie als Teil der Installation.

- Microsoft Visual C Redistributable Packages für Visual Studio 2015, Version 14.26.28720.3
- MySQL Community Edition Version 8.4.4
- Python 3.12.4

- OpenJDK Version 11.0.25
- 7-Zip Version 23.01 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, sollten Sie Folgendes sicherstellen:

- Es wird der Standardport verwendet.
- Die Beispieldatenbanken sind nicht installiert.
- Der Dienstname lautet „MYSQL84“.

Unified Manager wird auf einem WildFly-Webserver bereitgestellt. WildFly 26.1.3 ist mit Unified Manager gebündelt und konfiguriert.

Sie sollten eine laufende Instanz von Unified Manager herunterfahren, bevor Sie Software von Drittanbietern aktualisieren. Nachdem die Installation der Drittanbietersoftware abgeschlossen ist, können Sie Unified Manager neu starten.

Installationsvoraussetzungen

- Microsoft .NET 4.5.2 oder höher sollte installiert sein.
- Der `temp` Das Verzeichnis sollte mit 2 GB Speicherplatz zum Extrahieren der Installationsdateien konfiguriert werden. Um zu überprüfen, ob das Verzeichnis erstellt wurde, führen Sie den folgenden Befehl in der Befehlszeilenschnittstelle aus: `echo %temp%`
- Sie sollten 2 GB Speicherplatz auf dem Windows-Laufwerk für die Zwischenspeicherung der Unified Manager MSI-Dateien reservieren.
- Der Microsoft Windows Server, auf dem Sie Unified Manager installieren möchten, sollte mit einem vollqualifizierten Domänennamen (FQDN) konfiguriert sein, sodass `ping` Antworten auf den Hostnamen und den FQDN sind erfolgreich.
- Sie sollten den weltweiten Web-Publishing-Dienst von Microsoft IIS deaktivieren und sicherstellen, dass die Ports 80 und 443 frei sind.
- Sie sollten sicherstellen, dass die Remotedesktop-Sitzungshost-Einstellung für „Windows Installer RDS-Kompatibilität“ während der Installation deaktiviert ist.
- UDP-Port 514 sollte frei sein und von keinem anderen Dienst verwendet werden.
- Sie sollten vor der Installation von Unified Manager sämtliche Antivirenprogramme auf Ihrem System deaktivieren. Stellen Sie nach Abschluss der Installation sicher, dass Sie die folgenden Pfade manuell vom Virenscan ausschließen:
  - Unified Manager-Datenverzeichnis, zum Beispiel `C:\ProgramData\NetApp\OnCommandAppData\`
  - Unified Manager-Installationsverzeichnis, zum Beispiel `\C:\Program Files\NetApp\`
  - MySQL-Datenverzeichnis, zum Beispiel `C:\ProgramData\MySQL\MySQLServerData`

Unterstützte Browser

Verwenden Sie einen unterstützten Browser, um auf die Unified Manager-Web-Benutzeroberfläche zuzugreifen.

Die Interoperabilitätsmatrix enthält die Liste der unterstützten Browserversionen.

"mysupport.netapp.com/matrix"

Durch die Deaktivierung von Popup-Blockern wird bei allen Browsern sichergestellt, dass 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

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

Verbindungen zum Unified Manager-Server

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

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

Schnittstelle	Protokoll	Hafen	Beschreibung
Unified Manager-Web-Benutzeroberfläche	HTTP	80	Wird für den Zugriff auf die Unified Manager-Web-Benutzeroberfläche verwendet; leitet automatisch zum sicheren Port 443 um.
Unified Manager-Web-UI und Programme mit APIs	HTTPS	443	Wird verwendet, um sicher auf die Unified Manager-Web-Benutzeroberfläche zuzugreifen oder API-Aufrufe zu tätigen; API-Aufrufe können nur über HTTPS erfolgen.
Wartungskonsole	SSH/SFTP	22	Wird verwendet, um auf die Wartungskonsole zuzugreifen und Supportpakete abzurufen.

Schnittstelle	Protokoll	Hafen	Beschreibung
Linux-Befehlszeile	SSH/SFTP	22	Wird verwendet, um auf die Red Hat Enterprise Linux-Befehlszeile zuzugreifen und Support-Pakete abzurufen.
Syslog	UDP	514	Wird verwendet, um auf abonnementbasierte EMS-Nachrichten von ONTAP Systemen zuzugreifen und auf der Grundlage der Nachrichten Ereignisse zu erstellen.
AUSRUHEN	HTTPS	9443	Wird verwendet, um auf REST-API-basierte EMS-Ereignisse in Echtzeit von authentifizierten ONTAP Systemen zuzugreifen.
MySQL-Datenbank	MySQL	3306	Wird verwendet, um den Zugriff auf Unified Manager OnCommand Workflow Automation und OnCommand API Services zu ermöglichen.
AMQP QPID-Broker	TCP/IP	56072	Wird für die interne Nachrichtenkommunikation verwendet.
AMQP QPID-Broker	WebSocket über TCP	56080	Wird verwendet, um auf diesem Port auf von ONTAP (Cloud-Agent) empfangene Nachrichten zu lauschen.
AMQP QPID-Broker	WebSocket über TCP	56443	Wird verwendet, um auf diesem Port auf von ONTAP (Cloud-Agent) empfangene Nachrichten zu lauschen. Die Kommunikation über diesen Port unterstützt die Verschlüsselung durch TLS oder SSL.

Der Standardport für MySQL, 3306, ist bei der Installation von Unified Manager auf Windows-Systemen nur auf localhost beschränkt. Aktivieren Sie die Firewall, um den Zugriff auf den MySQL-Port 3306 einzuschränken, sobald die Installation abgeschlossen ist. Dies hat keine Auswirkungen auf Upgrade-Szenarien, bei denen die vorherige Konfiguration beibehalten wird. Diese Konfiguration kann geändert werden, und die Verbindung kann anderen Hosts zur Verfügung gestellt werden, indem man den `Control access to MySQL port 3306` Option auf der Wartungskonsole. Weitere Informationen finden Sie unter"Zusätzliche Menüoptionen" . Die für die HTTP- und HTTPS-Kommunikation verwendeten Ports (Ports 80 und 443) können über die Wartungskonsole von Unified Manager geändert werden. Weitere Informationen finden Sie unter "Konfigurieren von Active IQ Unified Manager".

Verbindungen vom Unified Manager-Server

Sie sollten Ihre Firewall so konfigurieren, dass Ports geöffnet werden, die die Kommunikation zwischen dem Unified Manager-Server und verwalteten Speichersystemen, Servern und anderen Komponenten ermöglichen. Wenn ein Port nicht geöffnet ist, schlägt die Kommunikation fehl.

Abhängig von Ihrer Umgebung können Sie die vom Unified Manager-Server zum Herstellen einer Verbindung mit bestimmten Zielen verwendeten Ports und Protokolle ändern.

Der Unified Manager-Server stellt über die folgenden Protokolle und Ports eine Verbindung zu den verwalteten Speichersystemen, Servern und anderen Komponenten her:

Ziel	Protokoll	Hafen	Beschreibung
Speichersystem	HTTPS	443/TCP	Wird zur Überwachung und Verwaltung von Speichersystemen verwendet.
Speichersystem	NDMP	10000/TCP	Wird für bestimmte Snapshot-Wiederherstellungsvorgänge verwendet.
AutoSupport -Server	HTTPS	443	Wird zum Senden von AutoSupport -Informationen verwendet. Für die Ausführung dieser Funktion ist ein Internetzugang erforderlich.
Authentifizierungsserver	LDAP	389	Wird verwendet, um Authentifizierungsanfragen sowie Benutzer- und Gruppensuchanfragen zu stellen.

Ziel	Protokoll	Hafen	Beschreibung
LDAPS	636	Wird für die sichere LDAP-Kommunikation verwendet.	Mailserver
SMTP	25	Wird zum Senden von E-Mail-Benachrichtigungen verwendet.	SNMP-Trap-Sender
SNMPv1 oder SNMPv3	162/UDP	Wird zum Senden von SNMP-Traps für Warnbenachrichtigungen verwendet.	Externer Datenanbieterserver
TCP	2003	Wird verwendet, um Leistungsdaten an einen externen Datenanbieter wie Graphite zu senden.	NTP-Server
NTP	123/UDP	Wird verwendet, um die Zeit auf dem Unified Manager-Server mit einem externen NTP-Zeitserver zu synchronisieren. (Nur VMware-Systeme)	AMQP QPID-Broker
TCP/IP	56072	Wird für die interne Nachrichtenkommunikation verwendet.	AMQP QPID-Broker
WebSocket über TCP	56080	Wird verwendet, um auf diesem Port auf von ONTAP (Cloud-Agent) empfangene Nachrichten zu lauschen.	AMQP QPID-Broker
WebSocket über TCP	56443	Wird verwendet, um auf diesem Port auf von ONTAP (Cloud-Agent) empfangene Nachrichten zu lauschen. Die Kommunikation über diesen Port unterstützt die Verschlüsselung durch TLS oder SSL.	Syslog

Füllen Sie das Arbeitsblatt aus

Bevor Sie Unified Manager installieren und konfigurieren, sollten Sie bestimmte Informationen zu Ihrer Umgebung zur Hand haben. Sie können die Informationen im Arbeitsblatt festhalten.

Unified Manager-Installationsinformationen

Die zur Installation von Unified Manager erforderlichen Details.

System, auf dem die Software bereitgestellt wird	Ihr Wert
Vollqualifizierter Domänenname des Hosts	
Host-IP-Adresse	
Netzwerkmaske	
Gateway-IP-Adresse	
Primäre DNS-Adresse	
Sekundäre DNS-Adresse	
Suchdomänen	
Wartungsbenutzername	
Wartungsbenutzerkennwort	

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	
Hostname oder IP-Adresse des SMTP-Servers	
SMTP-Benutzername	
SMTP-Passwort	
SMTP-Port	25 (Standardwert)

Einstellung	Ihr Wert
E-Mail, von der Warnbenachrichtigungen gesendet werden	
Hostname oder IP-Adresse des Authentifizierungsservers	
Active Directory-Administratorname oder LDAP-Bind-Distinguished Name	
Active Directory-Passwort oder LDAP-Bind-Passwort	
Basis-Distinguished Name des Authentifizierungsservers	
URL des Identitätsanbieters (IdP)	
Metadaten des Identitätsanbieters (IdP)	
IP-Adressen des SNMP-Trap-Zielhosts	
SNMP-Port	

Cluster-Informationen

Die Details für die Speichersysteme, die Sie mit Unified Manager verwalten.

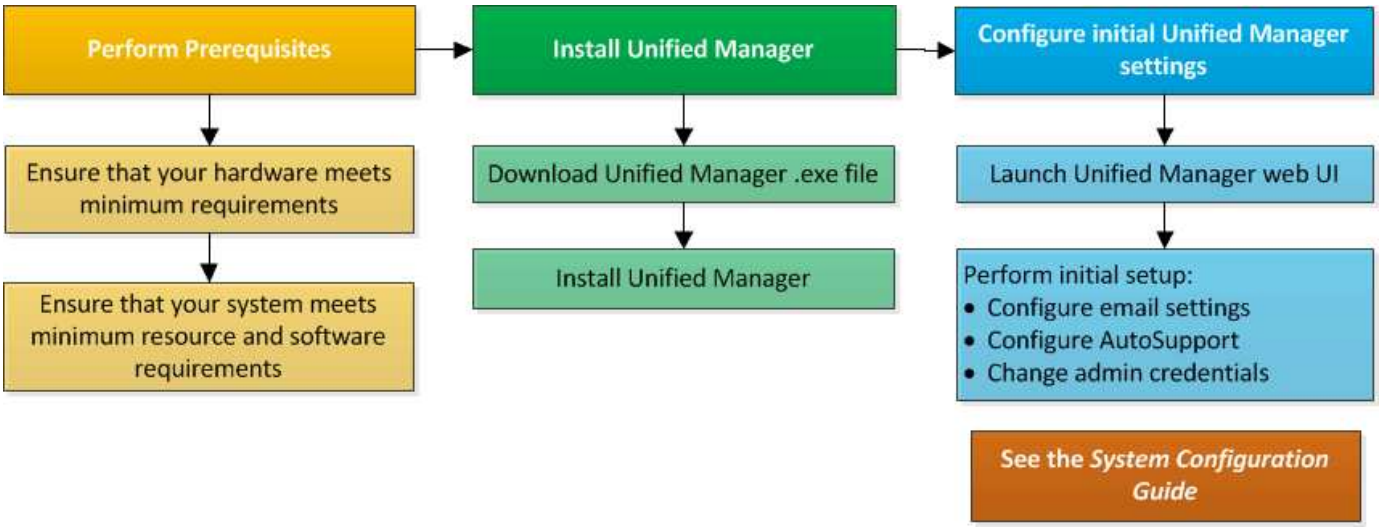
Cluster 1 von N	Ihr Wert
Hostname oder IP-Adresse zur Clusterverwaltung	
ONTAP -Administratorbenutzername Dem Administrator muss die Rolle „`admin`“ zugewiesen worden sein.	
ONTAP -Administratorkennwort	
Protokoll	HTTPS

Installieren, aktualisieren und entfernen Sie die Unified Manager-Software

Sie können Unified Manager installieren, auf eine neuere Version aktualisieren oder die Unified Manager-Anwendung entfernen.

Übersicht über den Installationsprozess

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



Installieren Sie Unified Manager unter Windows

Es ist wichtig, dass Sie die Abfolge der Schritte zum Herunterladen und Installieren von Unified Manager unter Windows verstehen.

Unified Manager installieren

Sie können Unified Manager installieren, um Probleme hinsichtlich der Datenspeicherkapazität, Verfügbarkeit, Leistung und Sicherheit zu überwachen und zu beheben.

Bevor Sie beginnen

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

  Sehen"Hardware-Systemanforderungen" .

  Sehen"Windows-Software- und Installationsanforderungen" .

  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. Stellen Sie sicher, dass Ihr Benutzername nicht mit einem Ausrufezeichen beginnt.!". `Installation of Unified Manager might fail if the user name of user running the installation begins with "!`".
- Alle Cluster werden unterstützt, mit Ausnahme von ASA R2-Systemen.
- Sie sollten über einen unterstützten Webbrowser verfügen.
- Das Wartungsbenutzerkennwort für Unified Manager sollte zwischen 8 und 20 Zeichen lang sein und Groß- oder Kleinbuchstaben, Ziffern und Sonderzeichen enthalten.

- Die folgenden Sonderzeichen sind in der Kennwortzeichenfolge für den Wartungsbenutzer oder für den MySQL-Root-Benutzer nicht zulässig: " ' ` % , = & < > | ^ \ / ( ) [ ] ;:

  Folgende Sonderzeichen sind erlaubt: ~ ! @ # $ * - ? . + { }

Schritte

1. Melden Sie sich mit dem standardmäßigen lokalen Administratorkonto bei Windows an.
2. Melden Sie sich bei der NetApp Support-Site an und navigieren Sie zur Download-Seite für Unified Manager:

   "NetApp Support Site"

3. Wählen Sie die erforderliche Version von Unified Manager aus und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA).
4. Laden Sie die Windows-Installationsdatei oder ZIP-Datei von Unified Manager in ein Zielverzeichnis auf dem Windows-System herunter.
5. Extrahieren Sie bei Bedarf die ZIP-Datei und navigieren Sie zu dem Verzeichnis, in dem sich die Installationsdatei befindet.
6. Klicken Sie mit der rechten Maustaste und führen Sie die ausführbare Datei (.exe) des Unified Manager-Installationsprogramms als Administrator aus.

   Unified Manager erkennt fehlende oder vorinstallierte Pakete von Drittanbietern und listet sie auf. Wenn die erforderlichen Pakete von Drittanbietern nicht im System installiert sind, installiert Unified Manager sie als Teil der Installation.

7. Klicken Sie auf **Weiter**.
8. Geben Sie den Benutzernamen und das Kennwort ein, um den Wartungsbenutzer zu erstellen.
9. Geben Sie im Datenbankverbindungsassistenten das MySQL-Root-Passwort ein.
10. Klicken Sie auf **Ändern**, um einen neuen Speicherort für das Unified Manager-Installationsverzeichnis und das MySQL-Datenverzeichnis anzugeben.

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

11. Klicken Sie auf **Weiter**.
12. Klicken Sie im Assistenten „Bereit zur Installation von Shield“ auf **Installieren**.
13. Klicken Sie nach Abschluss der Installation auf **Fertig**.
14. Wenn auf Ihrem Windows-System eine aktive Antivirensoftware installiert ist, schließen Sie nach Abschluss der Installation die folgenden Pfade manuell vom Antivirenscan aus:
    - Unified Manager-Datenverzeichnis
    - Unified Manager-Installationsverzeichnis
    - MySQL-Datenverzeichnis

Bei der Installation werden mehrere Verzeichnisse erstellt:

- 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, die 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\`

- Unified Manager-Anwendungsdatenverzeichnis (appDataDir)

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

Sie können auf die Web-Benutzeroberfläche zugreifen, um die Ersteinrichtung von Unified Manager durchzuführen, wie im Abschnitt"Konfigurieren von Active IQ Unified Manager" .

Führen Sie eine unbeaufsichtigte Installation von Unified Manager durch

Sie können Unified Manager ohne Benutzereingriff über die Befehlszeilenschnittstelle installieren. Sie können die unbeaufsichtigte Installation abschließen, indem Sie die Parameter in Schlüssel-Wert-Paaren übergeben.

Schritte

1. Melden Sie sich mit dem standardmäßigen lokalen Administratorkonto bei der Windows-Befehlszeilenschnittstelle an.
2. Navigieren Sie zu dem Speicherort, an dem Sie Unified Manager installieren möchten, und wählen Sie eine der folgenden Optionen:

Option	Anweisungen

Wenn Pakete von Drittanbietern 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"`

Wenn keine Pakete von Drittanbietern 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"`

Der `/qr` Option aktiviert den Ruhemodus mit einer reduzierten Benutzeroberfläche. Es wird eine einfache Benutzeroberfläche angezeigt, die den Installationsfortschritt anzeigt. Sie werden nicht zu Eingaben aufgefordert. Wenn Drittanbieterpakete wie JRE, MySQL und 7zip nicht vorinstalliert sind, sollten Sie die `/qr` Option. Die Installation schlägt fehl, wenn `/qn` Option wird auf einem Server verwendet, auf dem keine Pakete von Drittanbietern installiert sind.

Der `/qn` Option aktiviert den Ruhemodus ohne Benutzeroberfläche. Während der Installation werden keine Benutzeroberfläche oder Details angezeigt. Sie sollten nicht verwenden die `/qn` Option, wenn keine Pakete von Drittanbietern installiert sind.

3. Melden Sie sich mit der folgenden URL bei der Web-Benutzeroberfläche von Unified Manager an:

   `https://IP address`

Ändern des JBoss-Passworts

Sie können das instanzspezifische JBoss-Passwort zurücksetzen, das während der Installation festgelegt wurde. Sie können das Kennwort optional zurücksetzen, falls Ihre Site diese Sicherheitsfunktion benötigt, um die Installationseinstellung des Unified Managers zu überschreiben. Dieser Vorgang ändert auch das Kennwort, das JBoss für den Zugriff auf MySQL verwendet.

Bevor Sie beginnen

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

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

Schritte

1. Melden Sie sich als Administratorbenutzer auf dem Unified Manager-Hostcomputer an.
2. Verwenden Sie die Windows-Dienstekonsole, um die folgenden Unified Manager-Dienste zu stoppen:
   - NetApp Active IQ Acquisition Service (Ocie-au)
   - NetApp Active IQ Management Server-Dienst (Oncommandsvc)
3. Starten Sie die `password.bat` Skript zum Starten des Kennwortänderungsprozesses:

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

4. Geben Sie bei der entsprechenden Aufforderung das MySQL-Root-Benutzerkennwort ein.
5. Geben Sie bei entsprechender Aufforderung das neue JBoss-Benutzerkennwort ein und geben Sie es zur Bestätigung erneut ein.

   Beachten Sie, dass das Passwort zwischen 8 und 16 Zeichen lang sein sollte und mindestens eine Ziffer, einen Großbuchstaben, einen Kleinbuchstaben und mindestens eines dieser Sonderzeichen enthalten muss:

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

6. Wenn das Skript abgeschlossen ist, starten Sie die Unified Manager-Dienste mithilfe der Windows-Dienstekonsole:
   - NetApp Active IQ Management Server-Dienst (Oncommandsvc)
   - NetApp Active IQ Acquisition Service (Ocie-au)
7. Nachdem alle Dienste gestartet wurden, können Sie sich bei der Unified Manager-Benutzeroberfläche anmelden.

Unterstützter Upgrade-Pfad für Unified Manager-Versionen

Active IQ Unified Manager unterstützt für jede Version einen bestimmten Upgradepfad.

Nicht alle Versionen von Unified Manager können ein direktes Upgrade auf neuere Versionen durchführen. Die Unified Manager-Upgrades sind auf ein N-2-Modell beschränkt, d. h. ein Upgrade kann auf allen Plattformen nur innerhalb der nächsten zwei Versionen durchgeführt werden. Sie können beispielsweise nur von Unified Manager 9.13 und 9.14 ein Upgrade auf Unified Manager 9.16 durchführen.

Wenn Sie eine Version ausführen, die älter ist als die unterstützten Versionen, muss Ihre Unified Manager-Instanz zuerst auf eine der unterstützten Versionen und dann auf die aktuelle Version aktualisiert werden.

Wenn Sie beispielsweise die Version Unified Manager 9.9 installiert haben und auf Unified Manager 9.14 aktualisieren möchten, befolgen Sie eine Upgrade-Reihenfolge.

Beispielhafter Upgradepfad:

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

Weitere Informationen zur Upgrade-Pfadmatrix finden Sie hier "Wissensdatenbankartikel (KB)" .

Upgrade von Unified Manager

Sie können Unified Manager 9.13 oder 9.14 auf 9.16 aktualisieren, indem Sie die Installationsdatei auf der Windows-Plattform herunterladen und ausführen.

Bevor Sie beginnen

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

  Sehen"Hardware-Systemanforderungen" .

  Sehen"Windows-Software- und Installationsanforderungen" .

  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.

  Stellen Sie sicher, dass Microsoft .NET 4.5.2 oder höher auf Ihrem System installiert ist, bevor Sie mit dem Upgrade beginnen.

- MySQL Community Edition wird während des Unified Manager-Upgrades automatisch aktualisiert. Wenn die auf Ihrem System installierte MySQL-Version älter als 8.4.4 ist, aktualisiert der Upgrade-Prozess von Unified Manager MySQL automatisch auf 8.4.4. Sie dürfen kein eigenständiges Upgrade einer früheren MySQL-Version auf 8.4.4 ausführen.
- Alle Cluster werden unterstützt, mit Ausnahme von ASA r2-Systemen.
- Sie sollten über Windows-Administratorrechte verfügen. Stellen Sie sicher, dass Ihr Benutzername nicht mit einem Ausrufezeichen beginnt.!". `Installation of Unified Manager might fail if the user name of user running the installation begins with "!`".

- Sie sollten über gültige Anmeldeinformationen verfügen, um sich bei der NetApp Support-Site anzumelden.
- Um Datenverlust zu vermeiden, sollten Sie für den Fall, dass während des Upgrades ein Problem auftritt, eine Sicherungskopie der Unified Manager-Maschine erstellt haben.
- Für die Durchführung des Upgrades sollte ausreichend Speicherplatz verfügbar sein.

  Der verfügbare Speicherplatz auf dem Installationslaufwerk sollte 2,5 GB größer sein als die Größe des Datenverzeichnisses. Wenn nicht genügend freier Speicherplatz vorhanden ist, wird das Upgrade angehalten und eine Fehlermeldung mit der Angabe des hinzuzufügenden Speicherplatzes angezeigt.

- Während des Upgrades werden Sie möglicherweise aufgefordert zu bestätigen, ob Sie die vorherigen Standardeinstellungen für die Aufbewahrung der Leistungsdaten für 13 Monate beibehalten oder auf 6 Monate ändern möchten. Bei der Bestätigung werden die historischen Leistungsdaten nach 6 Monaten gelöscht.
- Vor dem Upgrade sollten Sie alle geöffneten Dateien oder Ordner in *<InstallDir>\JDK* und *MySQL Data Directory* schließen.
- Wenn auf Ihrem Windows-System eine aktive Antivirensoftware installiert ist, kann das Upgrade von Unified Manager fehlschlagen. Sie sollten alle Virenscan-Programme auf Ihrem System deaktivieren, bevor Sie Unified Manager aktualisieren.

Während des Upgrade-Vorgangs ist Unified Manager nicht verfügbar. Sie sollten alle laufenden Vorgänge abschließen, bevor Sie Unified Manager aktualisieren.

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 der Durchführung der Upgrades eine neue Workflow Automation-Verbindung einrichten. Wenn Sie ein Upgrade nur für eines der Produkte durchführen, sollten Sie sich nach dem Upgrade bei Workflow Automation anmelden und überprüfen, ob weiterhin Daten vom Unified Manager abgerufen werden.

Schritte

1. Melden Sie sich bei der NetApp Support-Site an und navigieren Sie zur Download-Seite für Unified Manager:

   "NetApp Support Site".

2. Wählen Sie die erforderliche Version von Unified Manager aus und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA).
3. Laden Sie die Windows-Installationsdatei oder ZIP-Datei von Unified Manager in ein Zielverzeichnis auf dem Windows-System herunter. Extrahieren Sie bei Bedarf die ZIP-Datei und navigieren Sie zu dem Verzeichnis, in dem sich die Installationsdatei befindet. Klicken Sie mit der rechten Maustaste und führen Sie die ausführbare Datei (.exe) des Unified Manager-Installationsprogramms als Administrator aus.

   Unified Manager fordert Sie mit der folgenden Meldung auf:

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

4. Klicken Sie auf **Ja** und dann auf **Weiter**.
5. Geben Sie das MySQL84-Root-Passwort ein, das während der Installation festgelegt wurde, und klicken Sie dann auf **Weiter**.

6. Starten Sie die Web-Benutzeroberfläche in einem neuen Fenster eines unterstützten Webbrowsers und melden Sie sich an, um die aktualisierte Version von Unified Manager zu verwenden.
7. Wenn auf Ihrem Windows-System eine aktive Antivirensoftware installiert ist, achten Sie darauf, die folgenden Pfade nach Abschluss des Upgrades manuell vom Antivirenscan auszuschließen:
   - Unified Manager-Datenverzeichnis
   - Unified Manager-Installationsverzeichnis
   - MySQL-Datenverzeichnis

> Um ein stilles Upgrade von Unified Manager durchzuführen, führen Sie den folgenden Befehl aus:
> `ActiveIQUnifiedManager-<version\>.exe /s /v"MYSQL_PASSWORD=<password> /qn /l*v <system_drive>:\install.log"`

Upgrade von Produkten von Drittanbietern

Sie können Produkte von Drittanbietern, wie etwa JRE, auf Unified Manager aktualisieren, wenn diese auf Windows-Systemen installiert sind.

Die Unternehmen, die diese Produkte von Drittanbietern entwickeln, melden regelmäßig Sicherheitslücken. Sie können nach Ihrem eigenen Zeitplan auf neuere Versionen dieser Software aktualisieren.

OpenJDK aktualisieren

Sie können auf dem Windows-Server, auf dem Unified Manager installiert ist, ein Upgrade auf eine neuere Version von OpenJDK durchführen, um Fixes für Sicherheitslücken zu erhalten.

Bevor Sie beginnen

Sie müssen über Windows-Administratorrechte für das System verfügen, auf dem Unified Manager installiert ist.

Sie können OpenJDK-Versionen innerhalb von Versionsfamilien aktualisieren. Sie können beispielsweise von OpenJDK 11.0.16 auf OpenJDK 11.0.18 aktualisieren, aber nicht direkt von OpenJDK 11 auf OpenJDK 12.

Schritte

1. Melden Sie sich als Administratorbenutzer auf dem Unified Manager-Hostcomputer an.
2. Laden Sie die entsprechende Version von OpenJDK (64-Bit) von der OpenJDK-Site auf das Zielsystem herunter.

   Laden Sie beispielsweise herunter `jdk-11.0.18_windows-x64_bin.zip from https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html` .

   > Zum Herunterladen der Datei ist ein Oracle-Konto erforderlich. Wenn Sie kein Oracle-Konto haben, gehen Sie zu"Oracle-Kontoanmeldung" Seite, um eine zu erstellen.

3. Verwenden Sie die Windows-Dienstekonsole, um die folgenden Unified Manager-Dienste zu stoppen:
   - NetApp Active IQ Acquisition Service (Ocie-au)

- NetApp Active IQ Management Server-Dienst (Oncommandsvc)

4. Erweitern Sie die `zip` Datei.
5. Kopieren Sie die Verzeichnisse und Dateien aus dem resultierenden `jdk` Verzeichnis (zum Beispiel `jdk-11.0.18` an den Ort, an dem Java installiert ist. Beispiel: `C:\Program Files\NetApp\JDK\`
6. Starten Sie die Unified Manager-Dienste mithilfe der Windows-Dienstekonsole:
   - NetApp Active IQ Management Server-Dienst (Oncommandsvc)
   - NetApp Active IQ Acquisition Service (Ocie-au)

Deinstallieren Sie Produkte von Drittanbietern

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

Deinstallieren Sie Python

Schritte

1. Wählen Sie in der **Systemsteuerung Programme** > **Programme und Funktionen**.
2. Wählen Sie Python aus der Programmliste aus.
3. Wählen Sie **Dieses Programm deinstallieren**. Deinstallieren Sie alle Python-Versionen außer 3.12. Stellen Sie sicher, dass Sie die Python-Version 3.12 behalten.

Deinstallieren Sie Microsoft Visual C++ 2013

Schritte

1. Wählen Sie in der **Systemsteuerung Programme** > **Programme und Funktionen**.
2. Wählen Sie **Microsoft Visual C++ 2013** aus der Programmliste.
3. Wählen Sie **Dieses Programm deinstallieren**.

Unified Manager neu starten

Möglicherweise müssen Sie Unified Manager neu starten, nachdem Sie Konfigurationsänderungen vorgenommen haben.

Bevor Sie beginnen

Sie müssen über Windows-Administratorrechte verfügen.

Schritte

1. Melden Sie sich mit dem standardmäßigen lokalen Administratorkonto bei Windows an.
2. Stoppen Sie die Unified Manager-Dienste:

Von der…	Stoppen Sie die Dienste in der folgenden Reihenfolge …
Befehlszeile	a. `sc stop ocie-au` b. `sc stop Oncommandsvc`

Von der…	Stoppen Sie die Dienste in der folgenden Reihenfolge …
Microsoft Service Manager	a. NetApp Active IQ Acquisition Service (Ocie-au) b. NetApp Active IQ Management Server-Dienst (Oncommandsvc)

3. Starten Sie die Unified Manager-Dienste:

Von der…	Starten Sie die Dienste in der folgenden Reihenfolge …
Befehlszeile	a. `sc start Oncommandsvc` b. `sc start ocie-au`
Microsoft Service Manager	a. NetApp Active IQ Management Server-Dienst (Oncommandsvc) b. NetApp Active IQ Acquisition Service (Ocie-au)

Deinstallieren Sie 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 müssen über Windows-Administratorrechte verfügen.
- Alle Cluster (Datenquellen) müssen vom Unified Manager-Server entfernt werden, bevor die Software deinstalliert wird.
- Sie sollten die Firewall-Regeln, die zum Zulassen oder Blockieren des MySQL-Ports 3306 erstellt wurden, manuell löschen. Die Firewall-Regeln werden nicht automatisch gelöscht.

Schritte

1. Deinstallieren Sie Unified Manager, indem Sie eine der folgenden Optionen auswählen:
   - Wenn Sie Unified Manager über den Assistenten **Programme und Funktionen** deinstallieren, führen Sie die folgenden Schritte aus:
     i. Navigieren Sie zu **Systemsteuerung** > **Programme und Funktionen**.
     ii. Wählen Sie Active IQ Unified Manager und klicken Sie auf **Deinstallieren**.
   - Wenn Sie Unified Manager über die Befehlszeile deinstallieren, führen Sie die folgenden Schritte aus:
     i. Melden Sie sich mit Administratorrechten bei der Windows-Befehlszeile an.
     ii. Navigieren Sie zum Active IQ Unified Manager -Verzeichnis und führen Sie den folgenden Befehl aus:

```
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 wird von Ihrem System deinstalliert.

2. Deinstallieren Sie die folgenden Pakete und Daten von Drittanbietern, die bei der Deinstallation von Unified Manager nicht entfernt werden:
   - Pakete von Drittanbietern: JRE, MySQL, Microsoft Visual C 2015 Redistributable, Python und 7zip
   - Von Unified Manager generierte MySQL-Anwendungsdaten
   - Anwendungsprotokolle und Inhalte des Anwendungsdatenverzeichnisses

Durchführen von Konfigurations- und Verwaltungsaufgaben

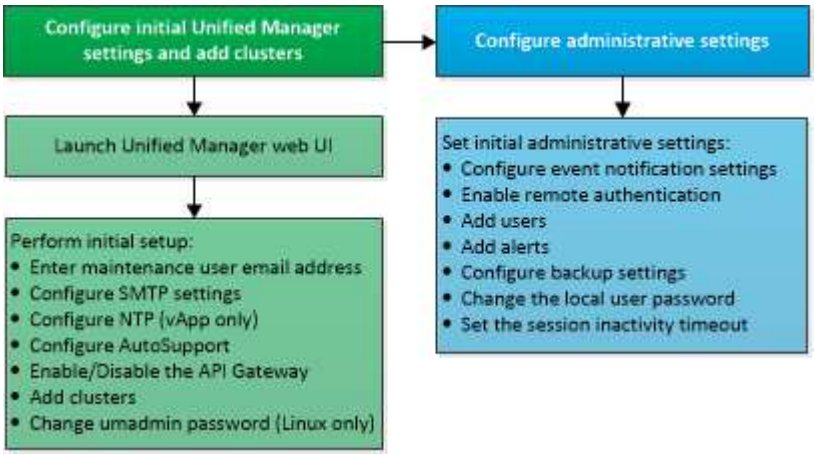
Konfigurieren Sie Active IQ Unified Manager

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-Benutzeroberfläche zuzugreifen. Anschließend können Sie zusätzliche Konfigurationsaufgaben ausführen, z. B. Cluster hinzufügen, Remote-Authentifizierung konfigurieren, Benutzer hinzufügen und Warnungen hinzufügen.

Einige der in diesem Handbuch beschriebenen Verfahren sind erforderlich, um die Ersteinrichtung Ihrer Unified Manager-Instanz abzuschließen. Bei anderen Verfahren handelt es sich um empfohlene Konfigurationseinstellungen, die für die Einrichtung Ihrer neuen Instanz hilfreich sind oder über die Sie Bescheid wissen sollten, bevor Sie mit der regelmäßigen Überwachung Ihrer ONTAP Systeme beginnen.

Übersicht über den Konfigurationsablauf

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



Zugriff auf die Unified Manager-Web-Benutzeroberfläche

Nachdem Sie Unified Manager installiert haben, können Sie auf die Web-Benutzeroberfläche zugreifen, um Unified Manager einzurichten und 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 (oder als Umadmin-Benutzer bei Linux-Installationen) anmelden.
- Wenn Sie Benutzern den Zugriff auf Unified Manager über den Kurznamen statt über den vollqualifizierten Domänennamen (FQDN) oder die 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 akzeptieren, um den Zugriff fortzusetzen, oder ein von einer Zertifizierungsstelle (CA) signiertes digitales Zertifikat zur Serverauthentifizierung installieren.

Schritte

1. Starten Sie die Unified Manager-Web-Benutzeroberfläche von Ihrem Browser aus, indem Sie die URL verwenden, die am Ende der Installation angezeigt wird. Die URL ist die IP-Adresse oder der vollqualifizierte Domänenname (FQDN) des Unified Manager-Servers.

   Der Link hat das folgende Format: `https://URL`.

2. Melden Sie sich mit Ihren Wartungsbenutzeranmeldeinformationen bei der Unified Manager-Web-Benutzeroberfläche an.

Wenn Sie innerhalb einer Stunde drei erfolglose Anmeldeversuche bei der Web-Benutzeroberfläche unternehmen, werden Sie aus dem System ausgesperrt und müssen sich an Ihren Systemadministrator wenden. Dies gilt nur für lokale Benutzer.

Führen Sie die Ersteinrichtung der Unified Manager-Web-Benutzeroberfläche durch

Um Unified Manager zu verwenden, müssen Sie zunächst die anfänglichen Einrichtungsoptionen konfigurieren, einschließlich des NTP-Servers, der E-Mail-Adresse des Wartungsbenutzers, des SMTP-Serverhosts und des Hinzufügens von ONTAP Clustern.

Bevor Sie beginnen

Sie müssen die folgenden Vorgänge ausgeführt haben:

- Die Unified Manager-Web-Benutzeroberfläche wurde über die nach der Installation bereitgestellte URL gestartet.
- Angemeldet mit dem Wartungsbenutzernamen und -kennwort (Umadmin-Benutzer für Linux-Installationen), die während der Installation erstellt wurden

Die Seite „Erste Schritte“ von Active IQ Unified Manager wird nur angezeigt, wenn Sie zum ersten Mal auf die Web-Benutzeroberfläche zugreifen. Die folgende Seite stammt aus einer Installation auf VMware.

Wenn Sie eine dieser Optionen später ändern möchten, können Sie Ihre Auswahl aus den allgemeinen Optionen im linken Navigationsbereich des Unified Managers treffen. Beachten Sie, dass die NTP-Einstellung nur für VMware-Installationen gilt und später über die Wartungskonsole von Unified Manager geändert werden kann.

Schritte

1. Geben Sie auf der Seite „Ersteinrichtung“ von Active IQ Unified Manager die E-Mail-Adresse des Wartungsbenutzers, den Hostnamen des SMTP-Servers und alle zusätzlichen SMTP-Optionen sowie den NTP-Server ein (nur VMware-Installationen). Klicken Sie dann auf **Weiter**.

Wenn Sie die Option **STARTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Weiter** eine Zertifikatsseite angezeigt. Überprüfen Sie die Zertifikatdetails und akzeptieren Sie das Zertifikat, um mit den anfänglichen Einrichtungseinstellungen der Web-Benutzeroberfläche fortzufahren.

2. Klicken Sie auf der AutoSupport -Seite auf **Zustimmen und fortfahren**, um das Senden von AutoSupport -Nachrichten von Unified Manager an NetAppActive IQ zu aktivieren.

   Wenn Sie einen Proxy für den Internetzugang festlegen müssen, um AutoSupport Inhalte zu senden, oder wenn Sie AutoSupport deaktivieren möchten, verwenden Sie die Option **Allgemein** > * AutoSupport* in der Web-Benutzeroberfläche.

3. Ändern Sie auf Red Hat-Systemen das Umadmin-Benutzerkennwort von der Standardzeichenfolge „`admin`“ in eine personalisierte Zeichenfolge.

4. Wählen Sie auf der Seite „API-Gateway einrichten“ aus, ob Sie die API-Gateway-Funktion verwenden möchten, mit der Unified Manager die ONTAP Cluster verwalten kann, die Sie mithilfe von ONTAP REST-APIs überwachen möchten. Klicken Sie dann 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. Fügen Sie die Cluster hinzu, die Unified Manager verwalten soll, und klicken Sie dann auf **Weiter**. Für jeden Cluster, den Sie verwalten möchten, benötigen Sie den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) für die Clusterverwaltung sowie den Benutzernamen und das Kennwort. Der Benutzer muss über die Rolle „admin“ verfügen.

   Dieser Schritt ist optional. Sie können Cluster später in der Web-Benutzeroberfläche unter **Speicherverwaltung** > **Cluster-Setup** hinzufügen.

6. Überprüfen Sie auf der Seite „Zusammenfassung“, ob alle Einstellungen korrekt sind, und klicken Sie auf „Fertig stellen“.

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

Cluster hinzufügen

Sie können Active IQ Unified Manager einen Cluster hinzufügen, damit Sie den Cluster überwachen können. Dazu gehört die Möglichkeit, Clusterinformationen wie Zustand, Kapazität, Leistung und Konfiguration des Clusters abzurufen, sodass Sie eventuell auftretende Probleme finden und beheben können.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen über die folgenden Informationen verfügen:
  - Unified Manager unterstützt lokale ONTAP -Cluster, ONTAP Select und Cloud Volumes ONTAP.
  - Hostname oder IP-Adresse zur Clusterverwaltung

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

    Die Cluster-Management-IP-Adresse muss die Cluster-Management-LIF der administrativen Storage Virtual Machine (SVM) sein. Wenn Sie ein Knotenverwaltungs-LIF verwenden, schlägt der Vorgang fehl.

  - Auf dem Cluster muss die ONTAP Softwareversion 9.1 oder höher ausgeführt werden.

- ONTAP -Administratorbenutzername und -kennwort

  Dieses Konto muss über die Rolle *admin* verfügen und der Anwendungszugriff muss auf *ontapi*, *console* und *http* eingestellt sein.

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

  SSL (HTTPS)-Zertifikat: Dieses Zertifikat ist Eigentum von Unified Manager. Bei einer Neuinstallation von Unified Manager wird ein standardmäßiges selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt, zur besseren Sicherheit ein Upgrade auf ein CA-signiertes Zertifikat durchzuführen. Wenn das Serverzertifikat abläuft, sollten Sie es neu generieren und Unified Manager neu starten, damit die Dienste das neue Zertifikat integrieren. Weitere Informationen zum Neugenerieren von SSL-Zertifikaten finden Sie unter"Generieren eines HTTPS-Sicherheitszertifikats" .

  EMS-Zertifikat: Dieses Zertifikat ist Eigentum von Unified Manager. Es wird während der Authentifizierung für von ONTAP empfangene EMS-Benachrichtigungen verwendet.

  Zertifikate für gegenseitige TLS-Kommunikation: Wird während der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatsbasierte Authentifizierung ist für einen Cluster basierend auf der ONTAP -Version aktiviert. Wenn auf dem Cluster eine niedrigere ONTAP Version als 9.5 ausgeführt wird, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

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

  - Sie können einen Cluster über die Web-Benutzeroberfläche hinzufügen und die zertifikatbasierte Authentifizierung wird automatisch aktiviert.
  - Sie können einen Cluster über die Unified Manager CLI hinzufügen. Die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie einen Cluster mithilfe der Unified Manager-CLI hinzufügen, müssen Sie den Cluster mithilfe der Unified Manager-Benutzeroberfläche bearbeiten. Sie können sehen"Unterstützte Unified Manager CLI-Befehle" um einen Cluster mithilfe der Unified Manager CLI hinzuzufügen.
  - Wenn die zertifikatbasierte Authentifizierung für einen Cluster aktiviert ist und Sie die Sicherung von Unified Manager von einem Server nehmen und auf einem anderen Unified Manager-Server wiederherstellen, auf dem der Hostname oder die IP-Adresse geändert wurde, kann die Überwachung des Clusters fehlschlagen. Um den Fehler zu vermeiden, bearbeiten und speichern Sie die Clusterdetails. Weitere Informationen zum Bearbeiten von Clusterdetails finden Sie unter"Cluster bearbeiten" .

+
Cluster-Zertifikate: Dieses Zertifikat ist Eigentum von ONTAP. Sie können Unified Manager keinen Cluster mit einem abgelaufenen Zertifikat hinzufügen. Wenn das Zertifikat bereits abgelaufen ist, sollten Sie es vor dem Hinzufügen des Clusters neu generieren. Informationen zur Zertifikatsgenerierung finden Sie im Knowledge Base-Artikel (KB). "So erneuern Sie ein selbstsigniertes ONTAP -Zertifikat in der System Manager-Benutzeroberfläche" .

- Sie müssen über ausreichend Speicherplatz auf dem Unified Manager-Server verfügen. Sie können dem Server keinen Cluster hinzufügen, wenn bereits mehr als 90 % des Speicherplatzes im Datenbankverzeichnis belegt sind.

Für eine MetroCluster -Konfiguration müssen Sie sowohl die lokalen als auch die Remote-Cluster hinzufügen und die Cluster müssen korrekt konfiguriert sein.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.
2. Klicken Sie auf der Seite „Cluster-Setup“ auf **Hinzufügen**.
3. Geben Sie im Dialogfeld „Cluster hinzufügen“ die erforderlichen Werte an, z. B. den Hostnamen oder die IP-Adresse des Clusters, den Benutzernamen, das Kennwort und die Portnummer.

   Sie können die IP-Adresse der Clusterverwaltung von IPv6 auf IPv4 oder von IPv4 auf IPv6 ändern. Die neue IP-Adresse wird nach Abschluss des nächsten Überwachungszyklus im Clusterraster und auf der Clusterkonfigurationsseite angezeigt.

4. Klicken Sie auf **Senden**.
5. Klicken Sie im Dialogfeld „Host autorisieren“ auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
6. Klicken Sie auf **Ja**.

   Nachdem Sie die Clusterdetails gespeichert haben, können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für einen Cluster sehen.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, überprüft Unified Manager das Zertifikat nur, wenn der Cluster zum ersten Mal hinzugefügt wird. Unified Manager überprüft 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 Leistungsdaten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Datenkontinuitätserfassung erfasst. Mit dieser Funktion erhalten Sie unmittelbar nach dem Hinzufügen eines Clusters Leistungsinformationen für mehr als zwei Wochen. Nachdem der Datenkontinuitätserfassungszyklus abgeschlossen ist, werden standardmäßig alle fünf Minuten Echtzeitdaten zur Clusterleistung erfasst.

Da die Erfassung von 15 Tagen Leistungsdaten CPU-intensiv ist, wird empfohlen, das Hinzufügen neuer Cluster zu staffeln, damit Abfragen zur Datenkontinuitätserfassung nicht auf zu vielen Clustern gleichzeitig ausgeführt werden. Wenn Sie Unified Manager während des Datenkontinuitätserfassungszeitraums neu starten, wird die Erfassung angehalten und Sie sehen Lücken in den Leistungsdiagrammen für den fehlenden Zeitraum.

Wenn Sie eine Fehlermeldung erhalten, dass Sie den Cluster nicht hinzufügen können, überprüfen Sie, ob die Uhren auf den beiden Systemen nicht synchronisiert sind und das Startdatum des Unified Manager-HTTPS-Zertifikats nach dem Datum auf dem Cluster liegt. Sie müssen sicherstellen, dass die Uhren über NTP oder einen ähnlichen Dienst synchronisiert werden.

Verwandte Informationen

"Installieren eines von einer Zertifizierungsstelle signierten und zurückgegebenen HTTPS-Zertifikats"

Konfigurieren Sie Unified Manager zum Senden von Warnbenachrichtigungen

Sie können Unified Manager so konfigurieren, dass Benachrichtigungen gesendet werden, die Sie über Ereignisse in Ihrer Umgebung informieren. Bevor Benachrichtigungen gesendet werden können, müssen Sie mehrere andere Unified Manager-Optionen konfigurieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Nachdem Sie Unified Manager bereitgestellt und die Erstkonfiguration abgeschlossen haben, sollten Sie Ihre Umgebung so konfigurieren, dass basierend auf dem Empfang von Ereignissen Warnungen ausgelöst und Benachrichtigungs-E-Mails oder SNMP-Traps generiert werden.

Schritte

1. "Konfigurieren der Ereignisbenachrichtigungseinstellungen".

   Wenn Sie beim Auftreten bestimmter Ereignisse in Ihrer Umgebung Warnbenachrichtigungen erhalten möchten, müssen Sie einen SMTP-Server konfigurieren und eine E-Mail-Adresse angeben, von der die Warnbenachrichtigung gesendet wird. Wenn Sie SNMP-Traps verwenden möchten, können Sie diese Option auswählen und die erforderlichen Informationen angeben.

2. "Remote-Authentifizierung aktivieren".

   Wenn Remote-LDAP- oder Active Directory-Benutzer auf die Unified Manager-Instanz zugreifen und Warnbenachrichtigungen erhalten sollen, müssen Sie die Remote-Authentifizierung aktivieren.

3. "Authentifizierungsserver hinzufügen".

   Sie können Authentifizierungsserver hinzufügen, sodass Remotebenutzer innerhalb des Authentifizierungsservers auf Unified Manager zugreifen können.

4. "Benutzer hinzufügen".

   Sie können verschiedene Arten von lokalen oder Remote-Benutzern hinzufügen und bestimmte Rollen zuweisen. Wenn Sie eine Warnung erstellen, weisen Sie einen Benutzer zu, der die Warnbenachrichtigungen erhalten soll.

5. "Benachrichtigungen hinzufügen".

   Nachdem Sie die E-Mail-Adresse zum Senden 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.

Konfigurieren der Ereignisbenachrichtigungseinstellungen

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

Bevor Sie beginnen

Sie müssen über die folgenden Informationen verfügen:

- E-Mail-Adresse, von der die Warnmeldung gesendet wird

  Die E-Mail-Adresse wird in gesendeten Warnbenachrichtigungen im Feld „Von“ angezeigt. Sollte die E-Mail aus irgendeinem Grund nicht zugestellt werden können, wird diese E-Mail-Adresse auch als Empfänger für unzustellbare E-Mails verwendet.

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

  Um mehrere Trap-Ziele anzugeben, trennen Sie jeden Host durch ein Komma. In diesem Fall müssen alle anderen SNMP-Einstellungen, wie z. B. Version und ausgehender Trap-Port, für alle Hosts in der Liste gleich sein.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benachrichtigungen**.
2. Konfigurieren Sie auf der Seite „Benachrichtigungen“ die entsprechenden Einstellungen.

   Anmerkungen:

   - Wenn die Absenderadresse bereits mit der Adresse „ActiveIQUnifiedManager@localhost.com“ ausgefüllt ist, sollten Sie sie in eine echte, funktionierende E-Mail-Adresse ändern, um sicherzustellen, dass alle E-Mail-Benachrichtigungen erfolgreich zugestellt werden.
   - Wenn der Hostname des SMTP-Servers nicht aufgelöst werden kann, können Sie anstelle des Hostnamens die IP-Adresse (IPv4 oder IPv6) des SMTP-Servers angeben.
3. Klicken Sie auf **Speichern**.
4. Wenn Sie die Option **STARTLS verwenden** oder **SSL verwenden** ausgewählt haben, wird nach dem Klicken auf die Schaltfläche **Speichern** eine Zertifikatsseite angezeigt. Überprüfen Sie die Zertifikatsdetails und akzeptieren Sie das Zertifikat, um die Benachrichtigungseinstellungen zu speichern.

   Sie können auf die Schaltfläche **Zertifikatdetails anzeigen** klicken, um die Zertifikatsdetails anzuzeigen. Wenn das vorhandene Zertifikat abgelaufen ist, deaktivieren Sie das Kontrollkästchen **STARTLS verwenden** oder **SSL verwenden**, speichern Sie die Benachrichtigungseinstellungen und aktivieren Sie das Kontrollkästchen **STARTLS verwenden** oder **SSL verwenden** erneut, um ein neues Zertifikat anzuzeigen.

Remote-Authentifizierung aktivieren

Sie können die Remote-Authentifizierung aktivieren, damit der Unified Manager-Server mit Ihren Authentifizierungsservern kommunizieren kann. Die Benutzer des Authentifizierungsservers können auf die grafische Benutzeroberfläche des Unified Managers zugreifen, um Speicherobjekte und Daten zu verwalten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

> 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 mit 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 389 als Standardport für nicht sichere Kommunikation und 636 als Standardport für sichere Kommunikation.

> Das zur Authentifizierung der Benutzer verwendete Zertifikat muss dem X.509-Format entsprechen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Aktivieren Sie das Kontrollkästchen **Remote-Authentifizierung aktivieren…**.
3. Wählen Sie im Feld „Authentifizierungsdienst“ den Diensttyp aus und konfigurieren Sie den Authentifizierungsdienst.

Für den Authentifizierungstyp …	Geben Sie die folgenden Informationen ein …
Active Directory	• Name des Authentifizierungsserver-Administrators in einem der folgenden Formate: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name`(unter Verwendung der entsprechenden LDAP-Notation) • Administratorkennwort • Basis-Distinguished Name (unter Verwendung der entsprechenden LDAP-Notation)
Öffnen Sie LDAP	• Bind-Distinguished Name (in der entsprechenden LDAP-Notation) • Bind-Passwort • Basis-Distinguished Name

Wenn die Authentifizierung eines Active Directory-Benutzers lange dauert oder ein Timeout auftritt, liegt das wahrscheinlich daran, dass der Authentifizierungsserver lange braucht, um zu antworten. Das Deaktivieren der Unterstützung für verschachtelte Gruppen in Unified Manager kann die Authentifizierungszeit verkürzen.

Wenn Sie die Option „Sichere Verbindung verwenden“ für den Authentifizierungsserver auswählen, kommuniziert Unified Manager mit dem Authentifizierungsserver über das Secure Sockets Layer (SSL)-Protokoll.

4. **Optional:** Fügen Sie Authentifizierungsserver hinzu und testen Sie die Authentifizierung.
5. Klicken Sie auf **Speichern**.

Deaktivieren Sie verschachtelte Gruppen von der Remote-Authentifizierung

Wenn Sie die Remote-Authentifizierung aktiviert haben, können Sie die verschachtelte Gruppenauthentifizierung deaktivieren, sodass sich nur einzelne Benutzer und keine Gruppenmitglieder remote bei Unified Manager authentifizieren können. Sie können verschachtelte Gruppen deaktivieren, wenn Sie die Antwortzeit der Active Directory-Authentifizierung verbessern möchten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.
- Das Deaktivieren verschachtelter Gruppen ist nur bei Verwendung von Active Directory möglich.

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Aktivieren Sie das Kontrollkästchen **Verschachtelte Gruppensuche deaktivieren**.
3. Klicken Sie auf **Speichern**.

Einrichten von Authentifizierungsdiensten

Authentifizierungsdienste ermöglichen die Authentifizierung von Remote-Benutzern oder Remote-Gruppen in einem Authentifizierungsserver, bevor ihnen Zugriff auf Unified Manager gewährt wird. Sie können Benutzer authentifizieren, indem Sie vordefinierte Authentifizierungsdienste (wie Active Directory oder OpenLDAP) verwenden oder Ihren eigenen Authentifizierungsmechanismus konfigurieren.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert haben.
- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Wählen Sie einen der folgenden Authentifizierungsdienste aus:

Wenn Sie auswählen…	Dann tun Sie Folgendes …
Active Directory	a. Geben Sie den Administratornamen und das Kennwort ein. b. Geben Sie den Basis-Distinguished Name des Authentifizierungsservers an. Wenn der Domänenname des Authentifizierungsservers beispielsweise ou@domain.com lautet, dann ist der Basis-Distinguished Name **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Geben Sie den definierten Bind-Namen und das Bind-Passwort ein. b. Geben Sie den Basis-Distinguished Name des Authentifizierungsservers an. Wenn der Domänenname des Authentifizierungsservers beispielsweise ou@domain.com lautet, dann ist der Basis-Distinguished Name **cn=ou,dc=domain,dc=com**.
Sonstige	a. Geben Sie den definierten Bind-Namen und das Bind-Passwort ein. b. Geben Sie den Basis-Distinguished Name des Authentifizierungsservers an. Wenn der Domänenname des Authentifizierungsservers beispielsweise ou@domain.com lautet, dann ist der Basis-Distinguished Name **cn=ou,dc=domain,dc=com**. c. Geben Sie die LDAP-Protokollversion an, die vom Authentifizierungsserver unterstützt wird. d. Geben Sie den Benutzernamen, die Gruppenmitgliedschaft, die Benutzergruppe und die Mitgliedsattribute ein.

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

3. Klicken Sie auf **Speichern**.

Authentifizierungsserver hinzufügen

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 vorliegen:
  - Hostname oder IP-Adresse des Authentifizierungsservers
  - Portnummer des Authentifizierungsservers
- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst konfiguriert haben, damit der Verwaltungsserver Remote-Benutzer oder -Gruppen im Authentifizierungsserver authentifizieren kann.
- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Wenn der Authentifizierungsserver, den Sie hinzufügen, Teil eines Hochverfügbarkeitspaars (HA) ist (das dieselbe Datenbank verwendet), können Sie auch den Partnerauthentifizierungsserver hinzufügen. Dadurch kann der Verwaltungsserver mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Aktivieren oder deaktivieren Sie die Option **Sichere Verbindung verwenden**:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Aktivieren Sie es	a. Wählen Sie die Option **Sichere Verbindung verwenden**. b. Klicken Sie im Bereich „Authentifizierungsserver“ auf **Hinzufügen**. c. Geben Sie im Dialogfeld „Authentifizierungsserver hinzufügen“ den Authentifizierungsnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers ein. d. Klicken Sie im Dialogfeld „Host autorisieren“ auf „Zertifikat anzeigen“. e. Überprüfen Sie im Dialogfeld „Zertifikat anzeigen“ die Zertifikatsinformationen und klicken Sie dann auf **Schließen**. f. Klicken Sie im Dialogfeld „Host autorisieren“ auf **Ja**. Wenn Sie die Option **Authentifizierung für sichere Verbindung verwenden** aktivieren, kommuniziert Unified Manager mit dem Authentifizierungsserver und zeigt das Zertifikat an. Unified Manager verwendet 636 als Standardport für sichere Kommunikation und Portnummer 389 für nicht sichere Kommunikation.
Deaktivieren Sie es	a. Deaktivieren Sie die Option **Sichere Verbindung verwenden**. b. Klicken Sie im Bereich „Authentifizierungsserver“ auf **Hinzufügen**. c. Geben Sie im Dialogfeld „Authentifizierungsserver hinzufügen“ entweder den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) des Servers sowie die Portdetails an. d. Klicken Sie auf **Hinzufügen**.

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

3. Führen Sie eine Testauthentifizierung durch, um zu bestätigen, dass Sie Benutzer auf dem von Ihnen hinzugefügten Authentifizierungsserver authentifizieren können.

Testen Sie die Konfiguration der Authentifizierungsserver

Sie können die Konfiguration Ihrer Authentifizierungsserver validieren, um sicherzustellen, dass der Verwaltungsserver mit ihnen kommunizieren kann. Sie können die Konfiguration validieren, indem Sie auf Ihren Authentifizierungsservern nach einem Remotebenutzer oder einer Remotegruppe suchen und diese mithilfe der konfigurierten Einstellungen authentifizieren.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsdienst konfiguriert haben, damit der Unified Manager-Server den Remote-Benutzer oder die Remote-Gruppe authentifizieren kann.
- Sie müssen Ihre Authentifizierungsserver hinzugefügt haben, damit der Verwaltungsserver von diesen Servern aus nach dem Remotebenutzer oder der Remotegruppe suchen und sie authentifizieren kann.
- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Wenn der Authentifizierungsdienst auf Active Directory eingestellt ist und Sie die Authentifizierung von Remotebenutzern validieren, die zur primären Gruppe des Authentifizierungsservers gehören, werden in den Authentifizierungsergebnissen keine Informationen zur primären Gruppe angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Klicken Sie auf **Authentifizierung testen**.
3. Geben Sie im Dialogfeld „Testbenutzer“ den Benutzernamen und das Kennwort des Remotebenutzers oder den Benutzernamen der Remotegruppe an und klicken Sie dann auf **Test**.

   Wenn Sie eine Remote-Gruppe authentifizieren, dürfen Sie das Kennwort nicht eingeben.

Benachrichtigungen hinzufügen

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

Bevor Sie beginnen

- Sie müssen Benachrichtigungseinstellungen wie die E-Mail-Adresse des Benutzers, den SMTP-Server und den SNMP-Trap-Host konfiguriert haben, damit der Active IQ Unified Manager Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Warnung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie möchten, dass basierend auf dem Ereignis ein Skript ausgeführt wird, müssen Sie das Skript über die Seite „Skripte“ zu Unified Manager hinzugefügt haben.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können nach dem Empfang eines Ereignisses direkt auf der Seite „Ereignisdetails“ eine Warnung erstellen. Außerdem können Sie eine Warnung auch auf der Seite „Warnungseinrichtung“ erstellen, wie hier beschrieben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
2. Klicken Sie auf der Seite „Alarm-Setup“ auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld „Warnung hinzufügen“ auf **Name** und geben Sie einen Namen und eine Beschreibung für die Warnung ein.
4. Klicken Sie auf **Ressourcen** und wählen Sie die Ressourcen aus, die in die Warnung einbezogen oder davon ausgeschlossen werden sollen.

   Sie können einen Filter festlegen, indem Sie im Feld **Name enthält** eine Textzeichenfolge angeben, um eine Gruppe von Ressourcen auszuwählen. Basierend auf der von Ihnen angegebenen Textzeichenfolge zeigt die Liste der verfügbaren Ressourcen nur die Ressourcen an, die der Filterregel entsprechen. Bei der von Ihnen angegebenen Textzeichenfolge wird zwischen Groß- und Kleinschreibung unterschieden.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschluss- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschlussregel und für Ereignisse im Zusammenhang mit der ausgeschlossenen Ressource wird keine Warnung generiert.

5. Klicken Sie auf **Ereignisse** und wählen Sie basierend auf dem Ereignisnamen oder dem Schweregradtyp die Ereignisse aus, für die Sie eine Warnung auslösen möchten.

   Um mehr als ein Ereignis auszuwählen, drücken Sie die Strg-Taste, während Sie Ihre Auswahl treffen.

6. Klicken Sie auf **Aktionen** und wählen Sie die Benutzer aus, die Sie benachrichtigen möchten, wählen Sie die Benachrichtigungshäufigkeit, wählen Sie, ob ein SNMP-Trap an den Trap-Empfänger gesendet werden soll, und weisen Sie ein Skript zu, das ausgeführt werden soll, wenn eine Warnung generiert wird.

   Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnung zur Bearbeitung erneut öffnen, wird das Feld „Name“ leer angezeigt, da die geänderte E-Mail-Adresse nicht mehr dem zuvor ausgewählten Benutzer zugeordnet ist. 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.

   Sie können Benutzer auch über SNMP-Traps benachrichtigen.

7. Klicken Sie auf **Speichern**.

Beispiel für das Hinzufügen einer Warnung

Dieses Beispiel zeigt, wie Sie eine Warnung erstellen, die die folgenden Anforderungen erfüllt:

- Warnungsname: HealthTest
- Ressourcen: schließt alle Volumes ein, 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

Führen Sie im Dialogfeld „Warnung hinzufügen“ die folgenden Schritte aus:

Schritte

1. Klicken Sie auf **Name** und geben Sie **HealthTest** in das Feld **Alert Name** ein.
2. Klicken Sie auf **Ressourcen** und wählen Sie auf der Registerkarte „Einschließen“ aus der Dropdownliste **Volumes** aus.
   a. Geben Sie **abc** in das Feld **Name enthält** ein, um die Volumes anzuzeigen, deren Name „`abc`“ enthält.
   b. Wählen Sie **+[All Volumes whose name contains 'abc']** + aus dem Bereich „Verfügbare Ressourcen“ und verschieben Sie es in den Bereich „Ausgewählte Ressourcen“.
   c. Klicken Sie auf **Ausschließen**, geben Sie **xyz** in das Feld **Name enthält** ein und klicken Sie dann auf **Hinzufügen**.
3. Klicken Sie auf **Ereignisse** und wählen Sie im Feld „Ereignisschweregrad“ die Option **Kritisch** aus.
4. Wählen Sie im Bereich „Übereinstimmende Ereignisse“ die Option „Alle kritischen Ereignisse“ aus und verschieben Sie sie in den Bereich „Ausgewählte Ereignisse“.
5. Klicken Sie auf **Aktionen** und geben Sie **sample@domain.com** in das Feld „Diese Benutzer benachrichtigen“ ein.
6. Wählen Sie **Alle 15 Minuten erinnern**, um den Benutzer alle 15 Minuten zu benachrichtigen.

   Sie können einen Alarm so konfigurieren, dass den Empfängern für einen bestimmten Zeitraum wiederholt Benachrichtigungen gesendet werden. Sie sollten den Zeitpunkt ermitteln, ab dem die Ereignisbenachrichtigung für den Alarm aktiv ist.
7. Wählen Sie im Menü „Auszuführendes Skript auswählen“ die Option „Skript **Test**“ aus.
8. Klicken Sie auf **Speichern**.

Ändern des lokalen Benutzerkennworts

Sie können Ihr lokales Benutzeranmeldekennwort 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. Um das Kennwort eines Remote-Benutzers zu ändern, wenden Sie sich an Ihren Kennwortadministrator. Informationen zum Ändern des Wartungsbenutzerkennworts finden Sie unter"Verwenden der Wartungskonsole" .

Schritte

1. Melden Sie sich bei Unified Manager an.
2. Klicken Sie in der oberen Menüleiste auf das Benutzersymbol und dann auf **Passwort ändern**.

   Die Option **Passwort ändern** wird nicht angezeigt, wenn Sie ein Remote-Benutzer sind.
3. Geben Sie im Dialogfeld „Passwort ändern“ das aktuelle und das neue Passwort ein.
4. Klicken Sie auf **Speichern**.

Wenn Unified Manager in einer Hochverfügbarkeitskonfiguration konfiguriert ist, müssen Sie das Kennwort auf dem zweiten Knoten des Setups ändern. Beide Instanzen müssen dasselbe Passwort haben.

Festlegen des Sitzungs-Inaktivitäts-Timeouts

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

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Diese Einstellung wirkt sich auf alle angemeldeten Benutzersitzungen aus.

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Geben Sie auf der Seite **Funktionseinstellungen** das Inaktivitäts-Timeout an, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Legen Sie kein Timeout fest, sodass die Sitzung nie automatisch geschlossen wird	Bewegen Sie im Bereich **Inaktivitäts-Timeout** den Schieberegler nach links (Aus) und klicken Sie auf **Übernehmen**.
Legen Sie eine bestimmte Anzahl von Minuten als Timeout-Wert fest	Bewegen Sie im Bereich **Inaktivitäts-Timeout** den Schieberegler nach rechts (Ein), geben Sie den Wert für das Inaktivitäts-Timeout in Minuten an und klicken Sie auf **Übernehmen**.

Legen Sie das Sitzungs-Timeout über die CLI fest

Sie können mithilfe der CLI einen maximalen Sitzungs-Timeout-Wert für Unified Manager festlegen, sodass die Sitzung nach einer bestimmten Zeit automatisch beendet wird. Standardmäßig ist Ihr Sitzungs-Timeout auf den Maximalwert von 4.320 Minuten (72 Stunden) eingestellt. Dies bedeutet, dass Ihre Sitzung nach 72 Stunden automatisch endet, auch wenn Sie angemeldet sind und Unified Manager aktiv verwenden.

Informationen zu diesem Vorgang

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Die Einstellung für das Sitzungs-Timeout wirkt sich auf alle angemeldeten Benutzersitzungen aus.

Schritte

1. Melden Sie sich bei der Unified Manager CLI an, indem Sie den `um cli login` Befehl. Verwenden Sie zur Authentifizierung einen gültigen Benutzernamen und ein gültiges Passwort.
2. Geben Sie den `um option set max.session.timeout.value=<in mins>` Befehl zum Ändern des Sitzungs-Timeout-Werts.

Ändern des Unified Manager-Hostnamens

Irgendwann möchten Sie möglicherweise den Hostnamen des Systems ändern, auf dem Sie Unified Manager installiert haben. Beispielsweise möchten Sie den Host möglicherweise umbenennen, um Ihre Unified Manager-Server einfacher nach Typ, Arbeitsgruppe oder überwachter Clustergruppe zu identifizieren.

Die zum Ändern des Hostnamens 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.

Ändern des Hostnamens der virtuellen Unified Manager-Appliance

Dem Netzwerkhost wird bei der ersten Bereitstellung der virtuellen Unified Manager-Appliance ein Name zugewiesen. Sie können den Hostnamen nach der Bereitstellung 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 die Rolle des Anwendungsadministrators zugewiesen sein.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Unified Manager-Web-Benutzeroberfläche zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie einen Namen für den Netzwerkhost festgelegt. Wenn Sie das Netzwerk mit DHCP konfiguriert haben, sollte der Hostname aus dem DNS übernommen werden. Wenn DHCP oder DNS nicht richtig konfiguriert sind, wird der Hostname „Unified Manager“ automatisch zugewiesen und mit dem Sicherheitszertifikat verknüpft.

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

Wenn Sie auf die Web-Benutzeroberfläche zugreifen, indem Sie die IP-Adresse des Servers anstelle des Hostnamens verwenden, 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 wird erst wirksam, wenn die virtuelle Unified Manager-Maschine neu gestartet wird.

Schritte

1. Generieren Sie ein HTTPS-Sicherheitszertifikat

   Wenn Sie den neuen Hostnamen für den Zugriff auf die Unified Manager-Web-Benutzeroberfläche verwenden möchten, müssen Sie das HTTPS-Zertifikat neu generieren, um es mit dem neuen Hostnamen zu verknüpfen.

2. Starten Sie die virtuelle Unified Manager-Maschine neu

   Nachdem Sie das HTTPS-Zertifikat neu generiert haben, müssen Sie die virtuelle Unified Manager-

Maschine neu starten.

Generieren Sie ein HTTPS-Sicherheitszertifikat

Bei der ersten Installation von Active IQ Unified Manager wird ein Standard-HTTPS-Zertifikat installiert. Sie können ein neues HTTPS-Sicherheitszertifikat generieren, das das vorhandene Zertifikat ersetzt.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Es kann mehrere Gründe geben, das Zertifikat neu zu generieren, beispielsweise wenn Sie bessere Werte für den Distinguished Name (DN) wünschen, eine höhere Schlüsselgröße oder eine längere Ablaufdauer wünschen oder wenn das aktuelle Zertifikat abgelaufen ist.

Wenn Sie keinen Zugriff auf die Unified Manager-Web-Benutzeroberfläche haben, können Sie das HTTPS-Zertifikat mithilfe der Wartungskonsole mit denselben Werten neu generieren. Beim Neugenerieren von Zertifikaten können Sie die Schlüsselgröße und die Gültigkeitsdauer des Schlüssels festlegen. Wenn Sie die `Reset Server Certificate` Option aus der Wartungskonsole, dann wird ein neues HTTPS-Zertifikat erstellt, das 397 Tage gültig ist. Dieses Zertifikat verfügt über einen RSA-Schlüssel mit einer Größe von 2048 Bit.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikat neu generieren**.

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

3. Wählen Sie eine der folgenden Optionen, je nachdem, wie Sie das Zertifikat generieren möchten:

Wenn Sie wollen…	Machen Sie Folgendes…
Zertifikat mit den aktuellen Werten neu generieren	Klicken Sie auf die Option **Mit aktuellen Zertifikatattributen neu generieren**.

Wenn Sie wollen…	Machen Sie Folgendes…
Generieren Sie das Zertifikat mit unterschiedlichen Werten	Klicken Sie auf die Option **Aktuelle Zertifikatattribute aktualisieren**. Wenn Sie keine neuen Werte eingeben, werden in den Feldern „Allgemeiner Name“ und „Alternative Namen“ die Werte aus dem vorhandenen Zertifikat verwendet. Der „Common Name“ sollte auf den FQDN des Hosts eingestellt werden. Für die anderen Felder sind keine Werte erforderlich, Sie können jedoch beispielsweise Werte für E-MAIL, FIRMA, ABTEILUNG, Stadt, Bundesland und Land eingeben, wenn diese Werte im Zertifikat eingetragen werden sollen. Sie können auch aus der verfügbaren SCHLÜSSELGRÖSSE (der Schlüsselalgorithmus ist „RSA“) und der GÜLTIGKEITSDAUER auswählen.

4. Klicken Sie auf **Ja**, um das Zertifikat neu zu generieren.
5. Starten Sie den Unified Manager-Server neu, damit das neue Zertifikat wirksam wird.
6. Überprüfen Sie die neuen Zertifikatsinformationen, indem Sie das HTTPS-Zertifikat anzeigen.

Starten Sie die virtuelle Unified Manager-Maschine neu

Sie können die virtuelle Maschine über die Wartungskonsole von Unified Manager neu starten. Nach der Generierung eines neuen Sicherheitszertifikats oder bei einem Problem mit der virtuellen Maschine ist ein Neustart erforderlich.

Bevor Sie beginnen

Die virtuelle Appliance ist eingeschaltet.

Sie sind als Wartungsbenutzer bei der Wartungskonsole angemeldet.

Sie können die virtuelle Maschine auch von vSphere aus neu starten, indem Sie die Option **Gast neu starten** verwenden. Weitere Informationen finden Sie in der VMware-Dokumentation.

Schritte

1. Greifen Sie auf die Wartungskonsole zu.
2. Wählen Sie **Systemkonfiguration** > **Virtuelle Maschine neu starten**.

Ändern des Unified Manager-Hostnamens auf Linux-Systemen

Irgendwann möchten Sie möglicherweise den Hostnamen der Red Hat Enterprise Linux-Maschine ändern, auf der Sie Unified Manager installiert haben. Beispielsweise möchten Sie möglicherweise den Host umbenennen, um Ihre Unified Manager-Server beim Auflisten Ihrer Linux-Computer einfacher nach Typ, Arbeitsgruppe oder überwachter Clustergruppe zu identifizieren.

Bevor Sie beginnen

Sie müssen über Root-Benutzerzugriff auf das Linux-System verfügen, auf dem Unified Manager installiert ist.

Sie können den Hostnamen (oder die Host-IP-Adresse) verwenden, um auf die Unified Manager-Web-Benutzeroberfläche zuzugreifen. Wenn Sie während der Bereitstellung eine statische IP-Adresse für Ihr Netzwerk konfiguriert haben, haben Sie einen Namen für den Netzwerkhost festgelegt. 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 den neuen Hostnamen für den Zugriff auf die Unified Manager-Web-Benutzeroberfläche verwenden möchten.

Wenn Sie auf die Web-Benutzeroberfläche zugreifen, indem Sie die IP-Adresse des Servers anstelle des Hostnamens verwenden, 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. Das neue Zertifikat wird erst nach einem Neustart der Linux-Maschine 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

- Die zulässigen Werte für die Schlüsselgröße sind `2048`, `3072` Und `4096`.
- Die Gültigkeitsdauer beträgt mindestens 1 Tag und höchstens 36500 Tage.

  Obwohl eine Gültigkeitsdauer von 36.500 Tagen zulässig ist, wird empfohlen, eine Gültigkeitsdauer von nicht mehr als 397 Tagen oder 13 Monaten zu verwenden. Denn wenn Sie eine Gültigkeitsdauer von mehr als 397 Tagen auswählen und planen, eine CSR für dieses Zertifikat zu exportieren und von einer bekannten Zertifizierungsstelle signieren zu lassen, wird die Gültigkeit des signierten Zertifikats, das Ihnen von der Zertifizierungsstelle zurückgegeben wird, auf 397 Tage reduziert.
- Sie können das Kontrollkästchen „Lokale Identifizierungsinformationen ausschließen (z. B. localhost)“ aktivieren, wenn Sie die lokalen Identifizierungsinformationen aus dem Feld „Alternative Namen“ im Zertifikat entfernen möchten. Wenn dieses Kontrollkästchen aktiviert ist, wird nur das von Ihnen eingegebene Feld „Alternative Namen“ verwendet. Wenn dieses Feld leer gelassen wird, enthält das resultierende Zertifikat überhaupt kein Feld für alternative Namen.

1. Melden Sie sich als Root-Benutzer beim Unified Manager-System an, das Sie ändern möchten.
2. Stoppen Sie die Unified Manager-Software und die zugehörige MySQL-Software, indem Sie den folgenden Befehl eingeben:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Ändern Sie den Hostnamen mit dem Linux `hostnamectl` Befehl:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Generieren Sie das HTTPS-Zertifikat für den Server neu:

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

5. Starten Sie den Netzwerkdienst neu:

   ```
   systemctl restart NetworkManager.service
   ```

6. Überprüfen Sie nach dem Neustart des Dienstes, ob der neue Hostname in der Lage ist, sich selbst anzupingen:

   ```
   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, starten Sie Unified Manager neu, indem Sie den folgenden Befehl eingeben:

   ```
   systemctl start mysqld ocie ocieau
   ```

Aktivieren und Deaktivieren der richtlinienbasierten Speicherverwaltung

Ab Unified Manager 9.7 können Sie Speicher-Workloads (Volumes und LUNs) auf Ihren ONTAP Clustern bereitstellen und diese Workloads basierend auf zugewiesenen Leistungsserviceleveln verwalten. Diese Funktionalität ähnelt dem Erstellen von Workloads im ONTAP System Manager und dem Anhängen von QoS-Richtlinien. Bei Anwendung mit Unified Manager können Sie jedoch Workloads über alle Cluster hinweg bereitstellen und verwalten, die Ihre Unified Manager-Instanz überwacht.

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Diese Option ist standardmäßig aktiviert, Sie können sie jedoch deaktivieren, wenn Sie Workloads nicht mit Unified Manager bereitstellen und verwalten möchten.

Wenn diese Option aktiviert ist, werden in der Benutzeroberfläche viele neue Elemente bereitgestellt:

Neue Inhalte	Standort
Eine Seite zum Bereitstellen neuer Workloads	Verfügbar unter **Allgemeine Aufgaben** > **Bereitstellung**
Eine Seite zum Erstellen von Richtlinien für Leistungsservicelevel	Verfügbar unter **Einstellungen** > **Richtlinien** > **Leistungs-Servicelevel**
Eine Seite zum Erstellen von Richtlinien zur Leistungsspeichereffizienz	Verfügbar unter **Einstellungen** > **Richtlinien** > **Speichereffizienz**
Panels, die Ihre aktuelle Workload-Leistung und Workload-IOPS beschreiben	Verfügbar über das Dashboard

Weitere Informationen zu diesen Seiten und dieser Funktionalität finden Sie in der Online-Hilfe des Produkts.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Deaktivieren oder aktivieren Sie auf der Seite **Funktionseinstellungen** die richtlinienbasierte Speicherverwaltung, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Deaktivieren Sie die richtlinienbasierte Speicherverwaltung	Bewegen Sie im Bereich **Richtlinienbasierte Speicherverwaltung** den Schieberegler nach links.
Aktivieren Sie die richtlinienbasierte Speicherverwaltung	Bewegen Sie im Bereich **Richtlinienbasierte Speicherverwaltung** den Schieberegler nach rechts.

Konfigurieren der Unified Manager-Sicherung

Sie können die Sicherungsfunktion von Unified Manager über eine Reihe von Konfigurationsschritten konfigurieren, die auf den Hostsystemen und über die Wartungskonsole ausgeführt werden.

Informationen zu den Konfigurationsschritten finden Sie unter"Verwalten von Sicherungs- und Wiederherstellungsvorgängen" .

Funktionseinstellungen verwalten

Auf der Seite „Funktionseinstellungen“ können Sie bestimmte Funktionen in Active IQ Unified Manager aktivieren und deaktivieren. Dazu gehören das Erstellen und Verwalten von Speicherobjekten basierend auf Richtlinien, das Aktivieren des API-Gateways und des Anmeldebanners, das Hochladen von Skripts zum Verwalten von Warnungen, das Timeout einer Web-UI-Sitzung basierend auf der Inaktivitätszeit und das Deaktivieren des

Empfangs von Active IQ Plattformereignissen.

Die Seite „Funktionseinstellungen“ ist nur für Benutzer mit der Rolle „Anwendungsadministrator“ verfügbar.

Informationen zum Hochladen von Skripten finden Sie unter"Aktivieren und Deaktivieren des Skript-Uploads" .

Aktivieren Sie die richtlinienbasierte Speicherverwaltung

Die Option **Richtlinienbasiertes Speichermanagement** ermöglicht ein Speichermanagement basierend auf Service Level Objectives (SLOs). Diese Option ist standardmäßig aktiviert.

Wenn Sie diese Funktion aktivieren, können Sie Speicher-Workloads auf den ONTAP -Clustern bereitstellen, die Ihrer Active IQ Unified Manager Instanz hinzugefügt wurden, und diese Workloads basierend auf den zugewiesenen Performance Service Levels und Speichereffizienzrichtlinien verwalten.

Sie können diese Funktion unter **Allgemein** > **Funktionseinstellungen** > **Richtlinienbasierte Speicherverwaltung** aktivieren oder deaktivieren. Nach Aktivierung dieser Funktion stehen folgende Seiten zur Bedienung und Überwachung zur Verfügung:

- Bereitstellung (Speicher-Workload-Bereitstellung)
- **Richtlinien** > **Leistungs-Service-Levels**
- **Richtlinien** > **Speichereffizienz**
- Spalte „Vom Leistungsservicelevel verwaltete Workloads“ auf der Seite „Cluster-Setup“
- Workload-Performance-Panel auf dem **Dashboard**

Sie können die Bildschirme verwenden, um Leistungsservicelevel und Speichereffizienzrichtlinien zu erstellen und Speicher-Workloads bereitzustellen. Sie können auch die Speicherarbeitslasten überwachen, die den zugewiesenen Leistungsserviceleveln entsprechen, sowie die nicht konformen. Über die Bedienfelder „Workload-Leistung“ und „Workload-IOPS“ können Sie außerdem die gesamte, verfügbare und genutzte Kapazität und Leistung (IOPS) der Cluster in Ihrem Rechenzentrum basierend auf den darauf bereitgestellten Speicher-Workloads bewerten.

Nachdem Sie diese Funktion aktiviert haben, können Sie die Unified Manager REST-APIs ausführen, um einige dieser Funktionen über **Menüleiste** > **Hilfe-Schaltfläche** > **API-Dokumentation** > Kategorie **Speicheranbieter** auszuführen. Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL für den Zugriff auf die REST-API-Seite im Format https://<hostname>/docs/api/ eingeben.

Weitere Informationen zu den APIs finden Sie unter"Erste Schritte mit Active IQ Unified Manager REST-APIs" .

API-Gateway aktivieren

Die API-Gateway-Funktion ermöglicht es Active IQ Unified Manager , eine einzige Steuerebene zu sein, von der aus Sie mehrere ONTAP Cluster verwalten können, ohne sich einzeln bei ihnen anmelden zu müssen.

Sie können diese Funktion auf den Konfigurationsseiten aktivieren, die angezeigt werden, wenn Sie sich zum ersten Mal bei Unified Manager anmelden. Alternativ können Sie diese Funktion unter **Allgemein** > **Funktionseinstellungen** > **API-Gateway** aktivieren oder deaktivieren.

Unified Manager REST-APIs unterscheiden sich von ONTAP REST-APIs und nicht alle Funktionen von ONTAP REST-APIs können durch die Verwendung der Unified Manager REST-APIs genutzt werden. Wenn Sie jedoch aus geschäftlichen Gründen auf die ONTAP -APIs zugreifen müssen, um bestimmte Funktionen zu verwalten, die nicht für Unified Manager verfügbar sind, können Sie die API-Gateway-Funktion aktivieren und die ONTAP -APIs ausführen. Das Gateway fungiert als Proxy zum Tunneln der API-Anfragen, indem es die Header- und Body-Anfragen im gleichen Format wie in den ONTAP -APIs verwaltet. Sie können Ihre Unified Manager-Anmeldeinformationen verwenden und die spezifischen APIs ausführen, um auf die ONTAP -Cluster zuzugreifen und sie zu verwalten, ohne einzelne Cluster-Anmeldeinformationen weiterzugeben. Unified Manager fungiert als zentraler Verwaltungspunkt für die Ausführung der APIs in den ONTAP Clustern, die von Ihrer Unified Manager-Instanz verwaltet werden. Die von den APIs zurückgegebene Antwort ist dieselbe wie die Antwort, die von den jeweiligen ONTAP REST-APIs zurückgegeben wird, die direkt von ONTAP ausgeführt werden.

Nachdem Sie diese Funktion aktiviert haben, können Sie die Unified Manager REST-APIs über **Menüleiste** > **Hilfe-Schaltfläche** > **API-Dokumentation** > Kategorie **Gateway** ausführen. Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL für den Zugriff auf die REST-API-Seite im Format `https://<hostname>/docs/api/`

Weitere Informationen zu den APIs finden Sie unter"Erste Schritte mit Active IQ Unified Manager REST-APIs" .

Inaktivitäts-Timeout angeben

Sie können den Inaktivitäts-Timeout-Wert für Active IQ Unified Manager angeben. Nach einer Inaktivität der angegebenen Zeit wird die Anwendung automatisch abgemeldet. Diese Option ist standardmäßig aktiviert.

Sie können diese Funktion deaktivieren oder die Zeit unter **Allgemein** > **Funktionseinstellungen** > **Inaktivitäts-Timeout** ändern. Sobald Sie diese Funktion aktivieren, sollten Sie im Feld **ABMELDEN NACH** das Zeitlimit der Inaktivität (in Minuten) angeben, nach dem sich das System automatisch abmeldet. Der Standardwert beträgt 4320 Minuten (72 Stunden).

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

Aktivieren von Active IQ Portalereignissen

Sie können angeben, ob Sie Active IQ Portalereignisse aktivieren oder deaktivieren möchten. Diese Einstellung ermöglicht es dem Active IQ Portal, zusätzliche Ereignisse zur Systemkonfiguration, Verkabelung usw. zu erkennen und anzuzeigen. Diese Option ist standardmäßig aktiviert.

Wenn Sie diese Funktion aktivieren, zeigt Active IQ Unified Manager Ereignisse an, die vom Active IQ Portal erkannt wurden. Diese Ereignisse werden erstellt, indem ein Satz von Regeln für AutoSupport -Nachrichten ausgeführt wird, die von allen überwachten Speichersystemen 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 **Allgemein** > **Funktionseinstellungen** > * Active IQ Portalereignisse* aktivieren oder deaktivieren. An Standorten ohne externen Netzwerkzugriff müssen Sie die Regeln manuell über **Speicherverwaltung** > **Ereigniseinrichtung** > **Regeln hochladen** hochladen.

Diese Funktion ist standardmäßig aktiviert. Durch Deaktivieren dieser Funktion werden Active IQ -Ereignisse

nicht mehr erkannt oder im Unified Manager angezeigt. Wenn diese Funktion deaktiviert ist, kann Unified Manager die Active IQ -Ereignisse auf einem Cluster zu einer vordefinierten Zeit von 00:15 Uhr für die Zeitzone dieses Clusters empfangen.

Aktivieren und Deaktivieren von Sicherheitseinstellungen zur Einhaltung der Vorschriften

Mithilfe der Schaltfläche **Anpassen** im Bereich **Sicherheits-Dashboard** der Seite „Funktionseinstellungen“ können Sie die Sicherheitsparameter für die Compliance-Überwachung im Unified Manager aktivieren oder deaktivieren.

Die Einstellungen, die auf dieser Seite aktiviert oder deaktiviert werden, regeln den allgemeinen Compliance-Status der Cluster und Speicher-VMs auf Unified Manager. Basierend auf den Auswahlen sind die entsprechenden Spalten in der Ansicht **Sicherheit: Alle Cluster** der Cluster-Inventarseite und in der Ansicht **Sicherheit: Alle Storage-VMs** der Storage-VM-Inventarseite sichtbar.

Nur Benutzer mit Administratorrolle können diese Einstellungen bearbeiten.

Die Sicherheitskriterien für Ihre ONTAP Cluster, Storage-VMs und Volumes werden anhand der Empfehlungen bewertet, die in der"Leitfaden zur Sicherheitshärtung für NetApp ONTAP 9" . Das Sicherheitsfenster auf dem Dashboard und die Sicherheitsseite zeigen den Standard-Sicherheitskonformitätsstatus Ihrer Cluster, Speicher-VMs und Volumes an. Außerdem werden Sicherheitsereignisse generiert und Verwaltungsaktionen für Cluster und Speicher-VMs aktiviert, bei denen Sicherheitsverletzungen vorliegen.

Sicherheitseinstellungen anpassen

Um die Einstellungen für die Compliance-Überwachung entsprechend Ihrer ONTAP Umgebung anzupassen, führen Sie die folgenden Schritte aus:

Schritte

1. Klicken Sie auf **Allgemein > Funktionseinstellungen > Sicherheits-Dashboard > Anpassen**. Das Popup **Einstellungen des Sicherheits-Dashboards anpassen** wird angezeigt.

   Die Sicherheitskonformitätsparameter, die Sie aktivieren oder deaktivieren, können sich direkt auf die Standardsicherheitsansichten, Berichte und geplanten Berichte auf den Bildschirmen „Cluster“ und „Speicher-VMs“ auswirken. Wenn Sie vor der Änderung der Sicherheitsparameter einen Excel-Bericht von diesen Bildschirmen hochgeladen haben, sind die heruntergeladenen Excel-Berichte möglicherweise fehlerhaft.

2. Um die benutzerdefinierten Einstellungen für Ihre ONTAP Cluster zu aktivieren oder zu deaktivieren, wählen Sie unter **Cluster** die gewünschte allgemeine Einstellung aus. Informationen zu den Optionen zum Anpassen der Cluster-Compliance finden Sie unter"Cluster-Compliance-Kategorien" .
3. Um die benutzerdefinierten Einstellungen für Ihre Speicher-VMs zu aktivieren oder zu deaktivieren, wählen Sie unter **Speicher-VM** die gewünschte allgemeine Einstellung aus. Informationen zu den Optionen zum Anpassen der Storage-VM-Compliance finden Sie unter"Storage-VM-Compliance-Kategorien" .

Passen Sie AutoSupport und Authentifizierungseinstellungen an

Im Abschnitt * AutoSupport -Einstellungen* können Sie angeben, ob zum Senden von AutoSupport -Nachrichten von ONTAP der HTTPS-Transport verwendet werden soll.

Im Abschnitt **Authentifizierungseinstellungen** können Sie die Ausgabe von Unified Manager-Warnungen für

den standardmäßigen ONTAP Administratorbenutzer aktivieren.

Aktivieren und Deaktivieren des Skript-Uploads

Die Möglichkeit, Skripte in Unified Manager hochzuladen und auszuführen, ist standardmäßig aktiviert. Wenn Ihre Organisation diese Aktivität aus Sicherheitsgründen nicht zulassen möchte, können Sie diese Funktion deaktivieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Deaktivieren oder aktivieren Sie auf der Seite „Funktionseinstellungen“ die Skripterstellung, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Skripte deaktivieren	Bewegen Sie im Bereich **Skript-Upload** den Schieberegler nach links.
Aktivieren von Skripten	Bewegen Sie im Bereich **Skript-Upload** den Schieberegler nach rechts.

Login-Banner hinzufügen

Durch das Hinzufügen eines Anmeldebanners kann Ihre Organisation beim An- und Abmelden beliebige Informationen anzeigen, beispielsweise wer auf das System zugreifen darf und welche Nutzungsbedingungen gelten.

Jeder Benutzer, beispielsweise Speicherbetreiber oder Administratoren, kann dieses Anmeldebanner-Popup während der Anmeldung, Abmeldung und Sitzungs-Timeout sehen.

Verwenden der Wartungskonsole

Sie können die Wartungskonsole verwenden, um Netzwerkeinstellungen zu konfigurieren, das System, auf dem Unified Manager installiert ist, zu konfigurieren und zu verwalten und andere Wartungsaufgaben auszuführen, die Ihnen helfen, mögliche Probleme zu verhindern und zu beheben.

Welche Funktionalität bietet die Wartungskonsole?

Mit der Unified Manager-Wartungskonsole können Sie die Einstellungen Ihres Unified Manager-Systems verwalten und alle erforderlichen Änderungen vornehmen, um das Auftreten von Problemen zu verhindern.

Abhängig vom Betriebssystem, auf dem Sie Unified Manager installiert haben, bietet die Wartungskonsole die folgenden Funktionen:

- Beheben Sie alle Probleme mit Ihrer virtuellen Appliance, insbesondere wenn die Unified Manager-Weboberfläche nicht verfügbar ist.
- Upgrade auf neuere Versionen von Unified Manager
- Erstellen Sie Support-Pakete zum Senden an den technischen Support
- Konfigurieren der Netzwerkeinstellungen
- Ändern des Wartungsbenutzerkennworts
- Stellen Sie eine Verbindung zu einem externen Datenanbieter her, um Leistungsstatistiken zu senden
- Ändern Sie die interne Leistungsdatenerfassung
- Stellen Sie die Unified Manager-Datenbank und Konfigurationseinstellungen aus einer zuvor gesicherten Version wieder her.

Was der Wartungsbenutzer tut

Der Wartungsbenutzer wird während der Installation von Unified Manager auf einem Red Hat Enterprise Linux-System erstellt. Der Wartungsbenutzername ist der Benutzer „`umadmin`“. Der Wartungsbenutzer verfügt in der Web-Benutzeroberfläche über die Rolle des Anwendungsadministrators und kann nachfolgende Benutzer erstellen und ihnen Rollen zuweisen.

Der Wartungsbenutzer oder Umadmin-Benutzer kann auch auf die Unified Manager-Wartungskonsole zugreifen.

Diagnosefunktionen für Benutzer

Der Zweck des Diagnosezugriffs besteht darin, dem technischen Support die Unterstützung bei der Fehlerbehebung zu ermöglichen. Sie sollten ihn nur verwenden, wenn Sie vom technischen Support dazu aufgefordert werden.

Der Diagnosebenutzer kann auf Anweisung des technischen Supports Befehle auf Betriebssystemebene zur Fehlerbehebung ausführen.

Zugriff auf die Wartungskonsole

Wenn die Benutzeroberfläche des Unified Managers nicht in Betrieb ist oder Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Wartungskonsole zugreifen, um Ihr Unified Manager-System zu verwalten.

Bevor Sie beginnen

Sie müssen Unified Manager installiert und konfiguriert haben.

Nach 15 Minuten Inaktivität werden Sie von der Wartungskonsole abgemeldet.

Wenn Sie bei der Installation auf VMware bereits über die VMware-Konsole als Wartungsbenutzer angemeldet sind, können Sie sich nicht gleichzeitig über Secure Shell anmelden.

Schritt

1. Führen Sie die folgenden Schritte aus, um auf die Wartungskonsole zuzugreifen:

Auf diesem Betriebssystem …	Befolgen Sie diese Schritte…
VMware	a. Stellen Sie mithilfe von Secure Shell eine Verbindung zur IP-Adresse oder zum vollqualifizierten Domänennamen der virtuellen Unified Manager-Appliance her. b. Melden Sie sich mit Ihrem Wartungsbenutzernamen und Kennwort bei der Wartungskonsole an.
Linux	a. Stellen Sie mithilfe von Secure Shell eine Verbindung zur IP-Adresse oder zum vollqualifizierten Domänennamen des Unified Manager-Systems her. b. Melden Sie sich mit dem Namen und Kennwort des Wartungsbenutzers (umadmin) beim System an. c. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
Windows	a. Melden Sie sich mit Administratoranmeldeinformationen beim Unified Manager-System an. b. Starten Sie PowerShell als Windows-Administrator. c. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.

Das Menü der Wartungskonsole von Unified Manager wird angezeigt.

Greifen Sie über die vSphere VM-Konsole auf die Wartungskonsole zu

Wenn die Benutzeroberfläche des Unified Managers nicht in Betrieb ist oder Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Wartungskonsole zugreifen, um Ihre virtuelle Appliance neu zu konfigurieren.

Bevor Sie beginnen

- Sie müssen der Wartungsbenutzer sein.
- Um auf die Wartungskonsole zugreifen zu können, muss die virtuelle Appliance eingeschaltet sein.

Schritte

1. Suchen Sie im vSphere-Client nach der virtuellen Unified Manager-Appliance.
2. Klicken Sie auf die Registerkarte **Konsole**.
3. Klicken Sie in das Konsolenfenster, um sich anzumelden.
4. Melden Sie sich mit Ihrem Benutzernamen und Kennwort bei der Wartungskonsole an.

   Nach 15 Minuten Inaktivität werden Sie von der Wartungskonsole abgemeldet.

Menüs der Wartungskonsole

Die Wartungskonsole besteht aus verschiedenen Menüs, mit denen Sie spezielle Funktionen und Konfigurationseinstellungen des Unified Manager-Servers warten und verwalten können.

Abhängig vom Betriebssystem, auf dem Sie Unified Manager installiert haben, besteht die Wartungskonsole aus den folgenden Menüs:

- Upgrade von Unified Manager (nur VMware)
- Netzwerkkonfiguration (nur VMware)
- Systemkonfiguration (nur VMware)
  a. Support/Diagnose
  b. Serverzertifikat zurücksetzen
  c. Externer Datenanbieter
  d. Backup-Wiederherstellung
  e. Konfiguration des Leistungsabfrageintervalls
  f. Deaktivieren der SAML-Authentifizierung
  g. Anwendungsports anzeigen/ändern
  h. Debug-Protokollkonfiguration
  i. Steuern Sie den Zugriff auf MySQL-Port 3306
  j. Ausfahrt

Sie wählen die Nummer aus der Liste aus, um auf die jeweilige Menüoption zuzugreifen. Wählen Sie beispielsweise für die Sicherung und Wiederherstellung *4* aus.

Menü „Netzwerkkonfiguration“

Über das Menü „Netzwerkkonfiguration“ können Sie die Netzwerkeinstellungen verwalten. Sie sollten dieses Menü verwenden, wenn die Unified Manager-Benutzeroberfläche nicht verfügbar ist.

Dieses Menü ist nicht verfügbar, wenn Unified Manager auf Red Hat Enterprise Linux oder Microsoft Windows installiert ist.

Die folgenden Menüoptionen stehen zur Verfügung.

- **IP-Adresseinstellungen anzeigen**

  Zeigt die aktuellen Netzwerkeinstellungen für die virtuelle Appliance an, einschließlich IP-Adresse, Netzwerk, Broadcast-Adresse, Netzmaske, Gateway und DNS-Server.

- **IP-Adresseinstellungen ändern**

  Ermöglicht Ihnen, alle Netzwerkeinstellungen für die virtuelle Appliance zu ändern, einschließlich IP-Adresse, Netzmaske, Gateway oder DNS-Server. Wenn Sie Ihre Netzwerkeinstellungen mithilfe der Wartungskonsole von DHCP auf statisches Netzwerk umstellen, können Sie den Hostnamen nicht bearbeiten. Sie müssen **Änderungen übernehmen** auswählen, damit die Änderungen wirksam werden.

- **Sucheinstellungen für Domänennamen anzeigen**

  Zeigt die Domänennamen-Suchliste an, die zum Auflösen von Hostnamen verwendet wird.

- **Einstellungen für die Domänennamensuche ändern**

  Ermöglicht Ihnen, die Domänennamen zu ändern, nach denen Sie beim Auflösen von Hostnamen suchen möchten. Sie müssen **Änderungen übernehmen** auswählen, damit die Änderungen wirksam werden.

- **Statische Routen anzeigen**

  Zeigt die aktuellen statischen Netzwerkrouten an.

- **Statische Routen ändern**

  Ermöglicht Ihnen, statische Netzwerkrouten hinzuzufügen oder zu löschen. Sie müssen **Änderungen übernehmen** auswählen, damit die Änderungen wirksam werden.

  - **Route hinzufügen**

    Ermöglicht Ihnen, eine statische Route hinzuzufügen.

  - **Route löschen**

    Ermöglicht Ihnen, eine statische Route zu löschen.

  - **Zurück**

    Bringt Sie zurück zum **Hauptmenü**.

  - **Ausfahrt**

    Beendet die Wartungskonsole.

- **Netzwerkschnittstelle deaktivieren**

  Deaktiviert alle verfügbaren Netzwerkschnittstellen. Wenn nur eine Netzwerkschnittstelle verfügbar ist, können Sie diese nicht deaktivieren. Sie müssen **Änderungen übernehmen** auswählen, damit die

Änderungen wirksam werden.

- **Netzwerkschnittstelle aktivieren**

  Aktiviert verfügbare Netzwerkschnittstellen. Sie müssen **Änderungen übernehmen** auswählen, damit die Änderungen wirksam werden.

- **Änderungen festschreiben**

  Wendet alle an den Netzwerkeinstellungen für die virtuelle Appliance vorgenommenen Änderungen an. Sie müssen diese Option auswählen, um die vorgenommenen Änderungen zu übernehmen, andernfalls werden die Änderungen nicht übernommen.

- **Ping einen Host**

  Pingt einen Zielhost an, um Änderungen der IP-Adresse 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**

  Bringt Sie zurück zum **Hauptmenü**.

- **Ausfahrt**

  Beendet die Wartungskonsole.

Menü „Systemkonfiguration“

Über das Menü „Systemkonfiguration“ können Sie Ihre virtuelle Appliance verwalten. Es bietet verschiedene Optionen, beispielsweise die Anzeige des Serverstatus sowie das Neustarten und Herunterfahren der virtuellen Maschine.

Wenn Unified Manager auf einem Linux- oder Microsoft Windows-System installiert ist, ist in diesem Menü nur die Option „Aus einer Unified Manager-Sicherung wiederherstellen“ verfügbar.

Folgende Menüoptionen stehen zur Verfügung:

- **Serverstatus anzeigen**

  Zeigt den aktuellen Serverstatus an. Zu den Statusoptionen gehören „Wird ausgeführt“ und „Wird nicht ausgeführt“.

  Wenn der Server nicht läuft, müssen Sie sich möglicherweise an den technischen Support wenden.

- **Virtuelle Maschine neu starten**

  Startet die virtuelle Maschine neu und stoppt alle Dienste. Nach dem Neustart werden die virtuelle Maschine und die Dienste neu gestartet.

- **Virtuelle Maschine herunterfahren**

Fährt die virtuelle Maschine herunter und stoppt alle Dienste.

Sie können diese Option nur über die Konsole der virtuellen Maschine auswählen.

- **Benutzerkennwort <angemeldeter Benutzer> ändern**

  Ändert das Passwort des aktuell angemeldeten Benutzers, was nur der Wartungsbenutzer sein kann.

- **Datenträgergröße erhöhen**

  Erhöht die Größe der Datenfestplatte (Festplatte 3) in der virtuellen Maschine.

- **Größe der Swap-Disk erhöhen**

  Erhöht die Größe der Auslagerungsfestplatte (Festplatte 2) in der virtuellen Maschine.

- **Zeitzone ändern**

  Ändert die Zeitzone auf Ihren Standort.

- **NTP-Server ändern**

  Ändert die NTP-Servereinstellungen, z. B. IP-Adresse oder vollqualifizierter Domänenname (FQDN).

- **NTP-Dienst ändern**

  Schaltet um zwischen `ntp` Und `systemd-timesyncd` Dienstleistungen.

- **Wiederherstellung aus einem Unified Manager-Backup**

  Stellt die Unified Manager-Datenbank und Konfigurationseinstellungen aus einer zuvor gesicherten Version wieder her.

- **Serverzertifikat zurücksetzen**

  Setzt das Sicherheitszertifikat des Servers zurück.

- **Hostnamen ändern**

  Ändert den Namen des Hosts, auf dem die virtuelle Appliance installiert ist.

- **Zurück**

  Verlässt das Systemkonfigurationsmenü und kehrt zum Hauptmenü zurück.

- **Ausfahrt**

  Beendet das Wartungskonsolenmenü.

Menü „Support und Diagnose“

Über das Menü „Support und Diagnose“ können Sie ein Supportpaket erstellen, das Sie zur Unterstützung bei der Fehlerbehebung an den technischen Support senden können.

Folgende Menüpunkte stehen zur Verfügung:

- **Light Support Bundle erstellen**

  Ermöglicht Ihnen die Erstellung eines schlanken Support-Pakets, das lediglich 30 Tage Protokolle und Konfigurationsdatenbankaufzeichnungen enthält – Leistungsdaten, Erfassungsaufzeichnungsdateien und Server-Heap-Dumps sind nicht enthalten.

- **Support-Paket erstellen**

  Ermöglicht Ihnen die Erstellung eines vollständigen Support-Pakets (7-Zip-Datei) mit Diagnoseinformationen im Home-Verzeichnis des Diagnosebenutzers. Wenn Ihr System mit dem Internet verbunden ist, können Sie das Support-Paket auch auf NetApp hochladen.

  Die Datei enthält von einer AutoSupport Nachricht generierte Informationen, den Inhalt der Unified Manager-Datenbank, detaillierte Daten zu den internen Komponenten des Unified Manager-Servers und ausführliche Protokolle, die normalerweise nicht in AutoSupport -Nachrichten oder im Lightweight-Support-Paket enthalten sind.

Zusätzliche Menüoptionen

Mit den folgenden Menüoptionen können Sie verschiedene Verwaltungsaufgaben auf dem Unified Manager-Server ausführen.

Folgende Menüoptionen stehen zur Verfügung:

- **Serverzertifikat zurücksetzen**

  Generiert das HTTPS-Serverzertifikat neu.

  Sie können das Serverzertifikat in der Unified Manager-GUI neu generieren, indem Sie auf **Allgemein** > **HTTPS-Zertifikate** > **HTTPS-Zertifikat neu generieren** klicken.

- **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 Konsolenoption wird normalerweise verwendet, wenn ein Problem mit dem IdP-Server oder der SAML-Konfiguration den Zugriff der Benutzer auf die Unified Manager-GUI blockiert.

- **Externer Datenanbieter**

  Bietet Optionen zum Verbinden von Unified Manager mit einem externen Datenanbieter. Nachdem Sie die Verbindung hergestellt haben, werden Leistungsdaten an einen externen Server gesendet, sodass Speicherleistungsexperten die Leistungsmetriken mithilfe von Software von Drittanbietern aufzeichnen können. Die folgenden Optionen werden angezeigt:

  - **Serverkonfiguration anzeigen** – Zeigt die aktuellen Verbindungs- und Konfigurationseinstellungen für einen externen Datenanbieter an.
  - **Serververbindung hinzufügen/ändern** – Ermöglicht Ihnen, neue Verbindungseinstellungen für einen externen Datenanbieter einzugeben oder vorhandene Einstellungen zu ändern.
  - **Serverkonfiguration ändern** – Ermöglicht Ihnen, neue Konfigurationseinstellungen für einen externen Datenanbieter einzugeben oder vorhandene Einstellungen zu ändern.
  - **Serververbindung löschen** – Löscht die Verbindung zu einem externen Datenanbieter.

Nachdem die Verbindung gelöscht wurde, verliert Unified Manager seine Verbindung zum externen Server.

- **Backup-Wiederherstellung**

  Weitere Informationen finden Sie in den Themen unter"Verwalten von Sicherungs- und Wiederherstellungsvorgängen" .

- **Konfiguration des Leistungsabfrageintervalls**

  Bietet eine Option zum Konfigurieren, wie häufig Unified Manager Leistungsstatistikdaten von Clustern sammelt. Das Standarderfassungsintervall beträgt 5 Minuten.

  Sie können dieses Intervall auf 10 oder 15 Minuten ändern, wenn Sie feststellen, dass Sammlungen aus großen Clustern nicht rechtzeitig abgeschlossen werden.

- **Anwendungsports anzeigen/ändern**

  Bietet eine Option zum Ändern der Standardports, die Unified Manager für 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 MySQL-Standardport 3306. Aus Sicherheitsgründen ist der Zugriff über diesen Port während einer Neuinstallation von Unified Manager auf Linux-, Windows- und VMware vSphere-Systemen nur auf localhost beschränkt. Mit dieser Option können Sie die Sichtbarkeit dieses Ports zwischen dem lokalen Host und den Remote-Hosts umschalten. Das heißt, wenn er in Ihrer Umgebung nur für den lokalen Host aktiviert ist, können Sie diesen Port auch für Remote-Hosts verfügbar machen. Alternativ können Sie, wenn die Option für alle Hosts aktiviert ist, den Zugriff auf diesen Port nur auf den lokalen Host beschränken. Wenn der Zugriff auf Remote-Hosts zuvor aktiviert wurde, bleibt die Konfiguration in einem Upgrade-Szenario erhalten. Sie sollten die Firewall-Einstellungen auf Windows-Systemen überprüfen, nachdem Sie die Port-Sichtbarkeit umgeschaltet haben, und die Firewall-Einstellungen deaktivieren, wenn die Einstellungen so konfiguriert sind, dass der Zugriff auf MySQL-Port 3306 eingeschränkt ist.

- **Ausfahrt**

  Beendet das Wartungskonsolenmenü.

Ändern des Wartungsbenutzerkennworts unter Windows

Sie können das Wartungsbenutzerkennwort von Unified Manager bei Bedarf ändern.

Schritte

1. Klicken Sie auf der Anmeldeseite der Unified Manager-Webbenutzeroberfläche auf **Passwort vergessen**.

   Es wird eine Seite angezeigt, auf der Sie nach dem Namen des Benutzers gefragt werden, dessen Kennwort Sie zurücksetzen möchten.

2. Geben Sie den Benutzernamen ein und klicken Sie auf **Senden**.

   Eine E-Mail mit einem Link zum Zurücksetzen des Kennworts wird an die für diesen Benutzernamen definierte E-Mail-Adresse gesendet.

3. Klicken Sie in der E-Mail auf den Link **Passwort zurücksetzen** und legen Sie das neue Passwort fest.
4. Kehren Sie zur Web-Benutzeroberfläche zurück und melden Sie sich mit dem neuen Kennwort bei Unified Manager an.

Ändern des Umadmin-Passworts auf Linux-Systemen

Aus Sicherheitsgründen müssen Sie das Standardkennwort für den Unified Manager-Benutzer umadmin unmittelbar nach Abschluss des Installationsvorgangs ändern. Bei Bedarf können Sie das Passwort später jederzeit wieder ändern.

Bevor Sie beginnen

- Unified Manager muss auf einem Red Hat Enterprise Linux-Linux-System installiert sein.
- Sie müssen über die Root-Benutzeranmeldeinformationen für das Linux-System verfügen, auf dem Unified Manager installiert ist.

Schritte

1. Melden Sie sich als Root-Benutzer beim Linux-System an, auf dem Unified Manager ausgeführt wird.
2. Ändern Sie das Umadmin-Passwort:

   ```
   passwd umadmin
   ```

   Das System fordert Sie auf, ein neues Passwort für den Benutzer umadmin einzugeben.

Ändern Sie die Ports, die Unified Manager für HTTP- und HTTPS-Protokolle verwendet

Die Standardports, die Unified Manager für die Protokolle HTTP und HTTPS verwendet, 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 Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.

> Es gibt einige Ports, die bei Verwendung der Browser Mozilla Firefox oder Google Chrome als unsicher gelten. Prüfen Sie dies mit Ihrem Browser, bevor Sie eine neue Portnummer für HTTP- und HTTPS-Verkehr zuweisen. Durch die Auswahl eines unsicheren Ports kann das System möglicherweise nicht mehr erreichbar sein. In diesem Fall müssten Sie sich zur Lösung des Problems an den Kundendienst wenden.

Die Instanz von Unified Manager wird nach der Portänderung automatisch neu gestartet. Stellen Sie daher sicher, dass dies ein guter Zeitpunkt ist, um das System für kurze Zeit herunterzufahren.

1. Melden Sie sich per SSH als Wartungsbenutzer beim Unified Manager-Host an.

   Die Eingabeaufforderungen der Unified Manager-Wartungskonsole werden angezeigt.

2. Geben Sie die Nummer der Menüoption mit der Bezeichnung **Anwendungsports anzeigen/ändern** ein und drücken Sie dann die Eingabetaste.

3. Geben Sie bei entsprechender Aufforderung das Wartungsbenutzerkennwort erneut ein.
4. Geben Sie die neuen Portnummern für die HTTP- und HTTPS-Ports ein und drücken Sie dann die Eingabetaste.

   Wenn Sie eine Portnummer leer lassen, wird der Standardport für das Protokoll zugewiesen.

   Sie werden gefragt, ob Sie die Ports ändern und Unified Manager jetzt neu starten möchten.

5. Geben Sie **y** ein, um die Ports zu ändern und Unified Manager neu zu starten.
6. Beenden Sie die Wartungskonsole.

Nach dieser Änderung müssen Benutzer die neue Portnummer in die URL aufnehmen, um auf die Unified Manager-Web-Benutzeroberfläche zuzugreifen, z. B. https://host.company.com:1234, https://12.13.14.15:1122 oder https://[2001:db8:0:1]:2123.

Netzwerkschnittstellen hinzufügen

Sie können neue Netzwerkschnittstellen hinzufügen, wenn Sie den Netzwerkverkehr trennen müssen.

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 unter Red Hat Enterprise Linux oder Microsoft Windows installiert ist.

Schritte

1. Wählen Sie im Hauptmenü der vSphere-Konsole **Systemkonfiguration** > **Betriebssystem neu starten**.

   Nach dem Neustart kann die Wartungskonsole die neu hinzugefügte Netzwerkschnittstelle erkennen.

2. Greifen Sie auf die Wartungskonsole zu.
3. Wählen Sie **Netzwerkkonfiguration** > **Netzwerkschnittstelle aktivieren**.
4. Wählen Sie die neue Netzwerkschnittstelle aus und drücken Sie **Enter**.

   Wählen Sie **eth1** und drücken Sie **Enter**.

5. Geben Sie **y** ein, um die Netzwerkschnittstelle zu aktivieren.
6. Geben Sie die Netzwerkeinstellungen ein.

   Sie werden aufgefordert, die Netzwerkeinstellungen einzugeben, wenn Sie eine statische Schnittstelle verwenden oder wenn DHCP nicht erkannt wird.

   Nach der Eingabe der Netzwerkeinstellungen gelangen Sie automatisch zurück in das Menü **Netzwerkkonfiguration**.

7. Wählen Sie **Änderungen übernehmen**.

   Sie müssen die Änderungen bestätigen, um die Netzwerkschnittstelle hinzuzufügen.

Fügen Sie dem Unified Manager-Datenbankverzeichnis Speicherplatz hinzu

Das Unified Manager-Datenbankverzeichnis enthält alle von ONTAP -Systemen erfassten Integritäts- und Leistungsdaten. Unter bestimmten Umständen kann es erforderlich sein, dass Sie die Größe des Datenbankverzeichnisses erhöhen.

Beispielsweise kann das Datenbankverzeichnis voll werden, wenn Unified Manager Daten aus einer großen Anzahl von Clustern sammelt, wobei jeder Cluster viele Knoten hat. Sie erhalten ein Warnereignis, wenn das Datenbankverzeichnis zu 90 % voll ist, und ein kritisches Ereignis, wenn das Verzeichnis zu 95 % voll ist.

Wenn das Verzeichnis zu 95 % gefüllt ist, werden keine weiteren Daten mehr aus den Clustern erfasst.

Die zum Hinzufügen von Kapazität zum Datenverzeichnis erforderlichen Schritte unterscheiden sich, je nachdem, ob Unified Manager auf einem VMware ESXi-Server, einem Red Hat-Server oder einem Microsoft Windows-Server ausgeführt wird.

Fügen Sie dem Datenverzeichnis des Linux-Hosts Speicherplatz hinzu

Wenn Sie nicht genügend Speicherplatz für die `/opt/netapp/data` Verzeichnis zur Unterstützung von Unified Manager, wenn Sie den Linux-Host ursprünglich eingerichtet und dann Unified Manager installiert haben, können Sie nach der Installation Speicherplatz hinzufügen, indem Sie den Speicherplatz auf dem `/opt/netapp/data` Verzeichnis.

Bevor Sie beginnen

Sie müssen über Root-Benutzerzugriff auf die Red Hat Enterprise Linux-Maschine verfügen, auf der Unified Manager installiert ist.

Wir empfehlen, dass Sie die Unified Manager-Datenbank sichern, bevor Sie die Größe des Datenverzeichnisses erhöhen.

Schritte

1. Melden Sie sich als Root-Benutzer bei der Linux-Maschine an, auf der Sie Speicherplatz hinzufügen möchten.
2. Stoppen Sie den Unified Manager-Dienst und die zugehörige MySQL-Software in der angezeigten Reihenfolge:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Erstellen Sie einen temporären Sicherungsordner (z. B. `/backup-data`) mit ausreichend Speicherplatz, um die Daten im aktuellen `/opt/netapp/data` Verzeichnis.
4. Kopieren Sie den Inhalt und die Berechtigungskonfiguration des bestehenden `/opt/netapp/data` Verzeichnis in das Sicherungsdatenverzeichnis:

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

5. Wenn SE Linux aktiviert ist:

   a. Holen Sie sich den SE Linux-Typ für Ordner auf 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 ähnlich der folgenden zurück:

```
echo $se_type
mysqld_db_t
```

a. Führen Sie den Befehl chcon aus, um den SE Linux-Typ für das Sicherungsverzeichnis festzulegen:

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Entfernen Sie den Inhalt des `/opt/netapp/data` Verzeichnis:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Erweitern Sie die Größe des `/opt/netapp/data` Verzeichnis auf mindestens 150 GB durch LVM-Befehle oder durch Hinzufügen zusätzlicher Festplatten.

> Wenn Sie erstellt haben `/opt/netapp/data` von einer Festplatte, dann sollten Sie nicht versuchen, zu mounten `/opt/netapp/data` als NFS- oder CIFS-Freigabe. Denn in diesem Fall, wenn Sie versuchen, den Speicherplatz zu erweitern, einige LVM-Befehle, wie zum Beispiel `resize` Und `extend` funktioniert möglicherweise nicht wie erwartet.

8. Bestätigen Sie, dass die `/opt/netapp/data` Verzeichnisbesitzer (mysql) und Gruppe (root) bleiben unverändert:

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

Das System gibt eine Bestätigung ähnlich der folgenden zurück:

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

9. Wenn SE Linux aktiviert ist, bestätigen Sie, dass der Kontext für die `/opt/netapp/data` Verzeichnis ist immer noch auf mysqld_db_t eingestellt:
   a. `touch /opt/netapp/data/abc`
   b. `ls -Z /opt/netapp/data/abc`

Das System gibt eine Bestätigung ähnlich der folgenden zurück:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Löschen Sie die Datei abc, damit diese überflüssige Datei in Zukunft keinen Datenbankfehler verursacht.

11. Kopieren Sie den Inhalt der Sicherungsdaten zurück in die erweiterte `/opt/netapp/data` Verzeichnis:

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

12. Wenn SE Linux aktiviert ist, führen Sie den folgenden Befehl aus:

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

13. Starten Sie den MySQL-Dienst:

    ```
    systemctl start mysqld
    ```

14. Nachdem der MySQL-Dienst gestartet wurde, starten Sie die Dienste ocie und ocieau in der angezeigten Reihenfolge:

    ```
    systemctl start ocie ocieau
    ```

15. Nachdem alle Dienste gestartet sind, löschen Sie den Sicherungsordner `/backup-data` :

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

Fügen Sie Speicherplatz zur Datenfestplatte der virtuellen VMware-Maschine hinzu

Wenn Sie den Speicherplatz auf der Datenfestplatte für die Unified Manager-Datenbank erhöhen müssen, können Sie nach der Installation Kapazität hinzufügen, indem Sie den Speicherplatz mithilfe der Unified Manager-Wartungskonsole erhöhen.

Bevor Sie beginnen

- Sie müssen Zugriff auf den vSphere-Client haben.
- Auf der virtuellen Maschine dürfen keine Snapshots lokal gespeichert sein.
- Sie müssen über die Anmeldeinformationen des Wartungsbenutzers verfügen.

Wir empfehlen Ihnen, Ihre virtuelle Maschine zu sichern, bevor Sie die Größe virtueller Festplatten erhöhen.

Schritte

1. Wählen Sie im vSphere-Client die virtuelle Maschine Unified Manager aus und fügen Sie dann mehr Festplattenkapazität zu Daten hinzu `disk 3` . Weitere Informationen finden Sie in der VMware-Dokumentation.

   In einigen seltenen Fällen verwendet die Unified Manager-Bereitstellung „Festplatte 2“ für die Datenfestplatte anstelle von „Festplatte 3“. Wenn dies bei Ihrer Bereitstellung der Fall ist, erhöhen Sie den Speicherplatz auf der größeren Festplatte. Auf der Datenfestplatte ist immer mehr Speicherplatz vorhanden als auf der anderen Festplatte.

2. Wählen Sie im vSphere-Client die virtuelle Maschine Unified Manager und dann die Registerkarte **Konsole** aus.
3. Klicken Sie in das Konsolenfenster und melden Sie sich dann mit Ihrem Benutzernamen und Kennwort bei der Wartungskonsole an.
4. Geben Sie im Hauptmenü die Nummer für die Option **Systemkonfiguration** ein.
5. Geben Sie im Systemkonfigurationsmenü die Zahl für die Option **Datenträgergröße erhöhen** ein.

Fügen Sie dem logischen Laufwerk des Microsoft Windows-Servers Speicherplatz hinzu

Wenn Sie den Speicherplatz für die Unified Manager-Datenbank erhöhen müssen, können Sie die Kapazität des logischen Laufwerks erhöhen, auf dem Unified Manager installiert ist.

Bevor Sie beginnen

Sie müssen über Windows-Administratorrechte verfügen.

Wir empfehlen Ihnen, die Unified Manager-Datenbank zu sichern, bevor Sie Speicherplatz hinzufügen.

Schritte

1. Melden Sie sich als Administrator bei dem Windows-Server an, auf dem Sie Speicherplatz hinzufügen möchten.
2. Führen Sie den Schritt aus, der der Methode entspricht, mit der Sie mehr Speicherplatz hinzufügen möchten:

Option	Beschreibung
Erhöhen Sie auf einem physischen Server die Kapazität des logischen Laufwerks, auf dem der Unified Manager-Server installiert ist.	Befolgen Sie die Schritte im Microsoft-Thema: "Erweitern eines Basisvolumes"
Fügen Sie auf einem physischen Server ein Festplattenlaufwerk hinzu.	Befolgen Sie die Schritte im Microsoft-Thema: "Hinzufügen von Festplattenlaufwerken"
Erhöhen Sie auf einer virtuellen Maschine die Größe einer Festplattenpartition.	Befolgen Sie die Schritte im VMware-Thema: "Erhöhen der Größe einer Festplattenpartition"

Verwalten des Benutzerzugriffs

Sie können Rollen erstellen und Berechtigungen zuweisen, um den Benutzerzugriff auf Active IQ Unified Manager zu steuern. Sie können Benutzer identifizieren, die über die erforderlichen Berechtigungen verfügen, um auf ausgewählte Objekte in Unified Manager zuzugreifen. Nur Benutzer mit diesen Rollen und Berechtigungen können die Objekte in Unified Manager verwalten.

Benutzer hinzufügen

Sie können lokale Benutzer oder Datenbankbenutzer über die Seite „Benutzer“ hinzufügen. Sie können auch Remotebenutzer oder -gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Sie können diesen Benutzern Rollen zuweisen und basierend auf den Berechtigungen der Rollen können Benutzer die Speicherobjekte und Daten mit Unified Manager verwalten oder die Daten in einer Datenbank anzeigen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.
- 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) Benutzer authentifiziert, die auf die grafische Benutzeroberfläche zugreifen, stellen Sie sicher, dass diese Benutzer als „Remote“-Benutzer definiert sind.

  Der Zugriff auf die Benutzeroberfläche ist für Benutzer vom Typ „`local`“ oder „`maintenance`“ nicht zulässig, 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 von OpenLDAP oder anderen Authentifizierungsdiensten hinzufügen, können sich nur die direkten Mitglieder dieser Gruppe bei Unified Manager authentifizieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Klicken Sie auf der Seite „Benutzer“ auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld „Benutzer hinzufügen“ den Benutzertyp aus, den Sie hinzufügen möchten, und geben Sie die erforderlichen Informationen ein.

   Beim Eingeben der erforderlichen Benutzerinformationen müssen Sie eine E-Mail-Adresse angeben, die für diesen Benutzer eindeutig ist. Sie müssen die Angabe von E-Mail-Adressen vermeiden, die von mehreren Benutzern gemeinsam genutzt werden.

4. Klicken Sie auf **Hinzufügen**.

Erstellen eines Datenbankbenutzers

Um eine Verbindung zwischen Workflow Automation und Unified Manager zu unterstützen oder auf Datenbankansichten zuzugreifen, müssen Sie zunächst einen Datenbankbenutzer mit der Rolle „Integrationsschema“ oder „Berichtsschema“ in der Unified Manager-Web-Benutzeroberfläche erstellen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Datenbankbenutzer ermöglichen die Integration mit Workflow Automation und den Zugriff auf berichtsspezifische Datenbankansichten. Datenbankbenutzer haben keinen Zugriff auf die Unified Manager-Web-Benutzeroberfläche oder die Wartungskonsole und können keine API-Aufrufe ausführen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Klicken Sie auf der Seite „Benutzer“ auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld „Benutzer hinzufügen“ in der Dropdownliste „Typ“ die Option „Datenbankbenutzer“ aus.
4. Geben Sie einen Namen und ein Kennwort für den Datenbankbenutzer ein.
5. Wählen Sie in der Dropdownliste **Rolle** die entsprechende Rolle aus.

Wenn Sie…	Wählen Sie diese Rolle
Unified Manager mit Workflow-Automatisierung verbinden	Integrationsschema
Zugriff auf Berichte und andere Datenbankansichten	Berichtsschema

6. Klicken Sie auf **Hinzufügen**.

Bearbeiten der Benutzereinstellungen

Sie können Benutzereinstellungen – wie etwa die E-Mail-Adresse und Rolle – bearbeiten, die für jeden Benutzer festgelegt sind. Sie möchten beispielsweise die Rolle eines Benutzers ändern, der Speicheroperator ist, und dem Benutzer Speicheradministratorrechte zuweisen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Wenn Sie die einem Benutzer zugewiesene Rolle ändern, werden die Änderungen angewendet, wenn eine der folgenden Aktionen eintritt:

- Der Benutzer meldet sich bei Unified Manager ab und wieder an.
- Das Sitzungs-Timeout von 24 Stunden ist erreicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Wählen Sie auf der Seite „Benutzer“ den Benutzer aus, für den Sie die Einstellungen bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
3. Bearbeiten Sie im Dialogfeld „Benutzer bearbeiten“ die entsprechenden Einstellungen, die für den Benutzer angegeben sind.
4. Klicken Sie auf **Speichern**.

Benutzer anzeigen

Auf der Seite „Benutzer“ können Sie die Liste der Benutzer anzeigen, die Speicherobjekte und Daten mit Unified Manager verwalten. Sie können Details zu den Benutzern anzeigen, z. B. Benutzername, Benutzertyp, E-Mail-Adresse und die den Benutzern zugewiesene Rolle.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritt

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.

Löschen von Benutzern oder Gruppen

Sie können einen oder mehrere Benutzer aus der Management-Server-Datenbank löschen, um bestimmten Benutzern den Zugriff auf Unified Manager zu verwehren. Sie können Gruppen auch löschen, sodass alle Benutzer in der Gruppe nicht mehr auf den Verwaltungsserver zugreifen können.

Bevor Sie beginnen

- Wenn Sie Remote-Gruppen löschen, müssen Sie die Ereignisse neu zugewiesen haben, die den Benutzern der Remote-Gruppen zugewiesen sind.

  Wenn Sie lokale Benutzer oder Remote-Benutzer löschen, wird die Zuweisung der diesen Benutzern zugewiesenen Ereignisse automatisch aufgehoben.

- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Wählen Sie auf der Seite „Benutzer“ die Benutzer oder Gruppen aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.

Was ist RBAC?

RBAC (rollenbasierte Zugriffskontrolle) bietet die Möglichkeit zu steuern, wer Zugriff auf verschiedene Funktionen und Ressourcen im Active IQ Unified Manager Server hat.

Was rollenbasierte Zugriffskontrolle bewirkt

Die rollenbasierte Zugriffskontrolle (RBAC) ermöglicht Administratoren die Verwaltung von Benutzergruppen durch die Definition von Rollen. Wenn Sie den Zugriff auf bestimmte Funktionen auf ausgewählte Administratoren beschränken müssen, müssen Sie für diese Administratorkonten einrichten. Wenn Sie die Informationen, die Administratoren anzeigen können, und die Vorgänge, die sie ausführen können, einschränken möchten, müssen Sie den von Ihnen erstellten Administratorkonten Rollen zuweisen.

Der Verwaltungsserver verwendet RBAC für die Benutzeranmeldung und Rollenberechtigungen. Wenn Sie die Standardeinstellungen des Verwaltungsservers für den Administratorbenutzerzugriff nicht geändert haben, müssen Sie sich nicht anmelden, um sie anzuzeigen.

Wenn Sie einen Vorgang starten, der bestimmte Berechtigungen erfordert, werden Sie vom Verwaltungsserver aufgefordert, sich anzumelden. Um beispielsweise Administratorkonten zu erstellen, müssen Sie sich mit dem Kontozugriff des Anwendungsadministrators anmelden.

Definitionen von Benutzertypen

Ein Benutzertyp gibt die Art des Kontos an, das der Benutzer besitzt, und umfasst Remotebenutzer, Remotegruppen, lokale Benutzer, Datenbankbenutzer und

Wartungsbenutzer. Jeder dieser Typen hat seine eigene Rolle, die von einem Benutzer mit der Rolle „Administrator“ zugewiesen wird.

Es gibt folgende Unified Manager-Benutzertypen:

- **Wartungsbenutzer**

  Wird während der Erstkonfiguration von Unified Manager erstellt. Anschließend legt der Wartungsbenutzer weitere Benutzer an und weist ihnen Rollen zu. Der Wartungsbenutzer ist auch der einzige Benutzer mit Zugriff auf die Wartungskonsole. 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 Funktionen basierend auf der Rolle aus, die vom Wartungsbenutzer oder einem Benutzer mit der Rolle „Anwendungsadministrator“ zugewiesen wurde.

- **Remote-Gruppe**

  Eine Gruppe von Benutzern, die mit den auf dem Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Unified Manager-Benutzeroberfläche 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-Benutzeroberfläche. Remote-Gruppen können Funktionen entsprechend ihrer zugewiesenen Rollen ausführen.

- **Remote-Benutzer**

  Greift mit den auf dem Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Unified Manager-Benutzeroberfläche zu. Ein Remote-Benutzer führt Funktionen basierend auf der Rolle aus, die ihm vom Wartungsbenutzer oder einem Benutzer mit der Rolle „Anwendungsadministrator“ zugewiesen wurde.

- **Datenbankbenutzer**

  Hat schreibgeschützten Zugriff auf Daten in der Unified Manager-Datenbank, keinen Zugriff auf die Unified Manager-Weboberfläche oder die Wartungskonsole und kann keine API-Aufrufe ausführen.

Definitionen von Benutzerrollen

Der Wartungsbenutzer oder Anwendungsadministrator weist jedem Benutzer eine Rolle zu. Jede Rolle beinhaltet bestimmte Privilegien. Der Umfang der Aktivitäten, die Sie in Unified Manager ausführen können, hängt von der Ihnen zugewiesenen Rolle und den mit der Rolle verbundenen Berechtigungen ab.

Unified Manager umfasst die folgenden vordefinierten Benutzerrollen:

- **Operator**

  Zeigt Speichersysteminformationen und andere von Unified Manager erfasste Daten an, einschließlich Verlaufsdaten und Kapazitätstrends. Mit dieser Rolle kann der Speicherbetreiber die Ereignisse anzeigen, zuordnen, bestätigen, beheben und Notizen hinzufügen.

- **Speicheradministrator**

  Konfiguriert Speicherverwaltungsvorgänge innerhalb von Unified Manager. Mit dieser Rolle kann der Speicheradministrator Schwellenwerte konfigurieren und Warnmeldungen sowie andere speicherverwaltungsspezifische Optionen und Richtlinien erstellen.

- **Anwendungsadministrator**

  Konfiguriert Einstellungen, die nichts mit der Speicherverwaltung zu tun haben. Diese Rolle ermöglicht die Verwaltung von Benutzern, Sicherheitszertifikaten, Datenbankzugriff und Verwaltungsoptionen, einschließlich Authentifizierung, SMTP, Netzwerk und AutoSupport.

  Wenn Unified Manager auf Linux-Systemen installiert wird, 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
  - Waagenmonitor

Unified Manager-Benutzerrollen und -Funktionen

Basierend auf Ihrer zugewiesenen Benutzerrolle können Sie bestimmen, welche Vorgänge Sie in Unified Manager ausführen können.

In der folgenden Tabelle sind die Funktionen aufgeführt, die jede Benutzerrolle ausführen kann:

Funktion	Operator	Speicheradministrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Anzeigen von Speichersysteminformationen	•	•	•	•	•

Funktion	Operator	Speicheradministrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Weitere Daten wie Verlaufsdaten und Kapazitätstrends anzeigen	•	•	•	•	•
Ereignisse anzeigen, zuweisen und lösen	•	•	•		
Anzeigen von Speicherdienstobjekten wie SVM-Zuordnungen und Ressourcenpools	•	•	•		
Schwellenwertrichtlinien anzeigen	•	•	•		
Verwalten Sie Speicherdienstobjekte wie SVM-Zuordnungen und Ressourcenpools		•	•		
Definieren von Warnungen		•	•		
Verwalten von Speicherverwaltungsoptionen		•	•		
Verwalten von Speicherverwaltungsrichtlinien		•	•		
Benutzer verwalten			•		

Funktion	Operator	Speicheradministrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Verwalten von Verwaltungsoptionen			•		
Definieren von Schwellenwertrichtlinien			•		
Verwalten des Datenbankzugriffs			•		
Verwalten Sie die Integration mit WFA und gewähren Sie Zugriff auf die Datenbankansichten				•	
Planen und Speichern von Berichten		•	•		
Führen Sie „Fix It“-Vorgänge über Verwaltungsaktionen aus		•	•		
Gewähren Sie schreibgeschützten Zugriff auf Datenbankansichten					•

Verwalten der SAML-Authentifizierungseinstellungen

Nachdem Sie die Remote-Authentifizierungseinstellungen konfiguriert haben, können Sie die Security Assertion Markup Language (SAML)-Authentifizierung aktivieren, sodass Remote-Benutzer von einem sicheren Identitätsanbieter (IdP) authentifiziert werden, bevor sie auf die Unified Manager-Web-Benutzeroberfläche zugreifen können.

Beachten Sie, dass nach der Aktivierung der SAML-Authentifizierung nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager haben. Lokale Benutzer und Wartungsbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf

die Wartungskonsole zugreifen.

Anforderungen an den Identitätsanbieter

Wenn Sie Unified Manager so konfigurieren, dass ein Identitätsanbieter (IdP) zur Durchführung der SAML-Authentifizierung für alle Remote-Benutzer verwendet wird, müssen Sie einige erforderliche Konfigurationseinstellungen beachten, damit die Verbindung zu Unified Manager erfolgreich ist.

Sie müssen die URI und Metadaten des Unified Managers in den IdP-Server eingeben. Sie können diese Informationen von der SAML-Authentifizierungsseite von Unified Manager kopieren. Unified Manager gilt als Dienstanbieter (SP) im Security Assertion Markup Language (SAML)-Standard.

Unterstützte Verschlüsselungsstandards

- Advanced Encryption Standard (AES): AES-128 und AES-256
- Secure Hash Algorithm (SHA): SHA-1 und SHA-256

Validierte Identitätsanbieter

- Shibboleth
- Active Directory-Verbunddienste (ADFS)

ADFS-Konfigurationsanforderungen

- Sie müssen drei Anspruchsregeln in der folgenden Reihenfolge definieren, die für Unified Manager erforderlich sind, um ADFS-SAML-Antworten für diesen Vertrauenseintrag der vertrauenden Seite zu analysieren.

Anspruchsregel	Wert
SAM-Kontoname	Namens-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 die Authentifizierungsmethode auf „Formularauthentifizierung“ einstellen, da Benutzer sonst beim Abmelden von Unified Manager möglicherweise eine Fehlermeldung erhalten. Gehen Sie folgendermaßen vor:
  a. Öffnen Sie die ADFS-Verwaltungskonsole.
  b. Klicken Sie in der linken Baumansicht auf den Ordner „Authentifizierungsrichtlinien“.
  c. Klicken Sie rechts unter „Aktionen“ auf „Globale primäre Authentifizierungsrichtlinie bearbeiten“.
  d. Legen Sie die Intranet-Authentifizierungsmethode auf „Formularauthentifizierung“ statt auf die Standardeinstellung „Windows-Authentifizierung“ fest.
- In einigen Fällen wird die Anmeldung über den IdP abgelehnt, wenn das Sicherheitszertifikat des Unified Managers von einer Zertifizierungsstelle signiert ist. Es gibt zwei Problemumgehungen, um dieses Problem zu beheben:

- Befolgen Sie die Anweisungen im Link, um die Widerrufsprüfung auf dem ADFS-Server für die mit einem verketteten CA-Zertifikat verbundene vertrauende Partei zu deaktivieren:

  "Deaktivieren der Widerrufsprüfung pro Vertrauensstellung der vertrauenden Partei"

- Lassen Sie den CA-Server innerhalb des ADFS-Servers residieren, um die Zertifikatsanforderung des Unified Manager-Servers zu signieren.

Weitere Konfigurationsanforderungen

- Die Zeitabweichung des Unified Managers ist auf 5 Minuten eingestellt, sodass der Zeitunterschied zwischen dem IdP-Server und dem Unified Manager-Server nicht mehr als 5 Minuten betragen kann, da sonst die Authentifizierung fehlschlägt.

Aktivieren der SAML-Authentifizierung

Sie können die SAML-Authentifizierung (Security Assertion Markup Language) aktivieren, sodass Remotebenutzer von einem sicheren Identitätsanbieter (IdP) authentifiziert werden, bevor sie auf die Unified Manager-Web-Benutzeroberfläche zugreifen können.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung konfiguriert und überprüft haben, ob sie erfolgreich ist.
- Sie müssen mindestens einen Remote-Benutzer oder eine Remote-Gruppe mit der Rolle „Anwendungsadministrator“ erstellt haben.
- Der Identitätsanbieter (IdP) muss von Unified Manager unterstützt und konfiguriert werden.
- Sie müssen über die IdP-URL und Metadaten verfügen.
- Sie müssen Zugriff auf den IdP-Server haben.

Nachdem Sie die SAML-Authentifizierung von Unified Manager aktiviert haben, können Benutzer erst auf die grafische Benutzeroberfläche zugreifen, wenn der IdP mit den Hostinformationen des Unified Manager-Servers konfiguriert wurde. Sie müssen also darauf vorbereitet sein, beide Teile der Verbindung abzuschließen, bevor Sie mit dem Konfigurationsprozess beginnen. Der IdP kann vor oder nach der Konfiguration von Unified Manager konfiguriert werden.

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 Wartungskonsole, die Unified Manager-Befehle oder ZAPIs zugreifen.

Unified Manager wird automatisch neu gestartet, nachdem Sie die SAML-Konfiguration auf dieser Seite abgeschlossen haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **SAML-Authentifizierung**.
2. Aktivieren Sie das Kontrollkästchen **SAML-Authentifizierung aktivieren**.

   Die zum Konfigurieren der IdP-Verbindung erforderlichen Felder werden angezeigt.

3. Geben Sie die IdP-URI und die IdP-Metadaten ein, die zum Verbinden des Unified Manager-Servers mit dem IdP-Server erforderlich sind.

Wenn der IdP-Server direkt vom Unified Manager-Server aus zugänglich ist, können Sie nach Eingabe der IdP-URI auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um das Feld „IdP-Metadaten“ automatisch auszufüllen.

4. Kopieren Sie die URI der Hostmetadaten von Unified Manager oder speichern Sie die Hostmetadaten in einer XML-Textdatei.

   Mit diesen Informationen können Sie den IdP-Server jetzt konfigurieren.

5. Klicken Sie auf **Speichern**.

   In einem Meldungsfeld können Sie bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

6. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der IdP-Anmeldeseite statt auf der Unified Manager-Anmeldeseite ein.

Greifen Sie, sofern noch nicht geschehen, auf Ihren IdP zu und geben Sie die URI und Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Wenn Sie ADFS als Ihren Identitätsanbieter verwenden, beachtet die Unified Manager-GUI das ADFS-Timeout nicht und funktioniert weiter, bis das Unified Manager-Sitzungstimeout erreicht ist. Sie können das GUI-Sitzungstimeout ändern, indem Sie auf **Allgemein** > **Funktionseinstellungen** > **Inaktivitätstimeout** klicken.

Ändern Sie den für die SAML-Authentifizierung verwendeten Identitätsanbieter

Sie können den Identitätsanbieter (IdP) ändern, den Unified Manager zur Authentifizierung von Remotebenutzern verwendet.

Bevor Sie beginnen

- Sie müssen über die IdP-URL und Metadaten verfügen.
- Sie müssen Zugriff auf den IdP haben.

Der neue IdP kann vor oder nach der Konfiguration von Unified Manager konfiguriert werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **SAML-Authentifizierung**.
2. Geben Sie die neue IdP-URI und die IdP-Metadaten ein, die zum Verbinden des Unified Manager-Servers mit dem IdP erforderlich sind.

   Wenn der IdP direkt vom Unified Manager-Server aus zugänglich ist, können Sie nach Eingabe der IdP-URL auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um das Feld „IdP-Metadaten“ automatisch auszufüllen.

3. Kopieren Sie die Metadaten-URI des Unified Managers oder speichern Sie die Metadaten in einer XML-Textdatei.
4. Klicken Sie auf **Konfiguration speichern**.

Zur Bestätigung, dass Sie die Konfiguration ändern möchten, wird ein Meldungsfeld angezeigt.

5. Klicken Sie auf **OK**.

Greifen Sie auf den neuen IdP zu und geben Sie die URI und Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der neuen IdP-Anmeldeseite statt auf der alten IdP-Anmeldeseite ein.

Aktualisieren Sie die SAML-Authentifizierungseinstellungen nach der Änderung des Unified Manager-Sicherheitszertifikats

Jede Änderung am auf dem Unified Manager-Server installierten HTTPS-Sicherheitszertifikat erfordert eine Aktualisierung der Konfigurationseinstellungen der SAML-Authentifizierung. Das Zertifikat wird aktualisiert, wenn Sie das Hostsystem umbenennen, dem Hostsystem eine neue IP-Adresse zuweisen oder das Sicherheitszertifikat für das System manuell ändern.

Nachdem das Sicherheitszertifikat geändert und der Unified Manager-Server neu gestartet wurde, funktioniert die SAML-Authentifizierung nicht und Benutzer können nicht auf die grafische Benutzeroberfläche von Unified Manager zugreifen. Sie müssen die SAML-Authentifizierungseinstellungen sowohl auf dem IdP-Server als auch auf dem Unified Manager-Server aktualisieren, um den Zugriff auf die Benutzeroberfläche wieder zu aktivieren.

Schritte

1. Melden Sie sich bei der Wartungskonsole an.
2. Geben Sie im **Hauptmenü** die Nummer für die Option **SAML-Authentifizierung deaktivieren** ein.

   Es wird eine Meldung angezeigt, in der Sie bestätigen müssen, dass Sie die SAML-Authentifizierung deaktivieren und Unified Manager neu starten möchten.

3. Starten Sie die Unified Manager-Benutzeroberfläche mit dem aktualisierten FQDN oder der aktualisierten IP-Adresse, akzeptieren Sie das aktualisierte Serverzertifikat in Ihrem Browser und melden Sie sich mit den Anmeldeinformationen des Wartungsbenutzers an.
4. Wählen Sie auf der Seite **Setup/Authentifizierung** die Registerkarte **SAML-Authentifizierung** und konfigurieren Sie die IdP-Verbindung.
5. Kopieren Sie die URI der Hostmetadaten von Unified Manager oder speichern Sie die Hostmetadaten in einer XML-Textdatei.
6. Klicken Sie auf **Speichern**.

   In einem Meldungsfeld können Sie bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

7. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.
8. Greifen Sie auf Ihren IdP-Server zu und geben Sie die URI und Metadaten des Unified Manager-Servers ein, um die Konfiguration abzuschließen.

Identitätsanbieter	Konfigurationsschritte
ADFS	a. Löschen Sie den vorhandenen Vertrauenseintrag der vertrauenden Seite in der ADFS-Verwaltungs-GUI. b. Fügen Sie einen neuen Vertrauenseintrag der vertrauenden Partei hinzu, indem Sie `saml_sp_metadata.xml` vom aktualisierten Unified Manager-Server. c. Definieren Sie die drei Anspruchsregeln, die Unified Manager benötigt, um ADFS-SAML-Antworten für diesen Vertrauenseintrag der vertrauenden Seite zu analysieren. d. Starten Sie den ADFS-Windows-Dienst neu.
Shibboleth	a. Aktualisieren Sie den neuen FQDN des Unified Manager-Servers in `attribute-filter.xml` Und `relying-party.xml` Dateien. b. Starten Sie den Apache Tomcat-Webserver neu und warten Sie, bis Port 8005 online ist.

9. Melden Sie sich bei Unified Manager an und überprüfen Sie, ob die SAML-Authentifizierung über Ihren IdP wie erwartet funktioniert.

Deaktivieren der SAML-Authentifizierung

Sie können die SAML-Authentifizierung deaktivieren, wenn Sie die Authentifizierung von Remotebenutzern über einen sicheren Identitätsanbieter (IdP) beenden möchten, bevor sie sich bei der Unified Manager-Web-Benutzeroberfläche anmelden können. Wenn die SAML-Authentifizierung deaktiviert ist, führen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP die Anmeldeauthentifizierung durch.

Nachdem Sie die SAML-Authentifizierung deaktiviert haben, können neben konfigurierten Remote-Benutzern auch lokale Benutzer und Wartungsbenutzer auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch über die Unified Manager-Wartungskonsole deaktivieren, wenn Sie keinen Zugriff auf die grafische Benutzeroberfläche haben.

Unified Manager wird automatisch neu gestartet, nachdem die SAML-Authentifizierung deaktiviert wurde.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **SAML-Authentifizierung**.
2. Deaktivieren Sie das Kontrollkästchen **SAML-Authentifizierung aktivieren**.
3. Klicken Sie auf **Speichern**.

   In einem Meldungsfeld können Sie bestätigen, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

4. Klicken Sie auf **Bestätigen und Abmelden** und Unified Manager wird neu gestartet.

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der Anmeldeseite von Unified Manager statt auf der Anmeldeseite des IdP ein.

Greifen Sie auf Ihren IdP zu und löschen Sie die URI und Metadaten des Unified Manager-Servers.

Deaktivieren Sie die SAML-Authentifizierung über die Wartungskonsole

Möglicherweise müssen Sie die SAML-Authentifizierung über die Wartungskonsole deaktivieren, wenn kein Zugriff auf die Unified Manager-GUI besteht. Dies kann bei Fehlkonfigurationen oder wenn der IdP nicht erreichbar ist, passieren.

Bevor Sie beginnen

Sie müssen als Wartungsbenutzer Zugriff auf die Wartungskonsole haben.

Wenn die SAML-Authentifizierung deaktiviert ist, führen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP die Anmeldeauthentifizierung durch. Neben konfigurierten Remote-Benutzern können auch lokale Benutzer und Wartungsbenutzer auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch auf der Seite „Setup/Authentifizierung“ in der Benutzeroberfläche deaktivieren.

Unified Manager wird automatisch neu gestartet, nachdem die SAML-Authentifizierung deaktiviert wurde.

Schritte

1. Melden Sie sich bei der Wartungskonsole an.
2. Geben Sie im **Hauptmenü** die Nummer für die Option **SAML-Authentifizierung deaktivieren** ein.

   Es wird eine Meldung angezeigt, in der Sie bestätigen müssen, dass Sie die SAML-Authentifizierung deaktivieren und Unified Manager neu starten möchten.

3. Geben Sie **y** ein und drücken Sie dann die Eingabetaste. Unified Manager wird neu gestartet.

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche von Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der Anmeldeseite von Unified Manager statt auf der Anmeldeseite des IdP ein.

Greifen Sie bei Bedarf auf Ihren IdP zu und löschen Sie die URL und Metadaten des Unified Manager-Servers.

SAML-Authentifizierungsseite

Sie können die Seite „SAML-Authentifizierung“ verwenden, um Unified Manager so zu konfigurieren, dass Remote-Benutzer mithilfe von SAML über einen sicheren Identitätsanbieter (IdP) authentifiziert werden, bevor sie sich bei der Web-Benutzeroberfläche von Unified Manager anmelden können.

- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen, um die SAML-Konfiguration zu erstellen oder zu ändern.

- Sie müssen die Remote-Authentifizierung konfiguriert haben.
- Sie müssen mindestens einen Remote-Benutzer oder eine Remote-Gruppe konfiguriert haben.

Nachdem die Remote-Authentifizierung und die Remote-Benutzer konfiguriert wurden, können Sie das Kontrollkästchen SAML-Authentifizierung aktivieren aktivieren, um die Authentifizierung mithilfe eines sicheren Identitätsanbieters zu 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 zugänglich ist, können Sie auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um dieses Feld auszufüllen.

- **Hostsystem (FQDN)**

  Der FQDN des Unified Manager-Hostsystems, wie während der Installation definiert. 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.

Verwalten der Authentifizierung

Sie können die Authentifizierung entweder mit LDAP oder Active Directory auf dem Unified Manager-Server aktivieren und so konfigurieren, dass sie mit Ihren Servern zur Authentifizierung von Remotebenutzern zusammenarbeitet.

Informationen zum Aktivieren der Remote-Authentifizierung, Einrichten von Authentifizierungsdiensten und Hinzufügen von Authentifizierungsservern finden Sie im vorherigen Abschnitt zum **Konfigurieren von Unified Manager zum Senden von Warnbenachrichtigungen**.

Authentifizierungsserver bearbeiten

Sie können den Port ändern, den der Unified Manager-Server zur Kommunikation mit Ihrem Authentifizierungsserver verwendet.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Aktivieren Sie das Kontrollkästchen **Verschachtelte Gruppensuche deaktivieren**.
3. Wählen Sie im Bereich **Authentifizierungsserver** den Authentifizierungsserver aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
4. Bearbeiten Sie im Dialogfeld **Authentifizierungsserver bearbeiten** die Portdetails.
5. Klicken Sie auf **Speichern**.

Authentifizierungsserver 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 müssen über die Rolle „Anwendungsadministrator“ verfügen.

Wenn Sie einen Authentifizierungsserver löschen, können Remotebenutzer oder Gruppen des Authentifizierungsservers nicht mehr auf Unified Manager zugreifen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Wählen Sie einen oder mehrere Authentifizierungsserver aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie auf **Ja**, um die Löschanforderung zu bestätigen.

   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

Sie können die Remote-Authentifizierung auf dem Verwaltungsserver aktivieren und den Verwaltungsserver für die Kommunikation mit Ihren Authentifizierungsservern konfigurieren, sodass Benutzer innerhalb der Authentifizierungsserver auf Unified Manager zugreifen können.

Sie können einen der folgenden vordefinierten Authentifizierungsdienste verwenden oder Ihren eigenen Authentifizierungsdienst angeben:

- Microsoft Active Directory

  Sie können Microsoft Lightweight Directory Services nicht verwenden.

- OpenLDAP

Sie können den erforderlichen Authentifizierungsdienst auswählen und die entsprechenden Authentifizierungsserver hinzufügen, um den Remotebenutzern im Authentifizierungsserver den Zugriff auf Unified Manager zu ermöglichen. Die Anmeldeinformationen für Remotebenutzer oder -gruppen werden vom Authentifizierungsserver verwaltet. Der Verwaltungsserver verwendet das Lightweight Directory Access Protocol (LDAP), um Remotebenutzer innerhalb des konfigurierten Authentifizierungsservers zu authentifizieren.

Für lokale Benutzer, die in Unified Manager erstellt werden, verwaltet der Verwaltungsserver eine eigene Datenbank mit Benutzernamen und Kennwörtern. Der Verwaltungsserver führt die Authentifizierung durch und verwendet weder Active Directory noch OpenLDAP zur Authentifizierung.

Überwachungsprotokollierung

Mithilfe von Audit-Protokollen können Sie feststellen, ob die Audit-Protokolle kompromittiert wurden. Alle von einem Benutzer ausgeführten Aktivitäten werden überwacht und in den Prüfprotokollen protokolliert. Die Audits werden für alle Benutzeroberflächen- und öffentlich zugänglichen API-Funktionen von Active IQ Unified Manager durchgeführt.

Sie können die **Audit-Protokolldateiansicht** verwenden, um alle in Ihrem Active IQ Unified Manager verfügbaren Audit-Protokolldateien anzuzeigen und darauf zuzugreifen. Die Dateien im Audit-Protokoll: Dateiansicht werden basierend auf ihrem Erstellungsdatum aufgelistet. Diese Ansicht zeigt Informationen zu allen Prüfprotokollen an, die seit der Installation oder Aktualisierung bis zum aktuellen Stand im System erfasst wurden. Immer wenn Sie eine Aktion in Unified Manager ausführen, werden die Informationen aktualisiert und sind in den Protokollen verfügbar. Der Status jeder Protokolldatei wird mithilfe des Attributs „Dateiintegritätsstatus“ erfasst, das aktiv überwacht wird, um Manipulationen oder Löschungen der Protokolldatei zu erkennen. Die Audit-Protokolle können einen der folgenden Zustände aufweisen, wenn die Audit-Protokolle im System verfügbar sind:

Status	Beschreibung
AKTIV	Datei, in der aktuell Protokolle protokolliert werden.
NORMAL	Datei, die inaktiv, komprimiert und im System gespeichert ist.
MANIPULIERT	Datei, die von einem Benutzer kompromittiert wurde, der die Datei manuell bearbeitet hat.
MANUAL_DELETE	Datei, die von einem autorisierten Benutzer gelöscht wurde.
ROLLOVER_DELETE	Datei, die aufgrund des Rolling-Offs basierend auf der Rolling-Konfigurationsrichtlinie gelöscht wurde.

Status	Beschreibung
UNEXPECTED_DELETE	Datei, die aus unbekannten Gründen gelöscht wurde.

Die Seite „Audit-Protokoll“ enthält die folgenden Befehlsschaltflächen:

- Konfigurieren
- Löschen
- Download

Mit der Schaltfläche **LÖSCHEN** können Sie alle in der Ansicht „Auditprotokolle“ aufgeführten Auditprotokolle löschen. Sie können ein Prüfprotokoll löschen und optional einen Grund für das Löschen der Datei angeben, der in Zukunft dabei hilft, eine gültige Löschung festzustellen. In der Spalte REASON werden der Grund sowie der Name des Benutzers aufgeführt, der den Löschvorgang durchgeführt hat.

Das Löschen einer Protokolldatei führt zum Löschen der Datei aus dem System, der Eintrag in der DB-Tabelle wird jedoch nicht gelöscht.

Sie können die Prüfprotokolle von Active IQ Unified Manager mithilfe der Schaltfläche **HERUNTERLADEN** im Abschnitt „Prüfprotokolle“ herunterladen und die Prüfprotokolldateien exportieren. Die Dateien, die mit „`NORMAL`“ oder „`TAMPERED`“ gekennzeichnet sind, werden in einer komprimierten `.gzip` Format.

Die Audit-Protokolldateien werden regelmäßig archiviert und zur Referenz in der Datenbank gespeichert. Vor der Archivierung werden die Prüfprotokolle zur Wahrung der Sicherheit und Integrität digital signiert.

Wenn ein vollständiges AutoSupport Paket generiert wird, enthält das Support-Paket sowohl archivierte als auch aktive Prüfprotokolldateien. Wenn jedoch ein Light-Support-Paket generiert wird, enthält es nur die aktiven Prüfprotokolle. Die archivierten Audit-Protokolle sind nicht enthalten.

Konfigurieren von Überwachungsprotokollen

Sie können die Schaltfläche **Konfigurieren** im Abschnitt „Audit-Protokolle“ verwenden, um die fortlaufende Richtlinie für Audit-Protokolldateien zu konfigurieren und auch die Remote-Protokollierung für die Audit-Protokolle zu aktivieren.

Sie können die Werte für **MAXIMALE DATEIGRÖSSE** und **AUFBEWAHRUNGSTAGE DES PRÜFPROTOKOLLS** entsprechend der gewünschten Menge und Häufigkeit der Daten festlegen, die Sie im System speichern möchten. Der Wert im Feld **TOTAL AUDIT LOG SIZE** ist die Größe der gesamten im System vorhandenen Audit-Protokolldaten. Die Rollover-Richtlinie wird durch die Werte in den Feldern **AUFBEWAHRUNGSZEIT DES AUDIT-LOGS**, **MAXIMALE DATEIGRÖSSE** und **GESAMTGRÖSSE DES AUDIT-LOGS** bestimmt. Wenn die Größe der Audit-Protokollsicherung den in **TOTAL AUDIT LOG SIZE** konfigurierten Wert erreicht, wird die zuerst archivierte Datei gelöscht. Dies bedeutet, dass die älteste Datei gelöscht wird. Der Dateieintrag ist jedoch weiterhin in der Datenbank vorhanden und mit „Rollover Delete“ gekennzeichnet. Der Wert **AUFBEWAHRUNGSTAGE DES AUDIT-LOGS** gibt die Anzahl der Tage an, die die Audit-Log-Dateien aufbewahrt werden. Alle Dateien, die älter sind als der in diesem Feld festgelegte Wert, werden übernommen.

Schritte

1. Klicken Sie auf **Audit-Protokolle** > > **Konfigurieren**.
2. Geben Sie Werte für **MAXIMALE DATEIGRÖSSE**, **GESAMTGRÖSSE DES AUDIT-PROTOKOLLS** und **AUFBEWAHRUNGSTAGE DES AUDIT-PROTOKOLLS** ein.

Wenn Sie die Remote-Protokollierung aktivieren möchten, sollten Sie **Remote-Protokollierung aktivieren** auswählen. /// 2025-6-11, OTHERDOC-133

Aktivieren der Remote-Protokollierung von Überwachungsprotokollen

Sie können das Kontrollkästchen **Remote-Protokollierung aktivieren** im Dialogfeld „Audit-Protokolle konfigurieren“ aktivieren, um die Remote-Audit-Protokollierung zu aktivieren. Mit dieser Funktion können Sie Überwachungsprotokolle auf einen Remote-Syslog-Server übertragen. Auf diese Weise können Sie Ihre Prüfprotokolle verwalten, wenn der Speicherplatz begrenzt ist.

Die Remote-Protokollierung von Prüfprotokollen bietet eine manipulationssichere Sicherung für den Fall, dass die Prüfprotokolldateien auf dem Active IQ Unified Manager Server manipuliert werden.

Schritte

1. Aktivieren Sie im Dialogfeld **Auditprotokolle konfigurieren** das Kontrollkästchen **Remoteprotokollierung aktivieren**.

   Es werden zusätzliche Felder zum Konfigurieren der Remote-Protokollierung angezeigt.

2. Geben Sie den **HOSTNAME** und **PORT** des Remote-Servers ein, zu dem Sie eine Verbindung herstellen möchten.
3. Klicken Sie im Feld **SERVER CA CERTIFICATE** auf **BROWSE**, um ein öffentliches Zertifikat des Zielservers auszuwählen.

   Das Zertifikat sollte hochgeladen werden in `.pem` Format. Dieses Zertifikat sollte vom Ziel-Syslog-Server bezogen werden und nicht abgelaufen sein. Das Zertifikat sollte den ausgewählten „Hostnamen“ als Teil des `SubjectAltName` (SAN)-Attribut.

4. Geben Sie die Werte für die folgenden Felder ein: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   Die Werte für diese Felder sollten in Millisekunden angegeben werden.

5. Wählen Sie in den Feldern **FORMAT** und **PROTOKOLL** das gewünschte Syslog-Format und die TLS-Protokollversion aus.
6. Aktivieren Sie das Kontrollkästchen **Client-Authentifizierung aktivieren**, wenn der Ziel-Syslog-Server eine zertifikatbasierte Authentifizierung erfordert.

   Sie müssen das Client-Authentifizierungszertifikat herunterladen und auf den Syslog-Server hochladen, bevor Sie die Audit-Log-Konfiguration speichern, da sonst die Verbindung fehlschlägt. Je nach Typ des Syslog-Servers müssen Sie möglicherweise einen Hash des Client-Authentifizierungszertifikats erstellen.

   Beispiel: syslog-ng erfordert einen <hash> des Zertifikats, das mit dem Befehl erstellt werden soll `openssl x509 -noout -hash -in cert.pem` , und dann sollten Sie das Client-Authentifizierungszertifikat symbolisch mit einer Datei verknüpfen, die nach dem <Hash> .0 benannt ist.

7. Klicken Sie auf **Speichern**, um die Verbindung mit Ihrem Server zu konfigurieren und die Remote-Protokollierung zu aktivieren.

   Sie werden zur Seite „Audit-Protokolle“ weitergeleitet.

Der Wert **Verbindungs-Timeout** kann die Konfiguration beeinflussen. Wenn die Konfiguration länger als der definierte Wert zum Antworten benötigt, kann dies aufgrund eines Verbindungsfehlers zu einem Konfigurationsfehler führen. Um eine erfolgreiche Verbindung herzustellen, erhöhen Sie den Wert **Verbindungs-Timeout** und versuchen Sie die Konfiguration erneut.

Seite „Remote-Authentifizierung“

Sie können die Seite „Remote-Authentifizierung“ verwenden, um Unified Manager für die Kommunikation mit Ihrem Authentifizierungsserver zu konfigurieren, um Remote-Benutzer zu authentifizieren, die versuchen, sich bei der Unified Manager-Web-Benutzeroberfläche anzumelden.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Nachdem Sie das Kontrollkästchen „Remote-Authentifizierung aktivieren“ aktiviert haben, können Sie die Remote-Authentifizierung mithilfe eines Authentifizierungsservers aktivieren.

- **Authentifizierungsdienst**

  Ermöglicht Ihnen, den Verwaltungsserver so zu konfigurieren, dass Benutzer bei Verzeichnisdienstanbietern wie Active Directory oder OpenLDAP authentifiziert werden, oder Ihren eigenen Authentifizierungsmechanismus anzugeben. Sie können einen Authentifizierungsdienst nur angeben, wenn Sie die Remote-Authentifizierung aktiviert haben.

  - **Active Directory**
    - Administratorname

      Gibt den Administratornamen des Authentifizierungsservers an.

    - Passwort

      Gibt das Kennwort für den Zugriff auf den Authentifizierungsserver an.

    - Basis-Distinguished Name

      Gibt den Standort der Remote-Benutzer im Authentifizierungsserver an. Wenn der Domänenname des Authentifizierungsservers beispielsweise ou@domain.com lautet, dann ist der Basis-Distinguished Name **cn=ou,dc=domain,dc=com**.

    - Verschachtelte Gruppensuche deaktivieren

      Gibt an, ob die Option zur Suche verschachtelter Gruppen aktiviert oder deaktiviert werden soll. Standardmäßig ist diese Option deaktiviert. Wenn Sie Active Directory verwenden, 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**
  - Definierter Name binden

    Gibt den Bind-Distinguished Name an, der zusammen mit dem Basis-Distinguished Name verwendet wird, um Remotebenutzer im Authentifizierungsserver zu finden.

  - Bind-Passwort

    Gibt das Kennwort für den Zugriff auf den Authentifizierungsserver an.

  - Basis-Distinguished Name

    Gibt den Standort der Remote-Benutzer im Authentifizierungsserver an. Wenn der Domänenname des Authentifizierungsservers beispielsweise ou@domain.com lautet, dann ist der Basis-Distinguished Name **cn=ou,dc=domain,dc=com**.

  - Sichere Verbindung verwenden

    Gibt an, dass Secure LDAP für die Kommunikation mit LDAP-Authentifizierungsservern verwendet wird.

- **Andere**
  - Definierter Name binden

    Gibt den Bind-Distinguished Name an, der zusammen mit dem Basis-Distinguished Name verwendet wird, um Remotebenutzer auf dem von Ihnen konfigurierten Authentifizierungsserver zu finden.

  - Bind-Passwort

    Gibt das Kennwort für den Zugriff auf den Authentifizierungsserver an.

  - Basis-Distinguished Name

    Gibt den Standort der Remote-Benutzer im Authentifizierungsserver an. Wenn der Domänenname des Authentifizierungsservers beispielsweise ou@domain.com lautet, dann ist der Basis-Distinguished Name **cn=ou,dc=domain,dc=com**.

  - Protokollversion

    Gibt die von Ihrem Authentifizierungsserver unterstützte Version des Lightweight Directory Access Protocol (LDAP) an. Sie können festlegen, ob die Protokollversion automatisch erkannt werden soll oder die Version auf 2 oder 3 einstellen.

  - Benutzernamenattribut

    Gibt den Namen des Attributs im Authentifizierungsserver an, das die Benutzeranmeldenamen enthält, die vom Verwaltungsserver authentifiziert werden sollen.

  - Gruppenmitgliedschaftsattribut

    Gibt einen Wert an, der Remotebenutzern die Mitgliedschaft in der Management-Server-Gruppe basierend auf einem Attribut und 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 Gruppenmitgliedschaft des Verwaltungsservers basierend auf einem angegebenen Attribut in diesem GroupOfUniqueNames-Objekt zuweisen.

- Verschachtelte Gruppensuche deaktivieren

  Gibt an, ob die Option zur Suche verschachtelter Gruppen aktiviert oder deaktiviert werden soll. Standardmäßig ist diese Option deaktiviert. Wenn Sie Active Directory verwenden, können Sie die Authentifizierung beschleunigen, indem Sie die Unterstützung für verschachtelte Gruppen deaktivieren.

- Mitglied

  Gibt den Attributnamen an, den Ihr Authentifizierungsserver zum Speichern von Informationen über die einzelnen Mitglieder einer Gruppe verwendet.

- Benutzerobjektklasse

  Gibt die Objektklasse eines Benutzers im Remote-Authentifizierungsserver an.

- Gruppenobjektklasse

  Gibt die Objektklasse aller Gruppen im Remote-Authentifizierungsserver an.

  Die Werte, die Sie für die Attribute *Member*, *User Object Class* und *Group Object Class* eingeben, sollten mit denen übereinstimmen, die Sie in Ihren Active Directory-, OpenLDAP- und LDAP-Konfigurationen hinzugefügt haben. Andernfalls kann die Authentifizierung fehlschlagen.

- Sichere Verbindung verwenden

  Gibt den Authentifizierungsdienst an, der für die Kommunikation mit Authentifizierungsservern verwendet wird.

Wenn Sie den Authentifizierungsdienst ändern möchten, stellen Sie sicher, dass Sie alle vorhandenen Authentifizierungsserver löschen und neue Authentifizierungsserver hinzufügen.

Bereich „Authentifizierungsserver“

Im Bereich „Authentifizierungsserver“ werden die Authentifizierungsserver angezeigt, mit denen der Verwaltungsserver kommuniziert, um Remotebenutzer zu finden und zu authentifizieren. Die Anmeldeinformationen für Remotebenutzer oder -gruppen werden vom Authentifizierungsserver verwaltet.

- **Befehlsschaltflächen**

  Ermöglicht Ihnen das Hinzufügen, Bearbeiten oder Löschen von Authentifizierungsservern.

  - Hinzufügen

    Ermöglicht Ihnen, einen Authentifizierungsserver hinzuzufügen.

Wenn der Authentifizierungsserver, den Sie hinzufügen, Teil eines Hochverfügbarkeitspaars ist (das dieselbe Datenbank verwendet), können Sie auch den Partnerauthentifizierungsserver hinzufügen. Dadurch kann der Verwaltungsserver mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

  - Bearbeiten

    Ermöglicht Ihnen, die Einstellungen für einen ausgewählten Authentifizierungsserver zu 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 Verwaltungsserver verwendet wird.

- **Hafen**

  Zeigt die Portnummer des Authentifizierungsservers an.

- **Authentifizierung testen**

  Diese Schaltfläche validiert die Konfiguration Ihres Authentifizierungsservers durch Authentifizierung eines Remotebenutzers oder einer Remotegruppe.

  Wenn Sie beim Testen nur den Benutzernamen angeben, sucht der Verwaltungsserver im Authentifizierungsserver nach dem Remotebenutzer, authentifiziert den Benutzer jedoch nicht. Wenn Sie sowohl den Benutzernamen als auch das Kennwort angeben, sucht und authentifiziert der Verwaltungsserver den Remotebenutzer.

  Sie können die Authentifizierung nicht testen, wenn die Remote-Authentifizierung deaktiviert ist.

Sicherheitszertifikate verwalten

Sie können HTTPS im Unified Manager-Server konfigurieren, um Ihre Cluster über eine sichere Verbindung zu überwachen und zu verwalten.

Zeigen Sie das HTTPS-Sicherheitszertifikat an

Sie können die HTTPS-Zertifikatdetails 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 müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Durch Anzeigen des Zertifikats können Sie den Inhalt eines neu generierten Zertifikats überprüfen oder Subject Alt Names (SAN) anzeigen, von denen aus Sie auf Unified Manager zugreifen können.

Schritt

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.

   Das HTTPS-Zertifikat wird oben auf der Seite angezeigt

Wenn Sie ausführlichere Informationen zum Sicherheitszertifikat benötigen als die, die auf der Seite „HTTPS-Zertifikat“ angezeigt werden, können Sie das Verbindungszertifikat in Ihrem Browser anzeigen.

Laden Sie eine HTTPS-Zertifikatsignieranforderung herunter

Sie können eine Zertifizierungssignaturanforderung für das aktuelle HTTPS-Sicherheitszertifikat herunterladen, sodass Sie die Datei einer Zertifizierungsstelle zur Signierung vorlegen können. Ein von einer Zertifizierungsstelle signiertes Zertifikat trägt dazu bei, Man-in-the-Middle-Angriffe zu verhindern und bietet einen besseren Sicherheitsschutz als ein selbstsigniertes Zertifikat.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikatsignieranforderung herunterladen**.
3. Speichern Sie die `<hostname>.csr` Datei.

Sie können die Datei einer Zertifizierungsstelle zur Signierung vorlegen und anschließend das signierte Zertifikat installieren.

Installieren Sie ein von einer CA signiertes und zurückgegebenes HTTPS-Zertifikat

Sie können ein Sicherheitszertifikat hochladen und installieren, nachdem es von einer Zertifizierungsstelle signiert und zurückgegeben wurde. Die Datei, die Sie hochladen und installieren, muss eine signierte Version des vorhandenen selbstsignierten Zertifikats sein. Ein von einer Zertifizierungsstelle signiertes Zertifikat trägt dazu bei, Man-in-the-Middle-Angriffe zu verhindern und bietet einen besseren Sicherheitsschutz als ein selbstsigniertes Zertifikat.

*Was .Bevor Sie beginnen

Sie müssen die folgenden Aktionen abgeschlossen haben:

- Die Certificate Signing Request-Datei heruntergeladen und von einer Zertifizierungsstelle signieren lassen
- Die Zertifikatskette wurde im PEM-Format gespeichert
- Alle Zertifikate in der Kette eingeschlossen, vom Unified Manager-Serverzertifikat bis zum Stammsignaturzertifikat, einschließlich aller vorhandenen Zwischenzertifikate

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Wenn die Gültigkeit des Zertifikats, für das ein CSR erstellt wurde, mehr als 397 Tage beträgt, wird die Gültigkeit von der Zertifizierungsstelle vor der Unterzeichnung und Rücksendung des Zertifikats auf 397 Tage verkürzt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **HTTPS-Zertifikat**.
2. Klicken Sie auf **HTTPS-Zertifikat installieren**.
3. Klicken Sie im angezeigten Dialogfeld auf **Datei auswählen…**, um die hochzuladende Datei zu suchen.
4. Wählen Sie die Datei aus und klicken Sie dann auf **Installieren**, um die Datei zu installieren.

   Weitere Informationen finden Sie unter"Installieren 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-----
```

Installieren Sie ein mit externen Tools generiertes HTTPS-Zertifikat

Sie können selbstsignierte oder von einer Zertifizierungsstelle signierte Zertifikate installieren, die mit einem externen Tool wie OpenSSL, BoringSSL oder LetsEncrypt generiert wurden.

Sie sollten den privaten Schlüssel zusammen mit der Zertifikatskette laden, da es sich bei diesen Zertifikaten um extern generierte öffentlich-private Schlüsselpaare handelt. Die zulässigen Schlüsselpaar-Algorithmen sind „RSA“ und „EC“. Die Option **HTTPS-Zertifikat installieren** ist auf der Seite „HTTPS-Zertifikate“ im Abschnitt „Allgemein“ verfügbar. Die Datei, die Sie hochladen, sollte das folgende Eingabeformat haben.

1. Privater Schlüssel des Servers, der zum Active IQ Unified Manager Host gehört
2. Zertifikat des Servers, das zum privaten Schlüssel passt
3. Zertifikat der CAs in umgekehrter Reihenfolge bis zur Wurzel, die zum Signieren des obigen Zertifikats verwendet werden

Format zum Laden eines Zertifikats mit einem EC-Schlüsselpaar

Die zulässigen Kurven sind „prime256v1“ und „secp384r1“. Musterzertifikat mit extern generiertem 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 Schlüsselgrößen 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-----
```

Nachdem das Zertifikat hochgeladen wurde, sollten Sie die Active IQ Unified Manager Instanz neu starten, damit die Änderungen wirksam werden.

Prüfungen beim Hochladen extern erstellter Zertifikate

Das System führt beim Hochladen eines mit externen Tools erstellten Zertifikats Prüfungen durch. Wenn eine der Prüfungen fehlschlägt, wird das Zertifikat abgelehnt. Es ist auch eine Validierung für die Zertifikate enthalten, die aus der CSR innerhalb des Produkts generiert werden, und für Zertifikate, die mit externen Tools generiert werden.

- Der private Schlüssel in der Eingabe wird anhand des Host-Zertifikats in der Eingabe validiert.
- Der Common Name (CN) im Host-Zertifikat wird mit dem FQDN des Hosts abgeglichen.
- Der allgemeine Name (CN) des Hostzertifikats darf nicht leer sein und darf nicht auf „localhost“ gesetzt werden.
- Das Gültigkeitsbeginndatum sollte nicht in der Zukunft und das Gültigkeitsablaufdatum des Zertifikats nicht in der Vergangenheit liegen.
- Wenn eine Zwischenzertifizierungsstelle oder Zertifizierungsstelle vorhanden ist, darf das Gültigkeitsbeginndatum des Zertifikats nicht in der Zukunft und das Gültigkeitsablaufdatum nicht in der Vergangenheit liegen.

Der private Schlüssel in der Eingabe sollte nicht verschlüsselt sein. Wenn verschlüsselte private Schlüssel vorhanden sind, werden diese vom System abgelehnt.

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-----
```

Wenn die Installation des Zertifikats fehlschlägt, lesen Sie den folgenden Knowledge Base-Artikel (KB):https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager kann ein extern generiertes Zertifikat nicht installieren"^]

Seitenbeschreibungen zur Zertifikatsverwaltung

Auf der Seite „HTTPS-Zertifikat“ können Sie die aktuellen Sicherheitszertifikate anzeigen und neue HTTPS-Zertifikate generieren.

HTTPS-Zertifikatseite

Auf der Seite „HTTPS-Zertifikat“ können Sie das aktuelle Sicherheitszertifikat anzeigen, eine Zertifikatsignieranforderung herunterladen, ein neues selbstsigniertes HTTPS-Zertifikat generieren oder ein neues HTTPS-Zertifikat installieren.

Wenn Sie kein neues selbstsigniertes HTTPS-Zertifikat generiert haben, handelt es sich bei dem auf dieser Seite angezeigten Zertifikat um das Zertifikat, das während der Installation generiert wurde.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Vorgänge ausführen:

- **HTTPS-Zertifikatsignieranforderung herunterladen**

  Lädt eine Zertifizierungsanforderung für das aktuell installierte HTTPS-Zertifikat herunter. Ihr Browser fordert Sie auf, die Datei <hostname>.csr zu speichern, damit Sie die Datei einer Zertifizierungsstelle zum Signieren vorlegen können.

- **HTTPS-Zertifikat installieren**

  Ermöglicht Ihnen das Hochladen und Installieren eines Sicherheitszertifikats, nachdem es von einer Zertifizierungsstelle signiert und zurückgegeben wurde. Das neue Zertifikat ist nach dem Neustart des Verwaltungsservers wirksam.

- **HTTPS-Zertifikat neu generieren**

  Ermöglicht Ihnen, ein neues selbstsigniertes HTTPS-Zertifikat zu generieren, das das aktuelle Sicherheitszertifikat ersetzt. Das neue Zertifikat ist nach dem Neustart von Unified Manager wirksam.

Dialogfeld „HTTPS-Zertifikat neu generieren“

Im Dialogfeld „HTTPS-Zertifikat neu generieren“ können Sie die Sicherheitsinformationen anpassen und dann mit diesen Informationen ein neues HTTPS-Zertifikat generieren.

Auf dieser Seite werden die aktuellen Zertifikatsinformationen angezeigt.

Mit der Auswahl „Mithilfe der aktuellen Zertifikatsattribute neu generieren“ und „Aktualisieren der aktuellen Zertifikatsattribute“ können Sie das Zertifikat mit den aktuellen Informationen neu generieren oder ein Zertifikat mit neuen Informationen erstellen.

- **Allgemeiner Name**

  Erforderlich. Der vollqualifizierte Domänenname (FQDN), den Sie sichern möchten.

  Verwenden Sie in Hochverfügbarkeitskonfigurationen von Unified Manager die virtuelle IP-Adresse.

- **E-Mail**

Optional. Eine E-Mail-Adresse zur Kontaktaufnahme mit Ihrer Organisation; normalerweise die E-Mail-Adresse des Zertifikatadministrators oder der IT-Abteilung.

- **Unternehmen**

  Optional. Normalerweise der eingetragene Name Ihres Unternehmens.

- **Abteilung**

  Optional. Der Name der Abteilung in Ihrem Unternehmen.

- **Stadt**

  Optional. Der Stadtstandort Ihres Unternehmens.

- **Zustand**

  Optional. Der Bundesstaat oder die Provinz, in der sich Ihr Unternehmen befindet (nicht abgekürzt).

- **Land**

  Optional. Der Standort Ihres Unternehmens. Dies ist normalerweise ein zweistelliger ISO-Code des Landes.

- **Alternative Namen**

  Erforderlich. Zusätzliche, nicht primäre Domänennamen, die zusätzlich zu den vorhandenen Localhost- oder anderen Netzwerkadressen für den Zugriff auf diesen Server verwendet werden können. Trennen Sie jeden alternativen Namen durch ein Komma.

  Aktivieren Sie das Kontrollkästchen „Lokale Identifizierungsinformationen ausschließen (z. B. localhost)“, wenn Sie die lokalen Identifizierungsinformationen 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 dieses Feld leer gelassen wird, enthält das resultierende Zertifikat überhaupt kein Feld für alternative Namen.

- **SCHLÜSSELGRÖSSE (SCHLÜSSELALGORITHMUS: RSA)**

  Der Schlüsselalgorithmus ist auf RSA eingestellt. Sie können eine der Schlüsselgrößen auswählen: 2048, 3072 oder 4096 Bit. Die Standardschlüsselgröße ist auf 2048 Bit eingestellt.

- **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 finden Sie unter "Generieren von HTTPS-Zertifikaten".

Überwachen und Verwalten des Speichers

Einführung in Active IQ Unified Manager

Mit Active IQ Unified Manager (früher OnCommand Unified Manager) können Sie den Zustand und die Leistung Ihrer ONTAP -Speichersysteme über eine einzige Schnittstelle überwachen und verwalten.

Unified Manager bietet die folgenden Funktionen:

- Erkennung, Überwachung und Benachrichtigungen für Systeme, auf denen ONTAP -Software installiert ist.
- Dashboard zur Anzeige der Kapazität, Sicherheit und Leistungsintegrität der Umgebung.
- Verbesserte Warn-, Ereignis- und Schwellenwertinfrastruktur.
- Zeigt detaillierte Diagramme an, die die Workload-Aktivität im Zeitverlauf darstellen, einschließlich IOPS (Operationen), MBps (Durchsatz), Latenz (Reaktionszeit), Auslastung, Leistungskapazität und Cache-Verhältnis.
- Identifiziert Workloads, die Clusterkomponenten übermäßig beanspruchen, und die Workloads, deren Leistung durch die erhöhte Aktivität beeinträchtigt wird.
- Bietet Vorschläge für Korrekturmaßnahmen, die zur Behebung bestimmter Vorfälle und Ereignisse durchgeführt werden können, sowie für einige Ereignisse eine Schaltfläche „Fix It“, damit Sie das Problem sofort beheben können.
- Integriert sich mit OnCommand Workflow Automation , 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 Leistungs- und Speicherziele für die Benutzer zu definieren, die mit diesem Workload auf die Anwendung zugreifen.

Einführung in die Integritätsüberwachung von Active IQ Unified Manager

Active IQ Unified Manager (früher OnCommand Unified Manager) hilft Ihnen, eine große Anzahl von Systemen mit ONTAP -Software über eine zentrale Benutzeroberfläche zu überwachen. Die Unified Manager-Serverinfrastruktur bietet Skalierbarkeit, Supportfähigkeit und erweiterte Überwachungs- und Benachrichtigungsfunktionen.

Zu den wichtigsten Funktionen von Unified Manager gehören Überwachung, Alarmierung, Verwaltung der Verfügbarkeit und Kapazität von Clustern, Verwaltung von Schutzfunktionen sowie Bündelung und Übermittlung von Diagnosedaten an den technischen Support.

Sie können Unified Manager zur Überwachung Ihrer Cluster verwenden. Wenn im Cluster Probleme auftreten, benachrichtigt Sie Unified Manager über die Details dieser Probleme durch Ereignisse. Bei einigen Ereignissen stehen Ihnen auch Abhilfemaßnahmen zur Verfügung, mit denen Sie die Probleme beheben können. Sie können Warnmeldungen für Ereignisse konfigurieren, sodass Sie beim Auftreten von Problemen per E-Mail und SNMP-Traps benachrichtigt werden.

Sie können Unified Manager verwenden, um Speicherobjekte in Ihrer Umgebung zu verwalten, indem Sie sie mit Anmerkungen verknüpfen. Sie können benutzerdefinierte Anmerkungen erstellen und Cluster, virtuelle Speichermaschinen (SVMs) und Volumes mithilfe von Regeln dynamisch mit den Anmerkungen verknüpfen.

Sie können den Speicherbedarf Ihrer Clusterobjekte auch anhand der in den Kapazitäts- und

Integritätsdiagrammen für das jeweilige Clusterobjekt bereitgestellten Informationen planen.

Körperliche und logische Leistungsfähigkeit

Unified Manager nutzt die Konzepte des physischen und logischen Speicherplatzes, die für ONTAP Speicherobjekte verwendet werden.

- Physische Kapazität: Physischer Speicherplatz bezieht sich auf die im Datenträger verwendeten physischen Speicherblöcke. Die „physisch genutzte Kapazität“ ist aufgrund der Datenreduzierung durch Speichereffizienzfunktionen (wie Deduplizierung und Komprimierung) normalerweise kleiner als die logisch genutzte Kapazität.
- Logische Kapazität: Der logische Speicherplatz bezieht sich auf den nutzbaren Speicherplatz (die logischen Blöcke) in einem Volume. Der logische Speicherplatz bezieht sich darauf, wie der theoretische Speicherplatz genutzt werden kann, ohne die Ergebnisse der Deduplizierung oder Komprimierung zu berücksichtigen. Der „genutzte logische Speicherplatz“ ist der genutzte physische Speicherplatz zuzüglich der Einsparungen durch konfigurierte Speichereffizienzfunktionen (wie Deduplizierung und Komprimierung). Dieser Messwert erscheint häufig größer als die physisch genutzte Kapazität, da er die Datenkomprimierung und andere Reduzierungen des physischen Speicherplatzes nicht berücksichtigt. Daher kann die gesamte logische Kapazität höher sein als der bereitgestellte Speicherplatz.

Kapazitätsmesseinheiten

Unified Manager berechnet die Speicherkapazität basierend auf Binäreinheiten von 1024 (2^{10}) Bytes. In ONTAP 9.10.0 und früher wurden diese Einheiten als KB, MB, GB, TB und PB angezeigt. Ab ONTAP 9.10.1 werden sie im Unified Manager als KiB, MiB, GiB, TiB und PiB angezeigt.

Die für den Durchsatz verwendeten Einheiten sind für alle Versionen von ONTAP weiterhin Kilobyte pro Sekunde (Kbps), Megabyte pro Sekunde (Mbps), Gigabyte pro Sekunde (Gbps) oder Terabyte pro Sekunde (Tbps) usw.

Kapazitätseinheit, die im Unified Manager für ONTAP 9.10.0 und früher angezeigt wird	Kapazitätseinheit, die im Unified Manager für ONTAP 9.10.1 angezeigt wird	Berechnung	Wert in Bytes
KB	KiB	1024	1024 Byte
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

Einführung in die Leistungsüberwachung von Active IQ Unified Manager

Active IQ Unified Manager (früher OnCommand Unified Manager) bietet Leistungsüberwachungsfunktionen und Ereignisursachenanalyse für Systeme, auf denen NetApp ONTAP -Software ausgeführt wird.

Unified Manager hilft Ihnen, Workloads zu identifizieren, die Clusterkomponenten überbeanspruchen und die

Leistung anderer Workloads im Cluster verringern. Durch die Definition von Richtlinien für Leistungsschwellenwerte können Sie auch Maximalwerte für bestimmte Leistungsindikatoren festlegen, sodass Ereignisse generiert werden, wenn der Schwellenwert überschritten wird. Unified Manager benachrichtigt Sie über diese Leistungsereignisse, sodass Sie Korrekturmaßnahmen ergreifen und die Leistung wieder auf das normale Betriebsniveau bringen können. Sie können Ereignisse in der Unified Manager-Benutzeroberfläche anzeigen und analysieren.

Unified Manager überwacht die Leistung von zwei Arten von Workloads:

- Benutzerdefinierte Workloads

  Diese Workloads bestehen aus FlexVol -Volumes und FlexGroup -Volumes, die Sie in Ihrem Cluster erstellt haben.

- Systemdefinierte Workloads

  Diese Arbeitslasten bestehen aus internen Systemaktivitäten.

Verwenden Sie Unified Manager REST-APIs

Active IQ Unified Manager bietet Ihnen REST-APIs zum Anzeigen von Informationen zur Überwachung und Verwaltung Ihrer Speicherumgebung. APIs ermöglichen außerdem die Bereitstellung und Verwaltung von Speicherobjekten auf der Grundlage von Richtlinien.

Sie können ONTAP -APIs auch auf allen von ONTAP verwalteten Clustern ausführen, indem Sie das von Unified Manager unterstützte API-Gateway verwenden.

Informationen zu Unified Manager REST-APIs finden Sie unter"Erste Schritte mit Active IQ Unified Manager REST-APIs" .

Was der Unified Manager-Server macht

Die Unified Manager-Serverinfrastruktur besteht aus einer Datenerfassungseinheit, einer Datenbank und einem Anwendungsserver. Es bietet Infrastrukturdienste wie Erkennung, Überwachung, rollenbasierte Zugriffskontrolle (RBAC), Auditing und Protokollierung.

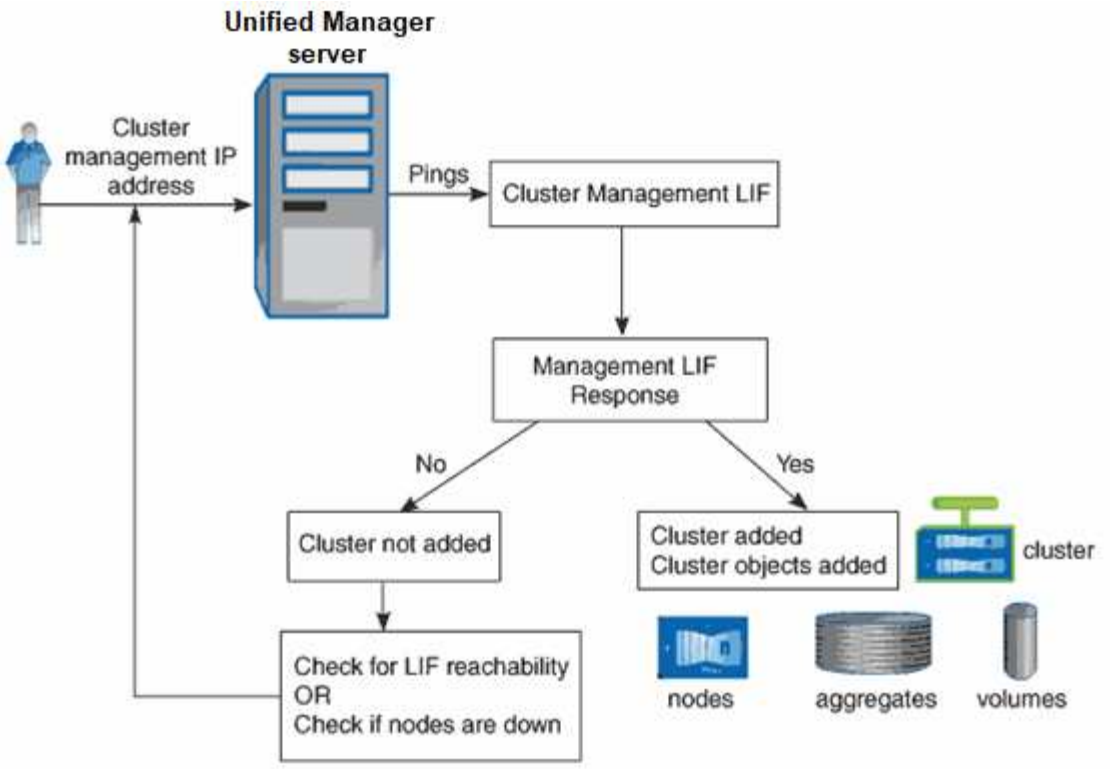
Unified Manager sammelt Clusterinformationen, speichert die Daten in der Datenbank und analysiert die Daten, um festzustellen, ob Clusterprobleme vorliegen.

So funktioniert der Discovery-Prozess

Nachdem Sie den Cluster zu Unified Manager hinzugefügt haben, erkennt der Server die Clusterobjekte und fügt sie seiner Datenbank hinzu. Wenn Sie verstehen, wie der Erkennungsprozess funktioniert, können Sie die Cluster und deren Objekte Ihrer Organisation besser verwalten.

Das Standardüberwachungsintervall beträgt 15 Minuten: Wenn Sie dem Unified Manager-Server einen Cluster hinzugefügt haben, dauert es 15 Minuten, bis die Clusterdetails in der Unified Manager-Benutzeroberfläche angezeigt werden.

Das folgende Bild veranschaulicht den Erkennungsprozess im Active IQ Unified Manager:



Verstehen Sie die Benutzeroberfläche

Die Benutzeroberfläche des Unified Managers besteht hauptsächlich aus einem Dashboard, das eine Übersicht über die überwachten Objekte bietet. Über die Benutzeroberfläche können Sie außerdem alle Clusterobjekte anzeigen.

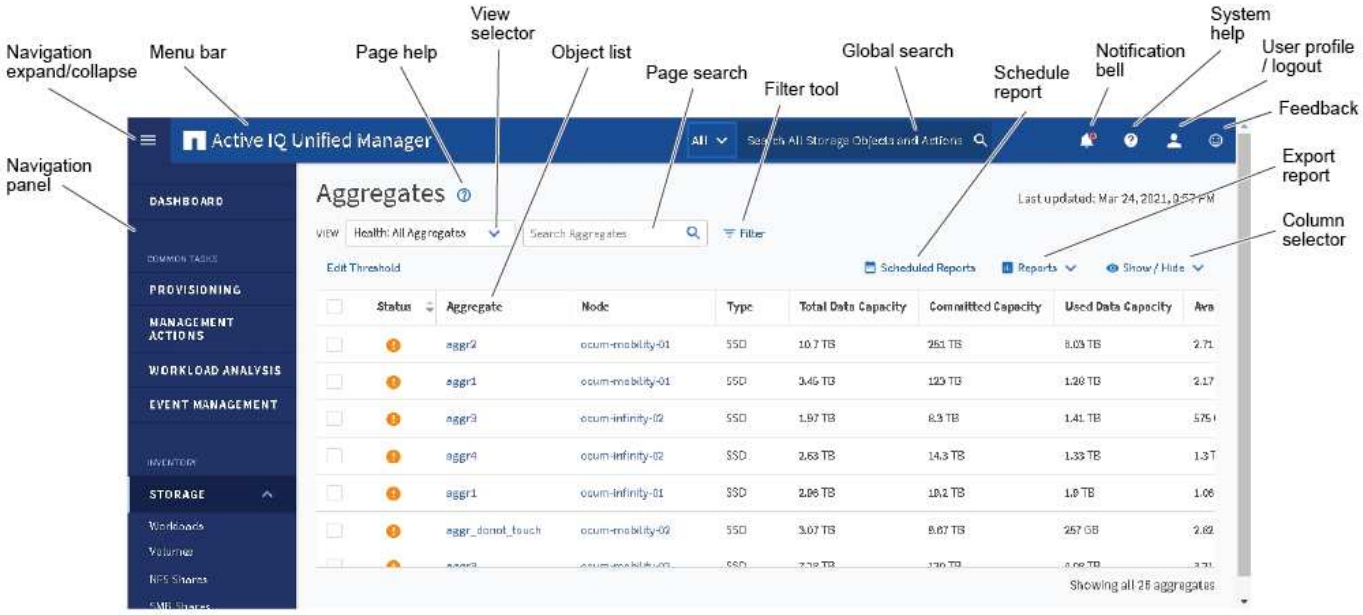
Sie können eine bevorzugte Ansicht auswählen und die Aktionsschaltflächen nach Bedarf verwenden. Ihre Bildschirmkonfiguration wird in einem Arbeitsbereich gespeichert, sodass beim Starten von Unified Manager alle benötigten Funktionen verfügbar sind. Wenn Sie jedoch von einer Ansicht zur anderen und dann zurück navigieren, ist die Ansicht möglicherweise nicht dieselbe.

Typische Fensterlayouts

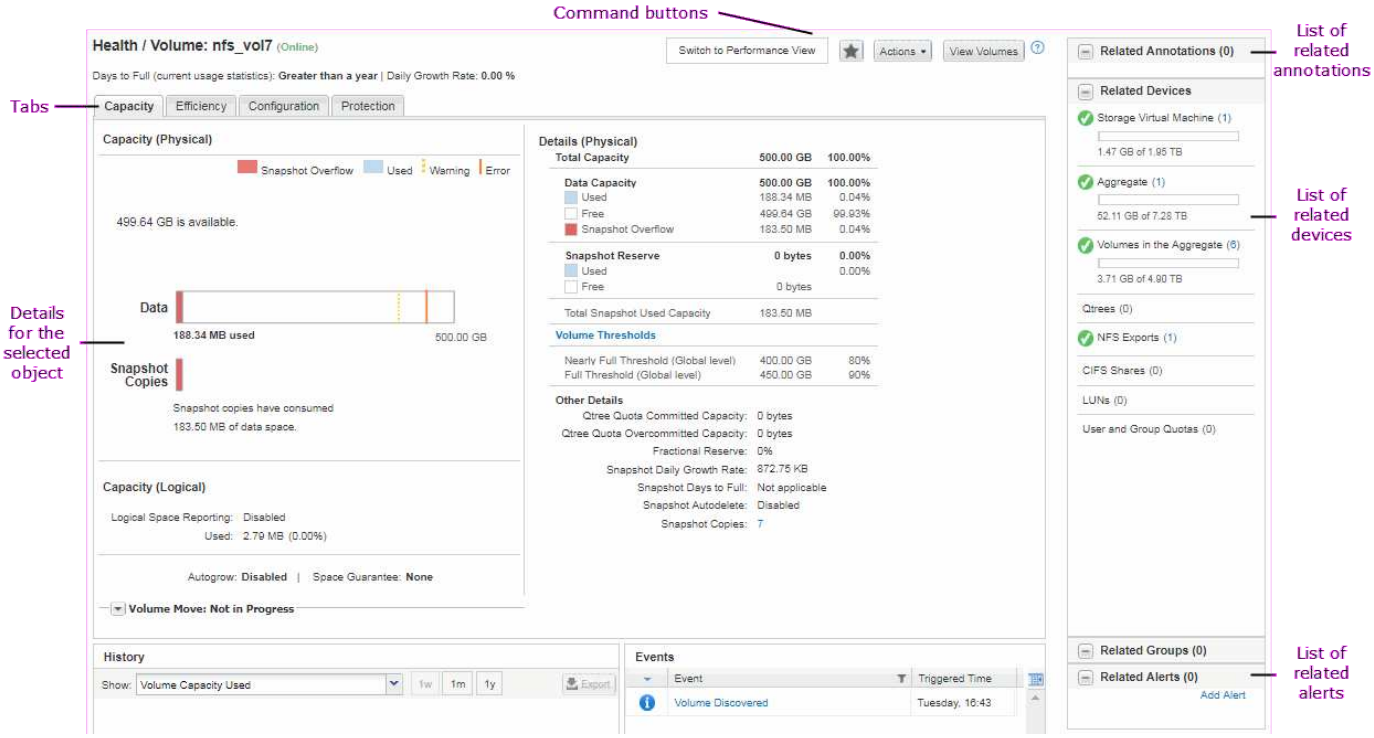
Wenn Sie die typischen Fensterlayouts verstehen, können Sie Active IQ Unified Manager effektiv navigieren und verwenden. Die meisten Unified Manager-Fenster ähneln einem von zwei allgemeinen Layouts: Objektliste oder Details. Die empfohlene Anzeigeeinstellung beträgt mindestens 1280 x 1024 Pixel.

Nicht jedes Fenster enthält jedes Element der folgenden Diagramme.

Layout des Objektlistenfensters



Layout des Fensters „Objektdetails“



Anpassung des Fensterlayouts

Mit Active IQ Unified Manager können Sie das Layout der Informationen auf den Speicher- und Netzwerkobjektseiten anpassen. Durch Anpassen der Fenster können Sie steuern, welche Daten angezeigt werden und wie die Daten angezeigt werden.

- **Sortierung**

  Sie können auf die Spaltenüberschrift klicken, um die Sortierreihenfolge der Spalteneinträge zu ändern.

Wenn Sie auf die Spaltenüberschrift klicken, werden die Sortierpfeile (Und) werden für diese Spalte angezeigt.

- **Filtern**

  Sie können auf das Filtersymbol ( ), um Filter anzuwenden und die Anzeige von Informationen auf den Speicher- und Netzwerkobjektseiten anzupassen, sodass nur die Einträge angezeigt werden, die den angegebenen Bedingungen entsprechen. Sie wenden Filter aus dem Filterbereich an.

  Im Filterbereich können Sie die meisten Spalten basierend auf den ausgewählten Optionen filtern. Beispielsweise können Sie in der Ansicht „Integrität: Alle Volumes“ den Bereich „Filter“ verwenden, um alle Volumes anzuzeigen, die offline sind, indem Sie unter „Status“ die entsprechende Filteroption auswählen.

  In den kapazitätsbezogenen Spalten einer Liste werden die Kapazitätsdaten immer in den entsprechenden Einheiten angezeigt, die auf zwei Dezimalstellen gerundet sind. Dies gilt auch beim Filtern von Kapazitätsspalten. Wenn Sie beispielsweise den Filter in der Spalte „Gesamtdatenkapazität“ in der Ansicht „Integrität: Alle Aggregate“ verwenden, um Daten größer als 20,45 GB zu filtern, wird die tatsächliche Kapazität von 20,454 GB als 20,45 GB angezeigt. Wenn Sie Daten mit weniger als 20,45 GB filtern, wird die tatsächliche Kapazität von 20,449 GB als 20,45 GB angezeigt.

  Wenn Sie den Filter in der Spalte „Verfügbare Daten %“ in der Ansicht „Integrität: Alle Aggregate“ verwenden, um Daten über 20,45 % zu filtern, wird die tatsächliche Kapazität von 20,454 % als 20,45 % angezeigt. Wenn Sie Daten unter 20,45 % filtern, wird die tatsächliche Kapazität von 20,449 % als 20,45 % angezeigt.

- **Spalten ausblenden oder anzeigen**

  Sie können auf das Symbol zur Spaltenanzeige (**Einblenden/Ausblenden**) klicken, um auszuwählen, welche Spalten angezeigt werden sollen. Nachdem Sie die entsprechenden Spalten ausgewählt haben, können Sie sie durch Ziehen mit der Maus neu anordnen.

- **Suche**

  Sie können das Suchfeld verwenden, um nach bestimmten Objektattributen zu suchen und so die Liste der Artikel auf der Inventarseite zu verfeinern. Sie können beispielsweise „Cloud“ eingeben, um die Liste der Volumes auf der Volume-Inventarseite zu verfeinern und alle Volumes anzuzeigen, die das Wort „Cloud“ enthalten.

- **Daten exportieren**

  Sie können auf die Schaltfläche **Berichte** (oder **Exportieren**) klicken, um Daten in eine durch Kommas getrennte Wertedatei zu exportieren. `(.csv)` Datei, `(.pdf)` Dokument oder Microsoft Excel `(.xlsx)` Datei und verwenden Sie die exportierten Daten zum Erstellen von Berichten.

Verwenden Sie die Unified Manager-Hilfe

Die Hilfe enthält Informationen zu allen in Active IQ Unified Manager enthaltenen Funktionen. Über das Inhaltsverzeichnis, den Index oder die Suchfunktion können Sie sich über die Funktionen und deren Verwendung informieren.

Hilfe ist auf jeder Registerkarte und in der Menüleiste der Unified Manager-Benutzeroberfläche verfügbar.

Das Suchtool in der Hilfe funktioniert bei Wortteilen nicht.

- Um mehr über bestimmte Felder oder Parameter zu erfahren, klicken Sie auf .
- Um alle Hilfeinhalte anzuzeigen, klicken Sie auf *** > *Hilfe/Dokumentation** in der Menüleiste.

  Ausführlichere Informationen erhalten Sie, indem Sie einen beliebigen Teil des Inhaltsverzeichnisses im Navigationsbereich erweitern.

- Um die Hilfeinhalte zu durchsuchen, klicken Sie im Navigationsbereich auf die Registerkarte **Suchen**, geben Sie das gewünschte Wort oder die gewünschte Wortfolge ein und klicken Sie auf **Los!**
- Um Hilfethemen auszudrucken, klicken Sie auf das Druckersymbol.

Setzen Sie ein Lesezeichen für Ihre bevorzugten Hilfethemen

Auf der Registerkarte „Hilfefavoriten“ können Sie häufig verwendete Hilfethemen mit einem Lesezeichen versehen. Mithilfe von Lesezeichen können Sie schnell auf Ihre Lieblingsthemen zugreifen.

Schritte

1. Navigieren Sie zu dem Hilfethema, das Sie als Favorit hinzufügen möchten.
2. Klicken Sie auf **Favoriten** und dann auf **Hinzufügen**.

Suche nach Speicherobjekten

Um schnell auf ein bestimmtes Objekt zuzugreifen, können Sie das Feld **Alle Speicherobjekte durchsuchen** oben in der Menüleiste verwenden. Mit dieser Methode der globalen Suche über alle Objekte hinweg können Sie bestimmte Objekte schnell nach Typ finden. Die Suchergebnisse werden nach Speicherobjekttyp sortiert und Sie können sie mithilfe des Dropdown-Menüs weiter nach Objekt filtern.

Bevor Sie beginnen

- Zum Ausführen dieser Aufgabe müssen Sie eine der folgenden Rollen innehaben: Operator, Anwendungsadministrator oder Speicheradministrator.
- Eine gültige Suche muss mindestens drei Zeichen enthalten.

Bei Verwendung des Dropdown-Menüwerts „Alle“ zeigt die globale Suche die Gesamtzahl der gefundenen Ergebnisse in allen Objektkategorien an; maximal 25 Suchergebnisse pro Objektkategorie. Sie können einen bestimmten Objekttyp aus dem Dropdown-Menü auswählen, um die Suche innerhalb eines bestimmten Objekttyps zu verfeinern. In diesem Fall ist die zurückgegebene Liste nicht auf die Top 25 Objekte beschränkt.

Zu den Objekttypen, nach denen Sie suchen können, gehören:

- Cluster
- Nodes
- Speicher-VMs
- Aggregate
- Bände
- Qtrees
- SMB-Aktien

- NFS-Freigaben
- Benutzer- oder Gruppenkontingente
- LUNs
- NVMe-Namespaces
- Initiatorgruppen
- Initiatoren
- Konsistenzgruppe

Durch Eingabe eines Workload-Namens wird die Liste der Workloads unter der entsprechenden Volume- oder LUN-Kategorie zurückgegeben.

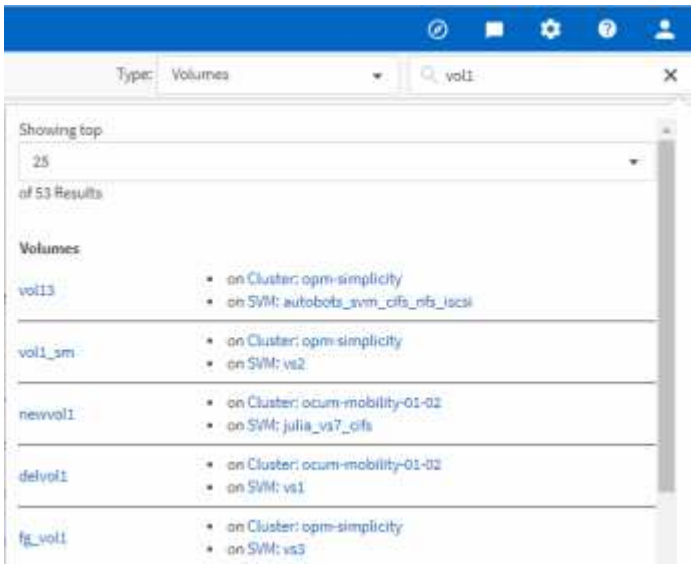
Sie können in den Suchergebnissen auf ein beliebiges Objekt klicken, um zur Seite mit den Integritätsdetails für dieses Objekt zu navigieren. Wenn für ein Objekt keine direkte Integritätsseite vorhanden ist, wird die Integritätsseite des übergeordneten Objekts angezeigt. Wenn Sie beispielsweise nach einer bestimmten LUN suchen, wird die SVM-Detailseite angezeigt, auf der sich die LUN befindet.

Ports und LIFs können in der globalen Suchleiste nicht durchsucht werden.

Schritte

1. Wählen Sie einen Objekttyp aus dem Menü aus, um die Suchergebnisse auf nur einen einzigen Objekttyp zu verfeinern.
2. Geben Sie mindestens drei Zeichen des Objektnamens in das Feld **Alle Speicherobjekte durchsuchen** ein.

   In diesem Beispiel ist im Dropdownfeld der Objekttyp „Volumes“ ausgewählt. Wenn Sie „vol1“ in das Feld **Alle Speicherobjekte durchsuchen** eingeben, wird eine Liste aller Volumes angezeigt, deren Namen diese Zeichen enthalten.



Speicherdaten als Berichte exportieren

Sie können Speicherdaten in verschiedenen Ausgabeformaten exportieren und die exportierten Daten dann zum Erstellen von Berichten verwenden. Wenn beispielsweise

10 kritische Ereignisse nicht behoben wurden, können Sie die Daten von der Inventarseite der Ereignisverwaltung exportieren, um einen Bericht zu erstellen, und den Bericht dann an Administratoren senden, die die Probleme beheben können.

Sie können Daten in eine `.csv` Datei, `.xlsx` Datei oder `.pdf` Dokument von den Inventarseiten **Speicher** und **Netzwerk** und verwenden Sie die exportierten Daten zum Erstellen von Berichten. Es gibt andere Stellen im Produkt, an denen nur `.csv` oder `.pdf` Dateien können generiert werden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Wenn Sie exportieren möchten…	Machen Sie Folgendes…
Details zum Speicherobjektbestand	Klicken Sie im linken Navigationsmenü auf **Speicher** oder **Netzwerk** und wählen Sie dann ein Speicherobjekt aus. Wählen Sie eine der vom System bereitgestellten Ansichten oder eine beliebige benutzerdefinierte Ansicht, die Sie erstellt haben.
Details zur QoS-Richtliniengruppe	Klicken Sie im linken Navigationsmenü auf **Speicher** > **QoS-Richtliniengruppen**.
Details zur Speicherkapazität und zum Schutzverlauf	Klicken Sie auf **Speicher** > **Aggregate** oder **Speicher** > **Volumes** und wählen Sie dann ein einzelnes Aggregat oder Volume aus.
Veranstaltungsdetails	Klicken Sie im linken Navigationsmenü auf **Eventverwaltung**.
Leistungsdetails der Top 10-Speicherobjekte	Klicken Sie auf **Speicher** > **Cluster** > **Leistung: Alle Cluster**, wählen Sie dann einen Cluster aus und wählen Sie die Registerkarte **Top-Performer**. Wählen Sie dann ein Speicherobjekt und einen Leistungsindikator aus.

2. Klicken Sie auf die Schaltfläche **Berichte** (oder auf einigen UI-Seiten auf die Schaltfläche **Exportieren**).
3. Klicken Sie auf **CSV herunterladen**, **PDF herunterladen** oder **Excel herunterladen**, um die Exportanforderung zu bestätigen.

   Auf der Registerkarte „Top Performers“ können Sie einen Bericht mit den Statistiken für den einzelnen Cluster, den Sie gerade anzeigen, oder für alle Cluster im Rechenzentrum herunterladen.

   Die Datei wird heruntergeladen.
4. Öffnen Sie die Datei in der entsprechenden Anwendung.

Verwandte Informationen

"Seite „Integrität/Cluster-Inventar“"

"Planen eines Berichts"

Inhalt der Inventarseite filtern

Sie können die Daten der Inventarseite im Unified Manager filtern, um Daten anhand bestimmter Kriterien schnell zu finden. Mithilfe von Filtern können Sie den Inhalt der Unified Manager-Seiten eingrenzen und nur die Ergebnisse anzeigen, die Sie interessieren. Dies bietet eine sehr effiziente Methode, nur die Daten anzuzeigen, an denen Sie interessiert sind.

Verwenden Sie **Filtern**, um die Rasteransicht Ihren Wünschen entsprechend anzupassen. Die verfügbaren Filteroptionen basieren auf dem Objekttyp, der im Raster angezeigt wird. Wenn derzeit Filter angewendet werden, wird die Anzahl der angewendeten Filter rechts neben der Schaltfläche „Filter“ angezeigt.

Es werden drei Arten von Filterparametern unterstützt.

Parameter	Validierung
Zeichenfolge (Text)	Die Operatoren sind **enthält**, **beginnt mit**, **endet mit** und **enthält nicht**.
Anzahl	Die Operatoren sind **größer als**, **kleiner als**, **im letzten** und **zwischen**.
Aufzählung (Text)	Die Operatoren sind **ist** und **ist nicht**.

Die Felder „Spalte“, „Operator“ und „Wert“ sind für jeden Filter erforderlich. Die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. Sie können maximal vier Filter anwenden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten in Ihrer gefilterten Suche, nicht nur für die aktuell angezeigte Seite.

Sie können Filter über das Filterfeld hinzufügen.

1. Klicken Sie oben auf der Seite auf die Schaltfläche **Filter**. Das Filterfeld wird angezeigt.
2. Klicken Sie auf die linke Dropdown-Liste und wählen Sie ein Objekt aus, beispielsweise *Cluster* oder einen Leistungsindikator.
3. Klicken Sie auf die mittlere Dropdown-Liste und wählen Sie den Operator aus, den Sie verwenden möchten.
4. Wählen Sie in der letzten Liste einen Wert aus oder geben Sie ihn ein, um den Filter für dieses Objekt zu vervollständigen.
5. Um einen weiteren Filter hinzuzufügen, klicken Sie auf **+Filter hinzufügen**. Ein zusätzliches Filterfeld wird angezeigt. Vervollständigen Sie diesen Filter mit dem in den vorhergehenden Schritten beschriebenen Verfahren. Beachten Sie, dass nach dem Hinzufügen Ihres vierten Filters die Schaltfläche **+Filter hinzufügen** nicht mehr angezeigt wird.
6. Klicken Sie auf **Filter anwenden**. Die Filteroptionen werden auf das Raster angewendet und die Anzahl der Filter wird rechts neben der Schaltfläche „Filter“ angezeigt.
7. Verwenden Sie das Filterfeld, um einzelne Filter zu entfernen, indem Sie auf das Papierkorbsymbol rechts neben dem zu entfernenden Filter klicken.

8. Um alle Filter zu entfernen, klicken Sie unten im Filterbereich auf **Zurücksetzen**.

Filterbeispiel

Die Abbildung zeigt das Filterbedienfeld mit drei Filtern. Die Schaltfläche **+Filter hinzufügen** wird angezeigt, wenn Sie weniger als die maximal vier Filter haben.

Nachdem Sie auf **Filter anwenden** geklickt haben, wird das Filterfenster geschlossen, Ihre Filter werden angewendet und die Anzahl der angewendeten Filter wird angezeigt (3).

Zeigen Sie aktive Ereignisse über die Benachrichtigungsglocke an

Die Benachrichtigungsglocke ( ) in der Menüleiste bietet eine schnelle Möglichkeit, die wichtigsten aktiven Ereignisse anzuzeigen, die Unified Manager verfolgt.

Die Liste der aktiven Ereignisse bietet eine Möglichkeit, die Gesamtzahl der kritischen Ereignisse, Fehler-, Warn- und Upgrade-Ereignisse auf allen Clustern anzuzeigen. Diese Liste enthält Ereignisse der letzten 7 Tage und keine Informationsereignisse. Sie können auf einen Link klicken, um die Liste der Ereignisse anzuzeigen, die Sie am meisten interessieren.

Beachten Sie, dass Unified Manager diese Informationen auf dieser Seite anzeigt, wenn ein Cluster nicht erreichbar ist. Sie können detaillierte Informationen zu einem nicht erreichbaren Cluster anzeigen, indem Sie auf die Schaltfläche **Details** klicken. Diese Aktion öffnet die Seite mit den Veranstaltungsdetails. Auf dieser Seite werden auch Probleme bei der Skalierungsüberwachung angezeigt, beispielsweise zu wenig Speicherplatz oder RAM auf der Verwaltungsstation.

Schritte

1. Klicken Sie in der Menüleiste auf .
2. Um Details zu einem der aktiven Ereignisse anzuzeigen, klicken Sie auf den Ereignistextlink, beispielsweise „2 Kapazität“ oder „4 Leistung“.

Überwachen und verwalten Sie Cluster über das Dashboard

Das Dashboard bietet auf einen Blick kumulative Informationen zum aktuellen Zustand Ihrer überwachten ONTAP Systeme. Das Dashboard bietet „Panels“, mit denen Sie die Gesamtkapazität, Leistung und Sicherheitsintegrität der von Ihnen überwachten Cluster beurteilen können.

Darüber hinaus gibt es bestimmte ONTAP Probleme, die Sie direkt über die Benutzeroberfläche des Unified Managers beheben können, anstatt den ONTAP System Manager oder die ONTAP CLI verwenden zu müssen.

Oben im 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 einen Drilldown zu einzelnen Clustern durchführen, wenn Sie detaillierte Informationen anzeigen möchten.

Je nach Ihrer Konfiguration werden einige der unten aufgeführten Bereiche möglicherweise nicht auf der Seite angezeigt.

Paneele	Beschreibung
Verwaltungsmaßnahmen	Wenn Unified Manager ein Problem diagnostizieren und eine einzelne Lösung dafür ermitteln kann, werden diese Lösungen in diesem Bereich mit einer Schaltfläche **Fix It** angezeigt.
Kapazität	Zeigt die gesamte und genutzte Kapazität für die lokale und die Cloud-Ebene sowie die Anzahl der Tage an, bis die lokale Kapazität die Obergrenze erreicht.
Leistungskapazität	Zeigt den Leistungskapazitätswert für jeden Cluster und die Anzahl der Tage an, bis die Leistungskapazität die Obergrenze erreicht.
Arbeitslast-IOPS	Zeigt die Gesamtzahl der Workloads an, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden.
Workload-Leistung	Zeigt die Gesamtzahl der konformen und nicht konformen Workloads an, die jedem definierten Performance-Service-Level zugewiesen sind.
Sicherheit	Zeigt die Anzahl der Cluster an, die konform oder nicht konform sind, die Anzahl der SVMs, die konform oder nicht konform sind, und die Anzahl der Volumes, die verschlüsselt oder nicht verschlüsselt sind.
Schutz	Zeigt die Anzahl der Storage-VMs an, die durch eine SVM-DR-Beziehung geschützt sind, die durch eine SnapMirror Beziehung geschützten Volumes, die durch Snapshot geschützten Volumes und die durch MetroCluster geschützten Cluster.
Nutzungsübersicht	Zeigt Cluster sortiert nach höchstem IOPS, höchstem Durchsatz (MBps) oder höchster genutzter physischer Kapazität an.

Dashboard-Seite

Die Dashboard-Seite verfügt über „Panels“, die die allgemeine Kapazität, Leistung und Sicherheitsintegrität der von Ihnen überwachten Cluster anzeigen. Diese Seite enthält außerdem ein Bedienfeld „Verwaltungsaktionen“, in dem Korrekturen aufgelistet sind, die Unified Manager zur Behebung bestimmter Ereignisse vornehmen kann.

Die meisten Panels zeigen auch die Anzahl der aktiven Ereignisse in dieser Kategorie und die Anzahl der in den letzten 24 Stunden hinzugefügten neuen Ereignisse an. Mithilfe dieser Informationen können Sie entscheiden, welche Cluster Sie möglicherweise weiter analysieren müssen, um Ereignisse aufzulösen. Durch Klicken auf die Ereignisse werden die wichtigsten Ereignisse angezeigt und ein Link zur Inventarseite des Ereignismanagements bereitgestellt, die gefiltert ist, um die aktiven Ereignisse in dieser Kategorie anzuzeigen.

Oben im Dashboard können Sie auswählen, ob die Panels Informationen für alle überwachten Cluster („Alle Cluster“) oder für einen einzelnen Cluster anzeigen. Sie können zunächst den Status aller Cluster anzeigen und dann einen Drilldown zu einzelnen Clustern durchführen, wenn Sie detaillierte Informationen anzeigen möchten.

Einige der unten aufgeführten Bedienfelder werden je nach Ihrer Konfiguration auf dem Dashboard angezeigt.

Bereich „Verwaltungsaktionen“

Es gibt bestimmte Probleme, die Unified Manager gründlich diagnostizieren und eine einzige Lösung bereitstellen kann. Sofern verfügbar, werden diese Lösungen in diesem Bereich mit der Schaltfläche **Fix It** oder **Fix All** angezeigt. Sie können diese Probleme sofort über Unified Manager beheben, anstatt ONTAP System Manager oder die ONTAP CLI verwenden zu müssen. Um alle Ausgaben anzuzeigen, klicken Sie auf „Anzeigen“"Beheben Sie ONTAP -Probleme direkt vom Unified Manager aus" für weitere Informationen.

Kapazitätspanel

Beim Anzeigen aller Cluster zeigt dieses Fenster die physisch genutzte Kapazität (nach Anwendung der Einsparungen bei der Speichereffizienz) und die physisch verfügbare Kapazität (ohne potenzielle Einsparungen bei der Speichereffizienz) für jeden Cluster, die Anzahl der Tage bis zur voraussichtlichen Volllast der Festplatten und das Datenreduktionsverhältnis (ohne Snapshot-Kopien) basierend auf den konfigurierten ONTAP Einstellungen zur Speichereffizienz an. Außerdem wird die genutzte Kapazität für alle konfigurierten Cloud-Ebenen aufgelistet. Durch Klicken auf das Balkendiagramm gelangen Sie zur Aggregate-Inventarseite für diesen Cluster. Wenn Sie auf den Text „Tage bis zur Vollauslastung“ klicken, wird eine Meldung angezeigt, die das Aggregat mit der geringsten Anzahl verbleibender Kapazitätstage identifiziert. Klicken Sie auf den Aggregatnamen, um weitere Details anzuzeigen.

Beim Anzeigen eines einzelnen Clusters zeigt dieses Fenster die physisch genutzte Kapazität und die physisch verfügbare Kapazität für die Datenaggregate an, sortiert nach den einzelnen Datenträgertypen auf der lokalen Ebene und für die Cloud-Ebene. Wenn Sie auf das Balkendiagramm für einen Datenträgertyp klicken, gelangen Sie zur Volume-Inventarseite für die Volumes, die diesen Datenträgertyp verwenden.

Leistungskapazitätspanel

Beim Anzeigen aller Cluster zeigt dieses Fenster den Leistungskapazitätswert für jeden Cluster (Durchschnittswert der letzten Stunde) und die Anzahl der Tage an, bis die Leistungskapazität die Obergrenze erreicht (basierend auf der täglichen Wachstumsrate). Durch Klicken auf das Balkendiagramm gelangen Sie zur Knotenbestandsseite für diesen Cluster. Beachten Sie, dass auf der Seite „Knoteninventar“ die durchschnittliche Leistungskapazität der letzten 72 Stunden angezeigt wird. Wenn Sie auf den Text „Tage bis zur Volllast“ klicken, wird eine Meldung angezeigt, die den Knoten mit der geringsten Anzahl verbleibender Tage für die Leistungskapazität identifiziert. Klicken Sie auf den Knotennamen, um weitere Details anzuzeigen.

Beim Anzeigen eines einzelnen Clusters zeigt dieses Fenster den Prozentsatz der genutzten Cluster-Leistungskapazität, die Gesamt-IOPS- und Gesamtdurchsatzwerte (MB/s) sowie die Anzahl der Tage an, bis jede dieser drei Kennzahlen voraussichtlich ihre Obergrenze erreicht.

Arbeitslast-IOPS-Panel

Beim Anzeigen eines einzelnen Clusters zeigt dieses Fenster die Gesamtzahl der Workloads an, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden, und gibt die Anzahl für jeden Datenträgertyp an, wenn Sie mit dem Cursor über das Diagramm fahren.

Bereich „Arbeitslastleistung“

In diesem Bereich wird die Gesamtzahl der konformen und nicht konformen Workloads angezeigt, die jeder Performance Service Level (PSL)-Richtlinie zugewiesen sind. Außerdem wird die Anzahl der Workloads angezeigt, denen keine PSL zugewiesen ist. Durch Klicken auf ein Balkendiagramm gelangen Sie zu den entsprechenden Arbeitslasten, die dieser Richtlinie auf der Seite „Arbeitslasten“ zugewiesen sind. Wenn Sie auf die Zahl hinter dem Balkendiagramm klicken, gelangen Sie zu den konformen und nicht konformen Arbeitslasten, die dieser Richtlinie zugewiesen sind.

Sicherheitspanel

Das Sicherheitsfenster zeigt den allgemeinen Sicherheitsstatus für alle Cluster oder einen einzelnen Cluster an, je nach Ihrer aktuellen Ansicht. Dieses Fenster zeigt Folgendes an:

- eine Liste der in den letzten 24 Stunden empfangenen Sicherheitsereignisse. Klicken Sie auf ein Ereignis, um die Details auf der Seite „Ereignisdetails“ anzuzeigen.
- den Cluster-Sicherheitsstatus (Anzahl der konformen und nicht konformen Cluster)
- der Sicherheitsstatus der Speicher-VM (Anzahl der konformen und nicht konformen Speicher-VMs)
- den Volume-Verschlüsselungsstatus (Anzahl der Volumes, die verschlüsselt oder nicht verschlüsselt sind)
- den Anti-Ransomware-Status des Volumes (Anzahl der Volumes mit aktiviertem oder deaktiviertem Anti-Ransomware-Schutz)

Sie können auf die Balkendiagramme der konformen und nicht konformen Cluster, Speicher-VMs, verschlüsselten und unverschlüsselten Volumes und des Volume-Anti-Ransomware-Status klicken, um zu den entsprechenden Seiten zu gelangen und die Sicherheitsdetails der gefilterten Cluster, Speicher-VMs und Volumes anzuzeigen.

Die Einhaltung basiert auf der "NetApp Security Hardening Guide für ONTAP 9" . Klicken Sie oben im Bereich auf den Rechtspfeil, um Sicherheitsdetails für alle Cluster auf der Seite „Sicherheit“ anzuzeigen. Weitere Informationen finden Sie unter"Anzeigen des detaillierten Sicherheitsstatus für Cluster und Storage-VMs" .

Datenschutzpanel

In diesem Bereich wird die Datenschutzzusammenfassung für einen einzelnen oder alle Cluster in einem Rechenzentrum angezeigt. 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. Wenn Sie auf den Link jedes dieser Ereignisse klicken, gelangen Sie zur Seite mit den Ereignisdetails. Sie können auf den Link **Alle anzeigen** klicken, um alle aktiven Schutzereignisse auf der Inventarseite der Ereignisverwaltung anzuzeigen. Das Bedienfeld zeigt Folgendes an:

- Die Anzahl der Volumes in einem Cluster oder alle Cluster in einem Rechenzentrum, die durch Snapshot-Kopien geschützt sind.
- Die Anzahl der Volumes in einem Cluster oder alle Cluster in einem Rechenzentrum, die durch SnapMirror -Beziehungen geschützt sind. Bei SnapMirror -Beziehungen wird die Volumeanzahl im Quellcluster berücksichtigt.
- Die Anzahl der Cluster oder alle Cluster in einem Rechenzentrum, die durch die MetroCluster -Konfiguration über IP oder FC geschützt sind.
- Die Anzahl der Volume-Beziehungen mit SnapMirror Recovery Point Objective (RPO)-Verzögerung basierend auf dem Verzögerungsstatus.

Sie können mit der Maus darüberfahren, um die jeweiligen Zählungen und Legenden anzuzeigen. Sie können oben im Bereich auf den rechten Pfeil klicken, um die Details für einen einzelnen oder alle Cluster auf der

Seite „Datenschutz“ anzuzeigen. Sie können auch auf Folgendes klicken:

- Die Balkendiagramme für ungeschützte Volumes und durch Snapshot-Kopien geschützte Volumes ermöglichen es Ihnen, zur Seite „Volumes“ zu gelangen und die Details anzuzeigen.
- Die Balkendiagramme für die durch die MetroCluster -Konfiguration geschützten oder nicht geschützten Cluster, um zur Seite „Cluster“ zu gelangen und die Details anzuzeigen.
- Die Balkendiagramme für alle Beziehungen führen zur Seite „Beziehungen“, wo die Details basierend auf dem Quellcluster gefiltert werden.

Weitere Informationen finden Sie unter "Anzeigen des Volume-Schutzstatus".

Bedienfeld „Nutzungsübersicht“

Beim Anzeigen aller Cluster können Sie die Cluster nach den höchsten IOPS, dem höchsten Durchsatz (MB/s) oder der höchsten genutzten physischen Kapazität sortiert anzeigen.

Beim Anzeigen eines einzelnen Clusters können Sie die Workloads nach den höchsten IOPS, dem höchsten Durchsatz (MB/s) oder der höchsten genutzten logischen Kapazität sortiert anzeigen.

Verwandte Informationen

"Beheben von Problemen mithilfe automatischer Korrekturen von Unified Manager"

"Anzeigen von Informationen zu Leistungsereignissen"

"Verwalten der Leistung mithilfe von Leistungskapazität und verfügbaren IOPS-Informationen"

"Seite mit den Volumen-/Gesundheitsdetails"

"Analyse und Benachrichtigung von Leistungsereignissen"

"Beschreibung der Ereignisschweregrade"

"Quellen von Leistungsereignissen"

"Verwalten von Cluster-Sicherheitszielen"

"Überwachen Sie die Clusterleistung von der Zielseite des Leistungsclusters aus"

"Überwachen Sie die Leistung mithilfe der Leistungsinventarseiten"

Verwalten Sie ONTAP -Probleme oder -Funktionen direkt vom Unified Manager

Sie können bestimmte ONTAP Probleme beheben oder bestimmte ONTAP Funktionen direkt über die Unified Manager-Benutzeroberfläche verwalten, anstatt den ONTAP System Manager oder die ONTAP CLI verwenden zu müssen. Die Option „Verwaltungsaktionen“ bietet Korrekturen für eine Reihe von ONTAP Problemen, die Unified Manager-Ereignisse ausgelöst haben.

Sie können Probleme direkt auf der Seite „Verwaltungsaktionen“ beheben, indem Sie im linken Navigationsbereich die Option **Verwaltungsaktionen** auswählen. Verwaltungsaktionen sind auch im Bereich „Verwaltungsaktionen“ auf dem Dashboard, auf der Seite mit den Ereignisdetails und in der Auswahl „Arbeitslastanalyse“ im linken Navigationsmenü verfügbar.

Es gibt bestimmte Probleme, die Unified Manager gründlich diagnostizieren und eine einzige Lösung bereitstellen kann. Für bestimmte ONTAP Funktionen, wie z. B. die Anti-Ransomware-Überwachung, führt Unified Manager interne Prüfungen durch und empfiehlt bestimmte Maßnahmen. Sofern verfügbar, werden diese Lösungen in den Verwaltungsaktionen mit der Schaltfläche **Fix It** angezeigt. Klicken Sie auf die Schaltfläche **Fix It**, um das Problem zu beheben. Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Unified Manager sendet ONTAP -Befehle an den Cluster, um die angeforderte Korrektur vorzunehmen. Wenn die Korrektur abgeschlossen ist, ist das Ereignis veraltet.

Einige Verwaltungsaktionen ermöglichen es Ihnen, dasselbe Problem auf mehreren Speicherobjekten mithilfe der Schaltfläche **Alles beheben** zu beheben. Beispielsweise kann es bei 5 Volumes das Ereignis „Volume-Speicherplatz voll“ geben, das durch Klicken auf die Verwaltungsaktion **Alles beheben** für „Volume-Autovergrößerung aktivieren“ behoben werden könnte. Mit einem Klick können Sie dieses Problem auf 5 Volumes beheben.

Informationen zu den ONTAP -Problemen und -Funktionen, die Sie mithilfe der automatischen Behebung verwalten können, finden Sie unter"Welche Probleme kann Unified Manager beheben?" .

Welche Optionen habe ich, wenn ich die Schaltfläche „Fix It“ oder „Fix All“ sehe?

Auf der Seite „Verwaltungsaktionen“ können Sie mit der Schaltfläche **Beheben** oder **Alles beheben** Probleme beheben, über die Unified Manager durch ein Ereignis benachrichtigt wurde.

Wir empfehlen Ihnen, bei Bedarf auf die Schaltflächen zu klicken, um ein Problem zu beheben. Wenn Sie jedoch nicht sicher sind, ob Sie das Problem wie von Unified Manager empfohlen beheben möchten, können Sie die folgenden Aktionen ausführen:

Was möchten Sie tun?	Aktion
Lassen Sie Unified Manager das Problem bei allen identifizierten Objekten beheben.	Klicken Sie auf die Schaltfläche **Alles beheben**.
Beheben Sie das Problem für keines der identifizierten Objekte zu diesem Zeitpunkt und verbergen Sie diese Verwaltungsaktion, bis das Ereignis erneut ausgelöst wird.	Klicken Sie auf den Abwärtspfeil und dann auf **Alle verwerfen**.
Beheben Sie das Problem nur bei einigen der identifizierten Objekte.	Klicken Sie auf den Namen der Verwaltungsaktion, um die Liste zu erweitern und alle einzelnen **Fix It** -Aktionen anzuzeigen. Folgen Sie dann den Schritten zum Beheben oder Ablehnen einzelner Verwaltungsaktionen.

Was möchten Sie tun?	Aktion
Lassen Sie das Problem von Unified Manager beheben.	Klicken Sie auf die Schaltfläche **Fix It**.

Was möchten Sie tun?	Aktion
Beheben Sie das Problem zu diesem Zeitpunkt nicht und verbergen Sie diese Verwaltungsaktion, bis das Ereignis erneut ausgelöst wird.	Klicken Sie auf den Abwärtspfeil und dann auf **Verwerfen**.
Zeigen Sie die Details zu diesem Ereignis an, damit Sie das Problem besser verstehen.	• Klicken Sie auf die Schaltfläche **Fix It** und überprüfen Sie die Korrektur, die im daraufhin angezeigten Dialogfeld angewendet wird. • Klicken Sie auf den Abwärtspfeil und dann auf **Ereignisdetails anzeigen**, um die Seite mit den Ereignisdetails anzuzeigen. Klicken Sie dann auf einer der resultierenden Seiten auf **Beheben**, wenn Sie das Problem beheben möchten.
Zeigen Sie die Details zu diesem Speicherobjekt an, damit Sie das Problem besser verstehen.	Klicken Sie auf den Namen des Speicherobjekts, um Details entweder im Leistungs-Explorer oder auf der Seite „Integritätsdetails“ anzuzeigen.

In einigen Fällen wird die Korrektur in der nächsten 15-minütigen Konfigurationsumfrage angezeigt. In anderen Fällen kann es mehrere Stunden dauern, bis die Konfigurationsänderung verifiziert und das Ereignis verworfen ist.

Um die Liste der abgeschlossenen oder laufenden Verwaltungsaktionen anzuzeigen, klicken Sie auf das Filtersymbol und wählen Sie **Abgeschlossen** oder **In Bearbeitung**.

Fix: Alle Vorgänge werden seriell ausgeführt. Wenn Sie also das Fenster „In Bearbeitung“ anzeigen, haben einige Objekte den Status „In Bearbeitung“, während andere den Status „Geplant“ haben. Dies bedeutet, dass sie noch auf ihre Implementierung warten.

Zeigen Sie den Status der Verwaltungsaktionen an, die Sie beheben möchten

Sie können den Status aller Verwaltungsaktionen, die Sie zur Behebung ausgewählt haben, auf der Seite „Verwaltungsaktionen“ anzeigen. Die meisten Aktionen werden ziemlich schnell als **Abgeschlossen** angezeigt, nachdem Unified Manager den ONTAP -Befehl an den Cluster gesendet hat. Einige Aktionen, beispielsweise das Verschieben eines Volumes, können jedoch länger dauern.

Auf der Seite „Verwaltungsaktionen“ stehen drei Filter zur Verfügung:

- **Abgeschlossen** zeigt sowohl erfolgreich abgeschlossene als auch fehlgeschlagene Verwaltungsaktionen an. **Fehlgeschlagene** Aktionen geben einen Grund für den Fehler an, sodass Sie das Problem manuell beheben können.
- **In Bearbeitung** zeigt sowohl die Verwaltungsmaßnahmen an, die gerade umgesetzt werden, als auch die, deren Umsetzung geplant ist.
- **Empfohlen** zeigt alle Verwaltungsaktionen an, die derzeit für alle überwachten Cluster aktiv sind.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Verwaltungsaktionen**. Alternativ klicken Sie auf ⋮ oben im Bereich **Verwaltungsaktionen** auf dem **Dashboard** und wählen Sie die Ansicht aus, die Sie anzeigen möchten.

   Die Seite „Verwaltungsaktionen“ wird angezeigt.

2. Sie können auf das Caret-Symbol neben der Verwaltungsaktion im Feld **Beschreibung** klicken, um Details zum Problem und den Befehl anzuzeigen, der zum Beheben des Problems verwendet wird.
3. Um alle **fehlgeschlagenen** Aktionen anzuzeigen, sortieren Sie nach der Spalte **Status** in der Ansicht **Abgeschlossen**. Sie können das **Filter**-Tool für denselben Zweck verwenden.
4. Wenn Sie weitere Informationen zu einer fehlgeschlagenen Verwaltungsaktion anzeigen möchten oder wenn Sie eine empfohlene Verwaltungsaktion korrigieren möchten, können Sie im erweiterten Bereich auf **Ereignisdetails anzeigen** klicken, nachdem Sie auf das Caret-Symbol neben der Verwaltungsaktion geklickt haben. Auf dieser Seite ist eine Schaltfläche „Fix It“ verfügbar.

Welche Probleme kann Unified Manager beheben?

Mithilfe der automatischen Korrekturfunktion 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 verwalten.

Diese Tabelle beschreibt diese ONTAP Probleme oder -Funktionen, die Sie direkt über die Schaltfläche **Fix It** oder **Fix All** auf der Unified Manager-Web-Benutzeroberfläche verwalten können.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
Volume-Speicherplatz voll Der Speicherplatz des Datenträgers ist fast erschöpft und die Kapazitätsgrenze wurde überschritten. Dieser Schwellenwert ist standardmäßig auf 90 % der Volumegröße eingestellt.	Automatisches Volume-Vergrößern aktivieren	Unified Manager stellt fest, dass die automatische Volumevergrößerung für dieses Volume nicht konfiguriert ist, und aktiviert diese Funktion, damit die Kapazität des Volumes bei Bedarf vergrößert wird.
Inodes voll Dieses Volume hat keine Inodes mehr und kann keine neuen Dateien aufnehmen.	Erhöhen Sie die Anzahl der Inodes auf dem Volume	Erhöht die Anzahl der Inodes auf dem Volume um 2 Prozent.
Nichtübereinstimmung der Speicherebenenrichtlinie erkannt Das Volume enthält viele inaktive Daten und die aktuelle Tiering-Richtlinie ist auf „Nur Snapshot“ oder „Keine“ eingestellt.	Aktivieren Sie das automatische Cloud-Tiering	Da sich das Volume bereits auf einem FabricPool befindet, wird die Tiering-Richtlinie auf „Auto“ geändert, sodass inaktive Daten in die kostengünstigere Cloud-Stufe verschoben werden.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
Speicherebenen-Nichtübereinstimmung erkannt Das Volume enthält viele inaktive Daten, befindet sich jedoch nicht auf einer Cloud-fähigen Speicherebene (FabricPool).	Ändern der Speicherebene des Volumes	Verschiebt das Volume in die Cloud-fähige Speicherebene und setzt die Tiering-Richtlinie auf „Auto“, um inaktive Daten in die Cloud-Ebene zu verschieben.
Überwachungsprotokoll deaktiviert Das Überwachungsprotokoll ist für die Speicher-VM nicht aktiviert	Aktivieren Sie die Überwachungsprotokollierung für die Speicher-VM	Aktiviert die Audit-Protokollierung auf der Speicher-VM. Beachten Sie, dass für die Speicher-VM bereits ein lokaler oder Remote-Speicherort für das Überwachungsprotokoll konfiguriert sein muss.
Login-Banner deaktiviert Das Anmeldebanner für den Cluster sollte aktiviert werden, um die Sicherheit durch deutliche Kennzeichnung der Zugriffsbeschränkungen zu erhöhen.	Anmeldebanner für den Cluster festlegen	Setzt das Cluster-Anmeldebanner auf „`Zugriff auf autorisierte Benutzer beschränkt`“.
Login-Banner deaktiviert Das Anmeldebanner für die Speicher-VM sollte aktiviert werden, um die Sicherheit durch deutliche Kennzeichnung der Zugriffsbeschränkungen zu erhöhen.	Anmeldebanner für die Speicher-VM festlegen	Legt das Anmeldebanner der Speicher-VM auf „Zugriff auf autorisierte Benutzer beschränkt“ fest.
SSH verwendet unsichere Chiffren Chiffren mit dem Suffix „-cbc“ gelten als unsicher.	Entfernen Sie unsichere Chiffren aus dem Cluster	Entfernt die unsicheren Chiffren – wie z. B. aes192-cbc und aes128-cbc – aus dem Cluster.
SSH verwendet unsichere Chiffren Chiffren mit dem Suffix „-cbc“ gelten als unsicher.	Entfernen unsicherer Chiffren aus der Speicher-VM	Entfernt die unsicheren Chiffren – wie z. B. aes192-cbc und aes128-cbc – aus der Speicher-VM.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
AutoSupport HTTPS-Transport deaktiviert Das zum Senden von AutoSupport -Nachrichten an den technischen Support verwendete Transportprotokoll sollte verschlüsselt sein.	Legen Sie HTTPS als Transportprotokoll für AutoSupport -Nachrichten fest	Legt HTTPS als Transportprotokoll für AutoSupport -Nachrichten im Cluster fest.
Schwellenwert für Cluster-Lastungleichgewicht überschritten Zeigt an, dass die Last zwischen den Knoten im Cluster unausgewogen ist. Dieses Ereignis wird generiert, wenn die Abweichung der genutzten Leistungskapazität zwischen den Knoten mehr als 30 % beträgt.	Ausbalancieren der Cluster-Workloads	Unified Manager ermittelt das Volume, das sich am besten von einem Knoten zum anderen verschieben lässt, um das Ungleichgewicht zu verringern, und verschiebt dann das Volume.
Schwellenwert für Cluster-Kapazitätsungleichgewicht überschritten Zeigt an, dass die Kapazität zwischen den Aggregaten im Cluster unausgewogen ist. Dieses Ereignis wird generiert, wenn die Abweichung der genutzten Kapazität zwischen Aggregaten mehr als 70 % beträgt.	Clusterkapazität ausgleichen	Unified Manager ermittelt das beste Volume zum Verschieben von einem Aggregat zu einem anderen, um das Ungleichgewicht zu reduzieren, und verschiebt dann das Volume.
Schwellenwert für genutzte Leistungskapazität überschritten Zeigt an, dass die Last auf dem Knoten überbeansprucht werden könnte, wenn Sie die Auslastung durch eine oder mehrere hochaktive Workloads nicht reduzieren. Dieses Ereignis wird generiert, wenn der Wert für die genutzte Knotenleistungskapazität länger als 12 Stunden über 100 % liegt.	Begrenzen Sie die hohe Belastung des Knotens	Unified Manager identifiziert das Volume mit den höchsten IOPS und wendet eine QoS-Richtlinie an, die die erwarteten und maximalen IOPS-Werte des Verlaufs verwendet, um die Belastung des Knotens zu reduzieren.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
Warnschwelle für dynamische Ereignisse überschritten Zeigt an, dass der Knoten aufgrund der ungewöhnlich hohen Belastung einiger Workloads bereits in einem überlasteten Zustand arbeitet.	Reduzieren Sie die Überlastung im Knoten	Unified Manager identifiziert das Volume mit den höchsten IOPS und wendet eine QoS-Richtlinie an, die die erwarteten und maximalen IOPS-Werte des Verlaufs verwendet, um die Belastung des Knotens zu reduzieren.
Übernahme nicht möglich Failover ist derzeit deaktiviert, sodass der Zugriff auf die Ressourcen des Knotens während eines Ausfalls oder Neustarts verloren geht, bis der Knoten wieder verfügbar ist.	Knoten-Failover aktivieren	Unified Manager sendet den entsprechenden Befehl, um das Failover auf allen Knoten im Cluster zu aktivieren.
Option Cf.takeover.on_panic ist deaktiviert Die Node-Shell-Option „cf.takeover.on_panic“ ist auf **Aus** gesetzt, was auf HA-konfigurierten Systemen zu einem Problem führen könnte.	Übernahme bei Panik aktivieren	Unified Manager sendet den entsprechenden Befehl an den Cluster, um diese Einstellung auf **Ein** zu ändern.
Deaktivieren Sie die NodeShell-Option snapmirror.enable Die alte NodeShell-Option „snapmirror.enable“ ist auf **on** eingestellt, was nach dem Upgrade auf ONTAP 9.3 oder höher zu Problemen beim Booten führen kann.	Setzen Sie die Option snapmirror.enable auf „Aus“	Unified Manager sendet den entsprechenden Befehl an den Cluster, um diese Einstellung auf **Aus** zu ändern.
Telnet aktiviert Weist auf ein potenzielles Sicherheitsproblem hin, da Telnet unsicher ist und Daten unverschlüsselt überträgt.	Telnet deaktivieren	Unified Manager sendet den entsprechenden Befehl an den Cluster, um Telnet zu deaktivieren.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
Konfigurieren des Anti-Ransomware-Lernens für Speicher-VMs Überprüft regelmäßig, ob Cluster mit Lizenzen für die Anti-Ransomware-Überwachung vorhanden sind. Überprüft, ob eine Speicher-VM in einem solchen Cluster nur NFS- oder SMB-Volumes unterstützt.	Platzieren Sie Speicher-VMs in einem `learning` Modus der Anti-Ransomware-Überwachung	Unified Manager setzt Anti-Ransomware-Überwachung auf `learning` Status für die Speicher-VMs über die Cluster-Verwaltungskonsole. Die Anti-Ransomware-Überwachung aller neuen Volumes, die auf der Speicher-VM erstellt werden, wird automatisch in einen Lernmodus versetzt. Durch diese Aktivierung kann ONTAP das Aktivitätsmuster auf den Volumes erlernen und Anomalien aufgrund potenzieller böswilliger Angriffe erkennen.
Konfigurieren des Volume-Anti-Ransomware-Lernens Überprüft regelmäßig, ob Cluster mit Lizenzen für die Anti-Ransomware-Überwachung vorhanden sind. Überprüft, ob ein Volume in einem solchen Cluster nur NFS- oder SMB-Dienste unterstützt.	Legen Sie Bände in `learning` Modus der Anti-Ransomware-Überwachung	Unified Manager setzt Anti-Ransomware-Überwachung auf `learning` Status für die Volumes über die Cluster-Verwaltungskonsole. Durch diese Aktivierung kann ONTAP das Aktivitätsmuster auf den Volumes erlernen und Anomalien aufgrund potenzieller böswilliger Angriffe erkennen.
Aktivieren Sie den Volume-Anti-Ransomware Überprüft regelmäßig, ob Cluster mit Lizenzen für die Anti-Ransomware-Überwachung vorhanden sind. Erkennt, ob die Volumes im `learning` Modus der Anti-Ransomware-Überwachung für mehr als 45 Tage und ermittelt die Aussicht, sie in den aktiven Modus zu versetzen.	Legen Sie Bände in `active` Modus der Anti-Ransomware-Überwachung	Unified Manager setzt Anti-Ransomware-Überwachung auf `active` auf den Volumes über die Cluster-Verwaltungskonsole. Durch diese Aktivierung kann ONTAP das Aktivitätsmuster auf den Volumes erlernen, Anomalien aufgrund potenzieller böswilliger Angriffe erkennen und Warnmeldungen für Datenschutzmaßnahmen erstellen.

Ereignisname und -beschreibung	Management-Maßnahmen	„Fix It“-Operation
Volume-Anti-Ransomware deaktivieren Überprüft regelmäßig, ob Cluster mit Lizenzen für die Anti-Ransomware-Überwachung vorhanden sind. Erkennt wiederholte Benachrichtigungen während der aktiven Anti-Ransomware-Überwachung auf den Volumes (z. B. werden über einen Zeitraum von 30 Tagen mehrere Warnungen vor potenziellen Ransomware-Angriffen zurückgegeben).	Deaktivieren Sie die Anti-Ransomware-Überwachung auf Volumes	Unified Manager deaktiviert die Anti-Ransomware-Überwachung auf den Volumes über die Cluster-Verwaltungskonsole.

Überschreiben von Verwaltungsaktionen durch Skripte

Sie können benutzerdefinierte Skripte erstellen und sie mit Warnungen verknüpfen, um bei bestimmten Ereignissen bestimmte Aktionen auszuführen, und müssen sich nicht für die standardmäßigen Verwaltungsaktionen entscheiden, die auf der Seite „Verwaltungsaktionen“ oder im Unified Manager-Dashboard dafür verfügbar sind.

Wenn Sie bestimmte Aktionen für einen Ereignistyp ausführen möchten und diese nicht als Teil der von Unified Manager bereitgestellten Verwaltungsaktionsfunktion beheben möchten, können Sie ein benutzerdefiniertes Skript für die bestimmte Aktion konfigurieren. Sie können das Skript dann mit einer Warnung für diesen Ereignistyp verknüpfen und sich einzeln um solche Ereignisse kümmern. In diesem Fall werden für diesen bestimmten Ereignistyp keine Verwaltungsaktionen auf der Seite „Verwaltungsaktionen“ oder im Unified Manager-Dashboard generiert.

Verwalten von Clustern

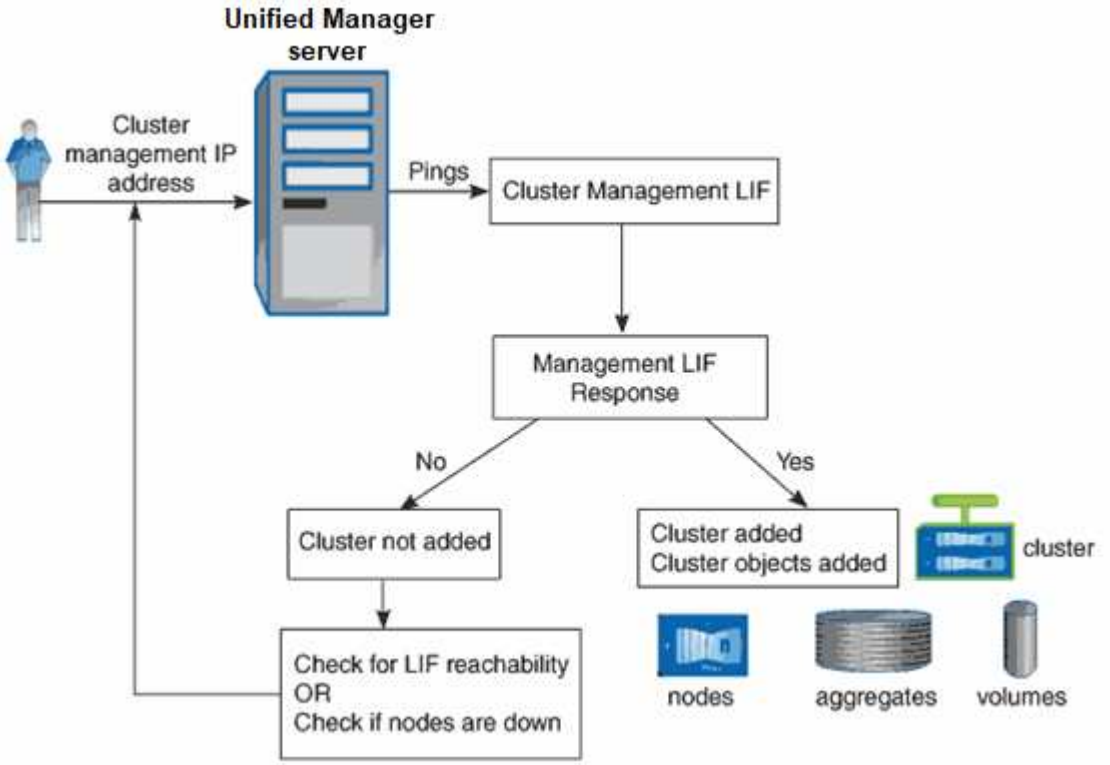
Sie können die ONTAP Cluster verwalten, indem Sie Unified Manager zum Überwachen, Hinzufügen, Bearbeiten und Entfernen von Clustern verwenden.

So funktioniert der Cluster-Erkennungsprozess

Nachdem Sie Unified Manager einen Cluster hinzugefügt haben, erkennt der Server die Clusterobjekte und fügt sie seiner Datenbank hinzu. Wenn Sie verstehen, wie der Erkennungsprozess funktioniert, können Sie die Cluster und deren Objekte Ihrer Organisation besser verwalten.

Das Überwachungsintervall zum Sammeln von Clusterkonfigurationsinformationen beträgt 15 Minuten. Nachdem Sie beispielsweise einen Cluster hinzugefügt haben, dauert es 15 Minuten, bis die Clusterobjekte in der Unified Manager-Benutzeroberfläche angezeigt werden. Dieser Zeitrahmen gilt auch für Änderungen an einem Cluster. Wenn Sie beispielsweise einem SVM in einem Cluster zwei neue Volumes hinzufügen, werden Ihnen diese neuen Objekte nach dem nächsten Abfrageintervall, das bis zu 15 Minuten dauern kann, in der Benutzeroberfläche angezeigt.

Das folgende Bild veranschaulicht den Erkennungsprozess:



Nachdem alle Objekte für einen neuen Cluster erkannt wurden, beginnt Unified Manager mit der Erfassung historischer Leistungsdaten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Datenkontinuitätserfassung erfasst. Mit dieser Funktion erhalten Sie unmittelbar nach dem Hinzufügen eines Clusters Leistungsinformationen für mehr als zwei Wochen. Nachdem der Datenkontinuitätserfassungszyklus abgeschlossen ist, werden standardmäßig alle fünf Minuten Echtzeitdaten zur Clusterleistung erfasst.

Da die Erfassung von 15 Tagen Leistungsdaten CPU-intensiv ist, wird empfohlen, das Hinzufügen neuer Cluster zu staffeln, damit Abfragen zur Datenkontinuitätserfassung nicht auf zu vielen Clustern gleichzeitig ausgeführt werden.

Liste der überwachten Cluster anzeigen

Auf der Seite „Cluster-Setup“ können Sie Ihren Clusterbestand anzeigen. Sie können Details zu den Clustern anzeigen, beispielsweise deren Namen oder IP-Adresse und Kommunikationsstatus.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritt

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.

   Alle von Unified Manager verwalteten Cluster in Ihrer Speicherumgebung werden angezeigt. Die Liste der Cluster ist nach der Spalte mit dem Schweregrad des Erfassungsstatus sortiert. Sie können auf eine Spaltenüberschrift klicken, um die Cluster nach verschiedenen Spalten zu sortieren.

Cluster hinzufügen

Sie können Active IQ Unified Manager einen Cluster hinzufügen, damit Sie den Cluster überwachen können. Dazu gehört die Möglichkeit, Clusterinformationen wie Zustand, Kapazität, Leistung und Konfiguration des Clusters abzurufen, sodass Sie eventuell auftretende Probleme finden und beheben können.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen über die folgenden Informationen verfügen:
  - Unified Manager unterstützt lokale ONTAP -Cluster, ONTAP Select und Cloud Volumes ONTAP.
  - Sie müssen über den Hostnamen oder die Cluster-Verwaltungs-IP-Adresse (IPv4 oder IPv6) für den Cluster verfügen.

    Bei Verwendung des Hostnamens muss dieser in die Cluster-Management-IP-Adresse für das Cluster-Management-LIF aufgelöst werden. Wenn Sie ein Knotenverwaltungs-LIF verwenden, schlägt der Vorgang fehl.
  - Sie müssen über den Benutzernamen und das Kennwort verfügen, um auf den Cluster zugreifen zu können.

    Dieses Konto muss über die Rolle *admin* verfügen und der Anwendungszugriff muss auf *ontapi*, *console* und *http* eingestellt sein.
  - Sie müssen die Portnummer kennen, um über das HTTPS-Protokoll eine Verbindung zum Cluster herzustellen (normalerweise Port 443).
  - Auf dem Cluster muss die ONTAP Softwareversion 9.9 oder höher ausgeführt werden.
  - Sie müssen über ausreichend Speicherplatz auf dem Unified Manager-Server verfügen. Sie können dem Server keinen Cluster hinzufügen, wenn bereits mehr als 90 % des Speicherplatzes belegt sind.
  - Sie verfügen über die erforderlichen Zertifikate:

    SSL (HTTPS)-Zertifikat: Dieses Zertifikat ist Eigentum von Unified Manager. Bei einer Neuinstallation von Unified Manager wird ein standardmäßiges selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt, zur besseren Sicherheit ein Upgrade auf ein CA-signiertes Zertifikat durchzuführen. Wenn das Serverzertifikat abläuft, sollten Sie es neu generieren und Unified Manager neu starten, damit die Dienste das neue Zertifikat integrieren. Weitere Informationen zum Neugenerieren von SSL-Zertifikaten finden Sie unter"Generieren eines HTTPS-Sicherheitszertifikats" .

    EMS-Zertifikat: Dieses Zertifikat ist Eigentum von Unified Manager. Es wird während der Authentifizierung für von ONTAP empfangene EMS-Benachrichtigungen verwendet.

    Zertifikate für gegenseitige TLS-Kommunikation: Wird während der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatsbasierte Authentifizierung ist für einen Cluster basierend auf der ONTAP -Version aktiviert. Wenn auf dem Cluster eine niedrigere ONTAP Version als 9.5 ausgeführt wird, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

    Die zertifikatbasierte Authentifizierung wird für einen Cluster nicht automatisch aktiviert, wenn Sie eine ältere Version von Unified Manager aktualisieren. Sie können es jedoch aktivieren, indem Sie die Clusterdetails ändern und speichern. Wenn das Zertifikat abläuft, sollten Sie es neu generieren, um das neue Zertifikat zu integrieren. Weitere Informationen zum Anzeigen und Neugenerieren des

Zertifikats finden Sie unter"Cluster bearbeiten" .

- Sie können einen Cluster über die Web-Benutzeroberfläche hinzufügen und die zertifikatbasierte Authentifizierung wird automatisch aktiviert.
- Sie können einen Cluster über die Unified Manager CLI hinzufügen. Die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie einen Cluster mithilfe der Unified Manager-CLI hinzufügen, müssen Sie den Cluster mithilfe der Unified Manager-Benutzeroberfläche bearbeiten. Sie können sehen"Unterstützte Unified Manager CLI-Befehle" um einen Cluster mithilfe der Unified Manager CLI hinzuzufügen.
- Wenn die zertifikatbasierte Authentifizierung für einen Cluster aktiviert ist und Sie die Sicherung von Unified Manager von einem Server nehmen und auf einem anderen Unified Manager-Server wiederherstellen, auf dem der Hostname oder die IP-Adresse geändert wurde, kann die Überwachung des Clusters fehlschlagen. Um den Fehler zu vermeiden, bearbeiten und speichern Sie die Clusterdetails. Weitere Informationen zum Bearbeiten von Clusterdetails finden Sie unter"Cluster bearbeiten" .
- Auf Clusterebene fügt die Active IQ Schnittstelle zwei neue Benutzergruppeneinträge für die Authentifizierungsmethode „cert“ hinzu.

+
Cluster-Zertifikate: Dieses Zertifikat ist Eigentum von ONTAP. Sie können Unified Manager keinen Cluster mit einem abgelaufenen Zertifikat hinzufügen. Wenn das Zertifikat bereits abgelaufen ist, sollten Sie es vor dem Hinzufügen des Clusters neu generieren. Informationen zur Zertifikatsgenerierung finden Sie im Knowledge Base-Artikel (KB). "So erneuern Sie ein selbstsigniertes ONTAP -Zertifikat 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. Eine Liste der unterstützten Knotenanzahl finden Sie im "Leitfaden zu Best Practices für Unified Manager" .

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.
2. Klicken Sie auf der Seite „Cluster-Setup“ auf **Hinzufügen**.
3. Geben Sie im Dialogfeld „Cluster hinzufügen“ die erforderlichen Werte an und klicken Sie dann auf **Senden**.
4. Klicken Sie im Dialogfeld „Host autorisieren“ auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
5. Klicken Sie auf **Ja**.

   Nachdem Sie die Clusterdetails gespeichert haben, können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für einen Cluster sehen.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, überprüft Unified Manager das Zertifikat nur, wenn der Cluster zum ersten Mal hinzugefügt wird. Unified Manager überprüft 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 Leistungsdaten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Datenkontinuitätserfassung erfasst. Mit dieser Funktion erhalten Sie unmittelbar nach dem Hinzufügen eines

Clusters Leistungsinformationen für mehr als zwei Wochen. Nachdem der Datenkontinuitätserfassungszyklus abgeschlossen ist, werden standardmäßig alle fünf Minuten Echtzeitdaten zur Clusterleistung erfasst.

- Die Erfassung von Leistungsdaten für 15 Tage ist CPU-intensiv. NetApp empfiehlt, das Hinzufügen neuer Cluster zeitlich zu staffeln, damit die Abfragen zur Datenkontinuitätserfassung nicht auf zu vielen Clustern gleichzeitig ausgeführt werden. Wenn Sie Unified Manager während des Datenkontinuitätserfassungszeitraums neu starten, wird die Erfassung angehalten und Sie sehen Lücken in den Leistungsdiagrammen für den fehlenden Zeitraum.
- Wenn Sie einen ONTAP Cluster mit Version 9.14.1 oder höher hinzufügen, erfolgt die Kommunikation über die Cloud-Agent-Funktion. ONTAP erstellt automatisch einen internen Servicekontobenutzer mit schreibgeschützten Berechtigungen (z. B. clus-agent-xxxx). Unified Manager stoppt die Datenerfassung aus diesen Clustern, wenn `clus-agent` Benutzer wird gelöscht.

Wenn Sie eine Fehlermeldung erhalten, dass Sie den Cluster nicht hinzufügen können, überprüfen Sie, ob die 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. Sie müssen sicherstellen, dass die Uhren über NTP oder einen ähnlichen Dienst synchronisiert werden.
- Wenn der Cluster die maximale Anzahl an EMS-Benachrichtigungszielen erreicht hat, kann die Unified Manager-Adresse nicht hinzugefügt werden. Standardmäßig können auf dem Cluster nur 20 EMS-Benachrichtigungsziele definiert werden.

Verwandte Informationen

"Benutzer hinzufügen"

"Anzeigen der Clusterliste und Details"

"Installieren eines von einer Zertifizierungsstelle signierten und zurückgegebenen HTTPS-Zertifikats"

Cluster bearbeiten

Sie können die Einstellungen eines vorhandenen Clusters, wie etwa Hostname oder IP-Adresse, Benutzername, Kennwort und Port, mithilfe des Dialogfelds „Cluster bearbeiten“ ändern.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Ab Unified Manager 9.7 können Cluster nur noch über HTTPS hinzugefügt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.
2. Wählen Sie auf der Seite **Cluster-Setup** den Cluster aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Cluster bearbeiten** die Werte nach Bedarf. + Wenn Sie die Details für einen zu Unified Manager hinzugefügten Cluster geändert haben, können Sie die Zertifikatsdetails für die

gegenseitige TLS-Kommunikation basierend auf der ONTAP Version anzeigen. Weitere Informationen zur ONTAP -Version finden Sie unter"Zertifikate für die gegenseitige TLS-Kommunikation" . + Sie können die Zertifikatsdetails anzeigen, indem Sie auf **Zertifikatsdetails** klicken. Wenn das Zertifikat abgelaufen ist, klicken Sie auf die Schaltfläche **Neu generieren**, um das neue Zertifikat einzubinden.

4. Klicken Sie auf **Senden**.
5. Klicken Sie im Dialogfeld „Host autorisieren“ auf **Zertifikat anzeigen**, um die Zertifikatsinformationen zum Cluster anzuzeigen.
6. Klicken Sie auf **Ja**.

Verwandte Informationen

"Benutzer hinzufügen"

"Anzeigen der Clusterliste und Details"

Cluster entfernen

Sie können einen Cluster über die Seite „Cluster-Setup“ aus Unified Manager entfernen. Sie können beispielsweise einen Cluster entfernen, wenn die Clustererkennung fehlschlägt oder wenn Sie ein Speichersystem außer Betrieb nehmen möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Diese Aufgabe entfernt den ausgewählten Cluster aus Unified Manager. Nachdem ein Cluster entfernt wurde, wird er nicht mehr überwacht. Die beim entfernten Cluster registrierte Instanz von Unified Manager wird ebenfalls vom Cluster abgemeldet.

Durch das Entfernen eines Clusters werden auch alle zugehörigen Speicherobjekte, Verlaufsdaten, Speicherdienste und alle zugehörigen Ereignisse aus Unified Manager gelöscht. Diese Änderungen werden nach dem nächsten Datenerfassungszyklus auf den Inventarseiten und den Detailseiten angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.
2. Wählen Sie auf der Seite „Cluster-Setup“ den Cluster aus, den Sie entfernen möchten, und klicken Sie auf **Entfernen**.
3. Klicken Sie im Meldungsdialogfeld **Datenquelle entfernen** auf **Entfernen**, um die Entfernungsanforderung zu bestätigen.

Verwandte Informationen

"Benutzer hinzufügen"

"Anzeigen der Clusterliste und Details"

Cluster neu entdecken

Sie können einen Cluster manuell über die Seite „Cluster-Setup“ erneut erkennen, um die neuesten Informationen zum Zustand, Überwachungsstatus und Leistungsstatus des Clusters zu erhalten.

Sie können einen Cluster manuell erneut erkennen, wenn Sie ihn aktualisieren möchten – etwa durch Erhöhen der Größe eines Aggregats, wenn nicht genügend Speicherplatz vorhanden ist – und Unified Manager die von Ihnen vorgenommenen Änderungen erkennen soll.

Wenn Unified Manager mit OnCommand Workflow Automation (WFA) gekoppelt wird, löst die Kopplung die erneute Erfassung der von WFA zwischengespeicherten Daten aus.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.
2. Klicken Sie auf der Seite **Cluster-Setup** auf **Neu erkennen**.

   Unified Manager erkennt den ausgewählten Cluster erneut und zeigt den neuesten Integritäts- und Leistungsstatus an.

Verwandte Informationen

"Anzeigen der Clusterliste und Details"

Überwachen Sie die virtuelle VMware-Infrastruktur

Active IQ Unified Manager bietet Einblick in die virtuellen Maschinen (VMs) in Ihrer virtuellen Infrastruktur und ermöglicht die Überwachung und Fehlerbehebung bei Speicher- und Leistungsproblemen in Ihrer virtuellen Umgebung. Sie können diese Funktion verwenden, um Latenzprobleme in Ihrer Speicherumgebung zu ermitteln oder wenn ein Leistungsereignis auf Ihrem vCenter Server gemeldet wird.

Eine typische Bereitstellung einer virtuellen Infrastruktur auf ONTAP umfasst verschiedene Komponenten, die über die Rechen-, Netzwerk- und Speicherebenen verteilt sind. Leistungsverzögerungen in einer VM-Anwendung können durch eine Kombination von Latenzen entstehen, denen die verschiedenen Komponenten auf den jeweiligen Ebenen ausgesetzt sind. Diese Funktion ist nützlich für Speicher- und vCenter Server-Administratoren und IT-Generalisten, die ein Leistungsproblem in einer virtuellen Umgebung analysieren und herausfinden müssen, in welcher Komponente das Problem aufgetreten ist.

Sie können jetzt über das vCenter-Menü des VMware-Bereichs auf den vCenter-Server zugreifen. Die Vorschau jeder aufgelisteten virtuellen Maschine verfügt über den Link **VCENTER SERVER** in der TOPOLOGIE-ANSICHT, der den vCenter Server in einem neuen Browser startet. Sie können auch die Schaltfläche **Topologie erweitern** verwenden, um den vCenter Server zu starten, und auf die Schaltfläche **In vCenter anzeigen** klicken, um die Datenspeicher im vCenter Server anzuzeigen.

Unified Manager stellt das zugrunde liegende Subsystem einer virtuellen Umgebung in einer topologischen Ansicht dar, um festzustellen, ob im Rechenknoten, Netzwerk oder Speicher ein Latenzproblem aufgetreten ist. Die Ansicht hebt außerdem das spezifische Objekt hervor, das die Leistungsverzögerung verursacht, damit Abhilfemaßnahmen ergriffen und das zugrunde liegende Problem behoben werden kann.

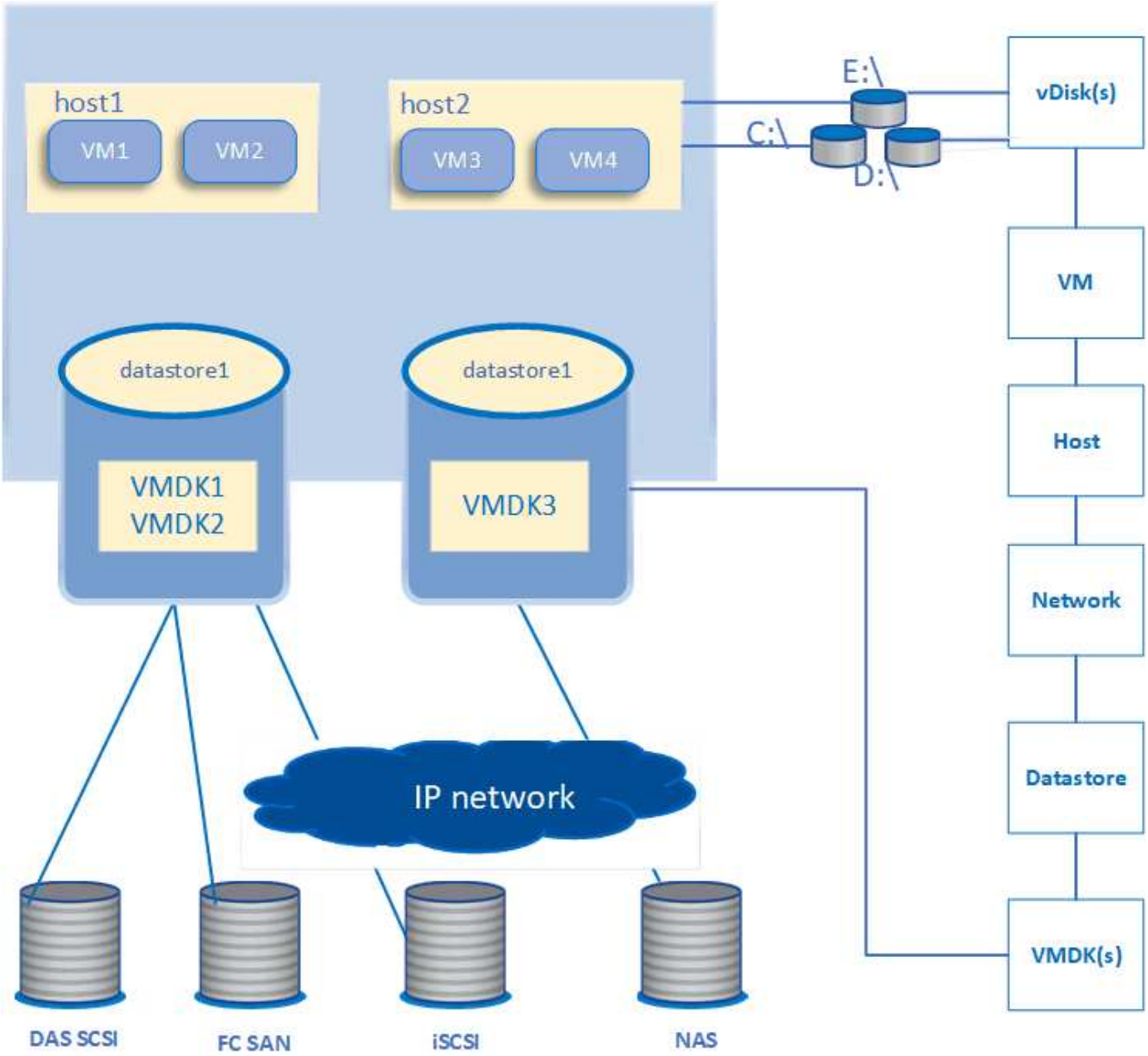
Eine auf ONTAP -Speicher bereitgestellte virtuelle Infrastruktur umfasst die folgenden Objekte:

- vCenter Server: Eine zentrale Steuerungsebene zum Verwalten der VMware-VMs, ESXi-Hosts und aller zugehörigen Komponenten in einer virtuellen Umgebung. Weitere Informationen zu vCenter Server finden Sie in der VMware-Dokumentation.
- Host: Ein physisches oder virtuelles System, auf dem ESXi, die Virtualisierungssoftware von VMware, ausgeführt wird und das die VM hostet.

- Datenspeicher: Datenspeicher sind virtuelle Speicherobjekte, die mit den ESXi-Hosts verbunden sind. Datenspeicher sind verwaltbare Speichereinheiten von ONTAP, wie LUNs oder Volumes, die als Repository für VM-Dateien wie Protokolldateien, Skripts, Konfigurationsdateien und virtuelle Datenträger verwendet werden. Sie sind über eine SAN- oder IP-Netzwerkverbindung mit den Hosts in der Umgebung verbunden. Datenspeicher außerhalb von ONTAP , die vCenter Server zugeordnet sind, werden im Unified Manager nicht unterstützt oder angezeigt.
- VM: Eine virtuelle VMware-Maschine.
- Virtuelle Datenträger: Die virtuellen Datenträger auf den Datenspeichern der VMs, die die Erweiterung VMDK haben. Daten von einer virtuellen Festplatte werden auf der entsprechenden VMDK gespeichert.
- VMDK: Eine virtuelle Maschinenfestplatte im Datenspeicher, die Speicherplatz für virtuelle Festplatten bereitstellt. Für jede virtuelle Festplatte gibt es ein entsprechendes VMDK.

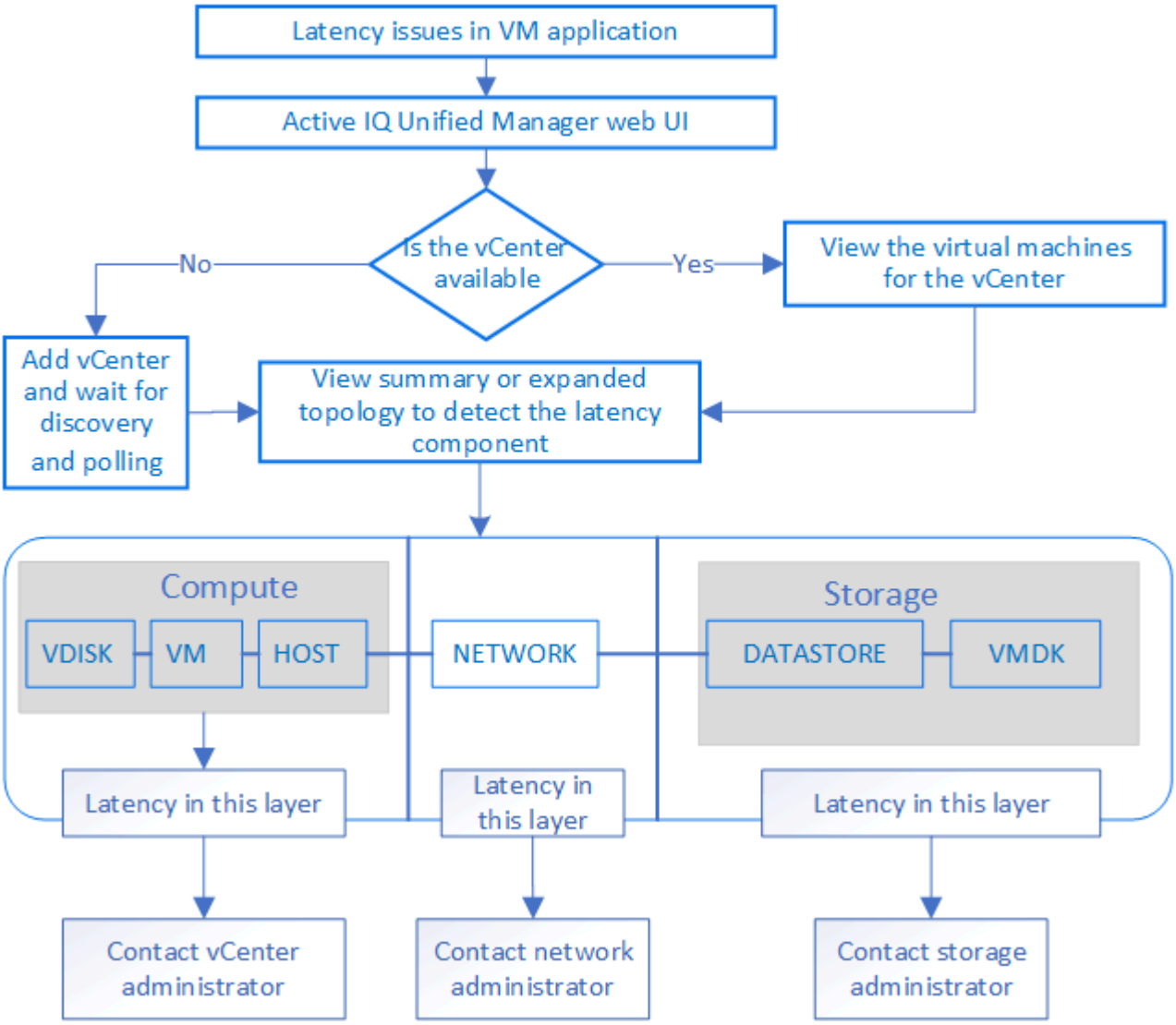
Diese Objekte werden in einer VM-Topologieansicht dargestellt.

VMware-Virtualisierung auf ONTAP



Benutzer-Workflow

Das folgende Diagramm zeigt einen typischen Anwendungsfall für die Verwendung der VM-Topologieansicht:



Was wird nicht unterstützt?

- Datenspeicher außerhalb von ONTAP , die den vCenter Server-Instanzen zugeordnet sind, werden von Unified Manager nicht unterstützt. VMs mit virtuellen Datenträgern auf diesen Datenspeichern werden ebenfalls nicht unterstützt.
- Ein Datenspeicher, der sich über mehrere LUNs erstreckt, wird nicht unterstützt.
- Datenspeicher, die Network Address Translation (NAT) zum Zuordnen von Daten-LIF (Zugriffsendpunkt) verwenden, werden nicht unterstützt.
- Das Exportieren von Volumes oder LUNs als Datenspeicher auf verschiedenen Clustern mit denselben IP-Adressen in einer Konfiguration mit mehreren LIFs wird nicht unterstützt, da Unified Manager nicht erkennen kann, welcher Datenspeicher zu welchem Cluster gehört.

  Beispiel: Angenommen, Cluster A hat Datenspeicher A. Datenspeicher A wird über Daten-LIF mit derselben IP-Adresse xxxx exportiert und VM A wird auf diesem Datenspeicher erstellt. Ebenso hat Cluster B den Datenspeicher B. Der Datenspeicher B wird über Daten-LIF mit derselben IP-Adresse xxxx exportiert und VM B wird auf dem Datenspeicher B erstellt. UM kann weder den Datenspeicher A für die

Topologie von VM A dem entsprechenden ONTAP Volume/LUN zuordnen noch VM B zuordnen.

- Als Datenspeicher werden nur NAS- und SAN-Volumes (iSCSI und FCP für VMFS) unterstützt, virtuelle Volumes (vVols) werden nicht unterstützt.
- Es werden nur virtuelle iSCSI-Festplatten unterstützt. Virtuelle Festplatten vom Typ NVMe und SATA werden nicht unterstützt.
- Die Ansichten ermöglichen nicht die Erstellung von Berichten zur Analyse der Leistung der verschiedenen Komponenten.
- Für die Notfallwiederherstellung (DR) der Storage Virtual Machine (Storage VM), die nur für virtuelle Infrastrukturen auf Unified Manager unterstützt wird, muss die Konfiguration in vCenter Server manuell geändert werden, um in Switchover- und Switchback-Szenarien auf die aktiven LUNs zu verweisen. Ohne manuelles Eingreifen sind ihre Datenspeicher nicht mehr zugänglich.

Anzeigen und Hinzufügen von vCenter Server

Um die Leistung der virtuellen Maschinen (VMs) anzuzeigen und Fehler zu beheben, müssen die zugehörigen vCenter-Server zu Ihrer Active IQ Unified Manager Instanz hinzugefügt werden.

Bevor Sie beginnen

Stellen Sie vor dem Hinzufügen oder Anzeigen von vCenter-Servern Folgendes sicher:

- Sie kennen die Namen der vCenter-Server.
- Sie kennen die IP-Adresse des vCenter Servers und verfügen über die erforderlichen Anmeldeinformationen. Die Anmeldeinformationen müssen von einem vCenter Server-Administrator oder einem Root-Benutzer mit schreibgeschütztem Zugriff auf vCenter Server stammen.
- Auf dem vCenter Server, den Sie hinzufügen möchten, wird vSphere 6.5 oder höher ausgeführt.

  Der Support von Unified Manager für VMware ESXi und vCenter Server ist in englischer und japanischer Sprache verfügbar.

- Die Datenerfassungseinstellung in vCenter Server ist auf die Statistikebene von *`Level 3`*, wodurch das erforderliche Maß an Metrikerfassung für alle überwachten Objekte sichergestellt wird. Die Intervalldauer sollte *`5 minutes`* und der Speicherzeitraum sollte *`1 day`*.

  Weitere Informationen finden Sie im Abschnitt „Datenerfassungsebenen“ des vSphere-Überwachungs- und Leistungshandbuchs in der VMware-Dokumentation.

- Für eine erfolgreiche Berechnung der Latenzwerte werden die Latenzwerte im vCenter Server in Millisekunden und nicht in Mikrosekunden konfiguriert.
- Beim Hinzufügen des Datenspeichers zu vCenter Server können Sie sowohl die IP-Adresse des Hosts als auch den vollqualifizierten Domänennamen (FQDN) verwenden. Wenn Sie FQDN hinzufügen, stellen Sie sicher, dass der Domänenname vom Unified Manager-Server aufgelöst werden kann. Stellen Sie beispielsweise bei einer Linux-Installation sicher, dass der Domänenname in der `/etc/resolv.conf` Datei.
- Die aktuelle Uhrzeit des vCenter Servers ist mit der Zeitzone des vCenter Servers 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 sammelt Unified Manager die Konfigurationsdaten, z. B. die vCenter Server- und ESXi-Serverdetails, die ONTAP Zuordnung, Datenspeicherdetails und die Anzahl der gehosteten VMs. Darüber hinaus werden die Leistungskennzahlen der Komponenten erfasst.

Schritte

1. Gehen Sie zu **VMWARE** > **vCenter** und prüfen Sie, ob Ihr vCenter Server in der Liste verfügbar ist.

   Wenn Ihr vCenter Server nicht verfügbar ist, müssen Sie vCenter Server hinzufügen.

   a. Klicken Sie auf **Hinzufügen**.
   b. Fügen Sie die richtige IP-Adresse für vCenter Server hinzu und stellen Sie sicher, dass das Gerät erreichbar ist.
   c. Fügen Sie den Benutzernamen und das Kennwort des Administrators oder Root-Benutzers mit schreibgeschütztem Zugriff auf vCenter Server hinzu.
   d. Fügen Sie die benutzerdefinierte Portnummer hinzu, wenn Sie einen anderen Port als den Standardport 443 verwenden.
   e. Klicken Sie auf **Speichern**.

      Nach erfolgreicher Erkennung wird Ihnen ein Serverzertifikat angezeigt, das Sie akzeptieren müssen.

   Wenn Sie das Zertifikat akzeptieren, wird vCenter Server zur Liste der verfügbaren vCenter Server 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 Seite **vCenters** verfügbar ist, überprüfen Sie seinen Status, indem Sie mit der Maus über das Feld **Status** fahren, um anzuzeigen, 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 Leistungs- und Latenzdaten der entsprechenden VMs nach dem Hinzufügen von vCenter Server korrekt wiedergegeben werden.

   - Grün: „Normal“, was bedeutet, dass vCenter Server erkannt wurde und Leistungsmetriken erfolgreich erfasst wurden
   - Gelb: „Warnung“ (z. B. wenn die Statistikebene für vCenter Server nicht auf 3 oder höher eingestellt wurde, um Statistiken für jedes Objekt zu erhalten)
   - Orange: „Fehler“ (weist auf interne Fehler hin, z. B. Ausnahme, Fehler bei der Konfigurationsdatenerfassung oder Nichterreichbarkeit des vCenter-Servers). Sie können auf das Spaltenanzeigesymbol (**Einblenden/Ausblenden**) klicken, um die Statusmeldung für einen vCenter-Server-Status anzuzeigen und das Problem zu beheben.

3. Falls der vCenter-Server nicht erreichbar ist oder sich die Anmeldeinformationen geändert haben, bearbeiten Sie die vCenter-Serverdetails, indem Sie **vCenter** > **Bearbeiten** auswählen.
4. Nehmen Sie die erforderlichen Änderungen auf der Seite **VMware vCenter Server bearbeiten** vor.
5. Klicken Sie auf **Speichern**.

Die Datenerfassung auf vCenter Server beginnt

vCenter Server sammelt in Echtzeit 20-sekündige Leistungsdatenproben und fasst sie zu 5-Minuten-Proben

zusammen. Der Zeitplan für die Leistungsdatenerfassung von Unified Manager basiert auf den Standardeinstellungen von vCenter Server. Unified Manager verarbeitet die vom vCenter Server erhaltenen 5-Minuten-Beispiele und berechnet einen stündlichen Durchschnitt der IOPS und Latenz für die virtuellen Festplatten, VMs und Hosts. Für Datenspeicher berechnet Unified Manager einen stündlichen Durchschnitt der IOPS und Latenz aus von ONTAP erhaltenen Beispielen. Diese Werte stehen zu jeder vollen Stunde zur Verfügung. Die Leistungsmetriken sind nicht sofort nach dem Hinzufügen von vCenter Server verfügbar, sondern erst zu Beginn der nächsten Stunde. Die Abfrage der Leistungsdaten beginnt nach Abschluss eines Zyklus der Konfigurationsdatenerfassung.

Zum Abfragen von vCenter Server-Konfigurationsdaten folgt Unified Manager demselben Zeitplan wie zum Erfassen von Cluster-Konfigurationsdaten. Informationen zur Konfiguration von vCenter Server und zum Zeitplan für die Leistungsdatenerfassung finden Sie unter „Clusterkonfiguration und Aktivität zur Leistungsdatenerfassung“.

Verwandte Informationen

"Clusterkonfiguration und Leistungsdatenerfassungsaktivität"

Entfernen von vCenter Server

Sie können vCenter-Server aus Ihrer Active IQ Unified Manager Instanz entfernen. Sie können beispielsweise einen vCenter Server entfernen, wenn die vCenter Server-Erkennung fehlschlägt oder wenn er nicht mehr benötigt wird.

Durch das Entfernen eines vCenter-Servers werden auch alle auf diesem vCenter gehosteten virtuellen Maschinen (VMs) und deren Konfigurationsdaten gelöscht. Nachdem der vCenter Server entfernt wurde, wird er zusammen mit den zugehörigen Objekten und Verlaufsdaten nicht mehr überwacht. Diese Änderungen werden auf den Inventarseiten von vCenter und virtuellen Maschinen angezeigt.

Bevor Sie beginnen

Stellen Sie vor dem Entfernen von vCenter-Servern Folgendes sicher:

- Sie verfügen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“.
- Sie sollten die Namen der vCenter-Server und die jeweiligen zugehörigen IP-Adressen kennen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **VMWARE>vCenter**.
2. Wählen Sie auf der vCenters-Seite den vCenter Server aus, den Sie entfernen möchten, und klicken Sie auf **Entfernen**.
3. Klicken Sie im Meldungsdialogfeld **vCenter entfernen** auf **OK**, um die Entfernungsanforderung zu bestätigen.

Überwachen virtueller Maschinen

Bei Latenzproblemen bei den Anwendungen der virtuellen Maschine (VM) müssen Sie möglicherweise die VMs überwachen, um die Ursache zu analysieren und zu beheben. Die VMs sind verfügbar, wenn ihr vCenter Server und die ONTAP Cluster, die den VM-Speicher hosten, zu Unified Manager hinzugefügt werden.

Die Details der VMs sehen Sie auf der Seite **VMWARE** > > **Virtuelle Maschinen**. Es werden Informationen wie Verfügbarkeit, Status, genutzte und zugewiesene Kapazität, Netzwerklatenz sowie IOPS und Latenz der VM,

des Datenspeichers und des Hosts angezeigt. Bei einer VM, die mehrere Datenspeicher unterstützt, zeigt das Raster die Metriken des Datenspeichers mit der schlechtesten Latenz an, wobei ein Sternchensymbol (*) zusätzliche Datenspeicher anzeigt. Wenn Sie auf das Symbol klicken, werden die Metriken des zusätzlichen Datenspeichers angezeigt. Einige dieser Spalten stehen zum Sortieren und Filtern nicht zur Verfügung.

Zum Anzeigen einer VM und ihrer Details muss die Erkennung (Polling oder Metrikerfassung) 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 können Sie auch die detaillierte Topologie einer VM anzeigen und die Komponenten anzeigen, mit denen die VM verbunden ist, beispielsweise den Host, die virtuelle Festplatte und den damit verbundenen Datenspeicher. Die Topologieansicht zeigt die zugrunde liegenden Komponenten in ihren spezifischen Ebenen in der folgenden Reihenfolge an: **Virtuelle Festplatte** > **VM** > **Host** > **Netzwerk** > **Datenspeicher** > **VMDK**.

Sie können den E/A-Pfad und die Latenzen auf Komponentenebene aus topologischer Sicht bestimmen und feststellen, ob der Speicher die Ursache des Leistungsproblems 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 erhalten, die jede Komponente separat zusammen mit der Latenz dieser Komponente darstellt. Sie können eine Komponente auswählen, um den durch die Ebenen hervorgehobenen E/A-Pfad zu bestimmen.

Anzeigen der Übersichtstopologie

So ermitteln Sie Leistungsprobleme, indem Sie die VMs in einer Übersichtstopologie anzeigen:

1. Gehen Sie zu **VMWARE** > **Virtuelle Maschinen**.
2. Suchen Sie nach Ihrer VM, indem Sie ihren Namen in das Suchfeld eingeben. Sie können Ihre Suchergebnisse auch nach bestimmten Kriterien filtern, indem Sie auf die Schaltfläche **Filter** klicken. Wenn Sie Ihre VM jedoch nicht finden können, stellen Sie sicher, dass der entsprechende vCenter Server hinzugefügt und erkannt wurde.

   vCenter Server erlauben Sonderzeichen (wie %, &, *, $, #, @, !, \, /, :, *, ?, "`, <, >, |, ;, ') in den Namen von vSphere-Entitäten wie VM, Cluster, Datenspeicher, Ordner oder Datei. Der VMware vCenter Server und der ESX/ESXi-Server maskieren Sonderzeichen, die in den Anzeigenamen verwendet werden, nicht. Wenn der Name jedoch im Unified Manager verarbeitet wird, wird er anders angezeigt. Beispielsweise eine VM mit dem Namen `%$VC_AIQUM_clone_191124%` in vCenter Server wird angezeigt als `%25$VC_AIQUM_clone_191124%25` im Unified Manager. Sie müssen dieses Problem beachten, wenn Sie eine VM abfragen, deren Name Sonderzeichen enthält.

3. Überprüfen Sie den Status der VM. Die VM-Status werden vom vCenter Server abgerufen. Die folgenden Status sind verfügbar. Weitere Informationen zu diesen Status finden Sie in der VMware-Dokumentation.
   - Normal
   - Warnung
   - Alarm
   - Nicht überwacht
   - Unbekannt
4. Klicken Sie auf den Abwärtspfeil neben der VM, um die Übersichtsansicht der Topologie der Komponenten auf den Compute-, Netzwerk- und Speicherebenen anzuzeigen. Der Knoten mit Latenzproblemen wird hervorgehoben. Die Übersichtsansicht zeigt die schlechteste Latenz der Komponenten. Wenn eine VM

beispielsweise über mehr als eine virtuelle Festplatte verfügt, wird in dieser Ansicht die virtuelle Festplatte mit der schlechtesten Latenz aller virtuellen Festplatten angezeigt.

5. Um die Latenz und den Durchsatz des Datenspeichers über einen bestimmten Zeitraum zu analysieren, klicken Sie auf die Schaltfläche **Workload Analyzer** über dem Symbol des Datenspeicherobjekts. Sie gelangen zur Seite „Workload-Analyse“, wo Sie einen Zeitraum auswählen und die Leistungsdiagramme des Datenspeichers anzeigen können. Weitere Informationen zum Workload-Analyzer finden Sie unter *Fehlerbehebung bei Workloads mit dem Workload-Analyzer*.

Erweiterte Topologie anzeigen

Sie können zu jeder Komponente einzeln einen Drilldown durchführen, indem Sie die erweiterte Topologie der VM anzeigen.

Schritte

1. Klicken Sie in der Übersichtsansicht der Topologie auf **Topologie erweitern**. Sie können die detaillierte Topologie jeder Komponente separat mit den Latenzzahlen für jedes Objekt anzeigen. Wenn in einer Kategorie mehrere Knoten vorhanden sind, beispielsweise mehrere Knoten im Datenspeicher oder VMDK, wird der Knoten mit der schlimmsten Latenz rot hervorgehoben.
2. Um den E/A-Pfad eines bestimmten Objekts zu überprüfen, klicken Sie auf das Objekt, um den E/A-Pfad und die entsprechende Zuordnung anzuzeigen. Um beispielsweise die Zuordnung einer virtuellen Festplatte anzuzeigen, klicken Sie auf die virtuelle Festplatte, um ihre hervorgehobene Zuordnung zum jeweiligen VMDK anzuzeigen. Im Falle einer Leistungsverzögerung dieser Komponenten können Sie weitere Daten von ONTAP sammeln und das Problem beheben.

> Für VMDKs werden keine Metriken gemeldet. In der Topologie werden nur die VMDK-Namen und keine Metriken angezeigt.

Verwandte Informationen

"Fehlerbehebung bei Workloads mit dem Workload Analyzer"

Anzeigen der virtuellen Infrastruktur in einem Disaster Recovery-Setup

Sie können die Konfigurations- und Leistungsmetriken der in einer MetroCluster -Konfiguration oder einem Disaster Recovery-Setup (SVM DR) einer Storage Virtual Machine (Storage VM) gehosteten Datenspeicher anzeigen.

Auf Unified Manager können Sie die NAS-Volumes oder LUNs in einer MetroCluster -Konfiguration anzeigen, die als Datenspeicher in vCenter Server angeschlossen sind. Die in einer MetroCluster -Konfiguration gehosteten Datenspeicher werden in derselben topologischen Ansicht dargestellt wie ein Datenspeicher in einer Standardumgebung.

Sie können auch die NAS-Volumes oder LUNs in einer Speicher-VM-Notfallwiederherstellungskonfiguration anzeigen, die den Datenspeichern in vCenter Server zugeordnet sind.

Anzeigen von Datenspeichern in der MetroCluster -Konfiguration

Beachten Sie die folgenden Voraussetzungen, bevor Sie Datenspeicher in einer MetroCluster -Konfiguration anzeigen:

- Im Falle eines Switchovers und Switchbacks sollte die Erkennung der primären und sekundären Cluster des HA-Paares und der vCenter-Server abgeschlossen sein.

- Die primären und sekundären Cluster des HA-Paares und die vCenter-Server müssen von Unified Manager verwaltet werden.
- Die erforderliche Einrichtung muss auf ONTAP und vCenter Server abgeschlossen werden. Weitere Informationen finden Sie in der ONTAP und vCenter-Dokumentation.

  "ONTAP 9 Dokumentationscenter"

Führen Sie die folgenden Schritte aus, um Datenspeicher anzuzeigen:

1. Klicken Sie auf der Seite **VMWARE** > **Virtuelle Maschinen** auf die VM, die den Datenspeicher hostet. Klicken Sie auf den **Workload Analyzer** oder den Datastore-Objektlink. Im Standardszenario, wenn der primäre Standort, der das Volume oder die LUN hostet, wie erwartet funktioniert, können Sie die vServer-Clusterdetails des primären Standorts sehen.
2. Im Falle einer Katastrophe und einer anschließenden Umschaltung auf den sekundären Standort verweist der Datastore-Link auf die Leistungsmetriken des Volumes oder LUN im sekundären Cluster. Dies wird nach Abschluss des nächsten Cluster-Zyklus und der vServer-Erkennung (Erfassung) widergespiegelt.
3. Nach einem erfolgreichen Switchback spiegelt die Datenspeicherverknüpfung wieder die Leistungsmetriken des Volumes oder LUN im primären Cluster wider. Dies wird nach Abschluss des nächsten Cluster-Zyklus und der vServer-Erkennung angezeigt.

Anzeigen von Datenspeichern in der Konfiguration zur Notfallwiederherstellung von Speicher-VMs

Beachten Sie die folgenden Voraussetzungen, bevor Sie Datenspeicher in einer Storage-VM-Notfallwiederherstellungskonfiguration anzeigen:

- Im Falle eines Switchovers und Switchbacks sollte die Erkennung der primären und sekundären Cluster des HA-Paares und der vCenter-Server abgeschlossen sein.
- Sowohl der Quell- als auch der Zielcluster und die Speicher-VM-Peers sollten von Unified Manager verwaltet werden.
- Die erforderliche Einrichtung muss auf ONTAP und vCenter Server abgeschlossen werden.
  - Bei NAS-Datenspeichern (NFS und VMFS) umfassen die Schritte im Katastrophenfall das Hochfahren der sekundären Speicher-VM, das Überprüfen der Daten-LIFs und -Routen, das Herstellen verlorener Verbindungen auf vCenter Server und das Starten der VMs.

    Für eine Umschaltung zurück zum primären Standort sollten die Daten zwischen den Volumes synchronisiert werden, bevor der primäre Standort mit der Bereitstellung der Daten beginnt.

  - Für SAN-Datenspeicher (iSCSI und FC für VMFS) formatiert vCenter Server die gemountete LUN in einem VMFS-Format. Im Katastrophenfall umfassen die Schritte das Hochfahren der sekundären Speicher-VM und die Überprüfung der Daten-LIFs und -Routen. Wenn sich die iSCSI-Ziel-IPs von den primären LIFs unterscheiden, müssen sie manuell hinzugefügt werden. Die neuen LUNs sollten als Geräte unter dem iSCSI-Adapter des Speicheradapters des Hosts verfügbar sein. Anschließend sollten neue VMFS-Datenspeicher mit den neuen LUNs erstellt und die alten VMs mit neuen Namen registriert werden. Die VMs müssen betriebsbereit sein.

    Im Falle einer Wiederherstellung sollten die Daten zwischen den Volumes synchronisiert werden. Neue VMFS-Datenspeicher sollten erneut unter Verwendung der LUNs erstellt und die alten VMs mit neuen Namen registriert werden.

    Informationen zum Setup finden Sie in der ONTAP und vCenter Server-Dokumentation.

"ONTAP 9 Dokumentationscenter"

Führen Sie die folgenden Schritte aus, um Datenspeicher anzuzeigen:

1. Klicken Sie auf der Seite **VMWARE** > **Virtuelle Maschinen** auf das VM-Inventar, das den Datenspeicher hostet. Klicken Sie auf den Link zum Datenspeicherobjekt. Im Standardszenario können Sie die Leistungsdaten der Volumes und LUNs in der primären Storage-VM sehen.
2. Im Falle einer Katastrophe und einer anschließenden Umschaltung auf die sekundäre Speicher-VM verweist der Datenspeicher-Link auf die Leistungsmetriken des Volumes oder LUN in der sekundären Speicher-VM. Dies wird nach Abschluss des nächsten Cluster-Zyklus und der vServer-Erkennung (Erfassung) widergespiegelt.
3. Nach einem erfolgreichen Switchback spiegelt die Datenspeicherverknüpfung wieder die Leistungsmetriken des Volumes oder LUN in der primären Speicher-VM wider. Dies wird nach Abschluss des nächsten Cluster-Zyklus und der vServer-Erkennung angezeigt.

Nicht unterstützte Szenarien

- Beachten Sie bei einer MetroCluster -Konfiguration die folgenden Einschränkungen:
  - Cluster nur in der `NORMAL` Und `SWITCHOVER` Staaten werden aufgenommen. Andere Staaten, wie z. `PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK` , Und `NOT_REACHABLE` werden nicht unterstützt.
  - Sofern die automatische Umschaltung (ASO) nicht aktiviert ist, kann der sekundäre Cluster beim Ausfall des primären Clusters nicht erkannt werden und die Topologie verweist weiterhin auf das Volume oder die LUN im primären Cluster.
- Beachten Sie bei einer Storage-VM-Notfallwiederherstellungskonfiguration die folgende Einschränkung:
  - Eine Konfiguration mit aktiviertem Site Recovery Manager (SRM) oder Storage Replication Adapter (SRA) für eine SAN-Speicherumgebung wird nicht unterstützt.

Bereitstellen und Verwalten von Workloads

Die aktive Verwaltungsfunktion von Active IQ Unified Manager bietet Leistungsservicelevel, Speichereffizienzrichtlinien und Speicheranbieter-APIs für die Bereitstellung, Überwachung und Verwaltung von Speicher-Workloads in einem Rechenzentrum.

Unified Manager bietet diese Funktionalität standardmäßig. Sie können es unter **Speicherverwaltung** > **Funktionseinstellungen** deaktivieren, wenn Sie diese Funktion nicht verwenden möchten.

Wenn diese Option aktiviert ist, können Sie Workloads auf den ONTAP Clustern bereitstellen, die von Ihrer Instanz von Unified Manager verwaltet werden. Sie können den Workloads auch Richtlinien wie Leistungsservicelevel und Speichereffizienzrichtlinien zuweisen und Ihre Speicherumgebung basierend auf diesen Richtlinien verwalten.

Diese Funktion ermöglicht die folgenden Funktionen:

- Automatische Erkennung von Speicher-Workloads auf den hinzugefügten Clustern, was eine einfache Auswertung und Bereitstellung von Speicher-Workloads ermöglicht
- Bereitstellung von NAS-Workloads mit Unterstützung der Protokolle NFS und CIFS

- Bereitstellung von SAN-Workloads mit Unterstützung der iSCSI- und FCP-Protokolle
- Unterstützung für NFS- und CIFS-Protokolle auf derselben Dateifreigabe
- Verwaltung von Leistungsserviceleveln und Speichereffizienzrichtlinien
- Zuweisen von Leistungsserviceleveln und Speichereffizienzrichtlinien zu Speicher-Workloads

Mit den Optionen **Bereitstellung**, **Speicher** > **Workloads** und **Richtlinien** im linken Bereich der Benutzeroberfläche können Sie verschiedene Konfigurationen ändern.

Mit diesen Optionen können Sie die folgenden Funktionen ausführen:

- Zeigen Sie Speicher-Workloads auf der Seite **Speicher** > **Workloads** an.
- Erstellen Sie Speicher-Workloads auf der Seite „Workload bereitstellen“
- Erstellen und Verwalten von Leistungsservicelevels anhand von Richtlinien
- Erstellen und Verwalten von Speichereffizienzrichtlinien aus Richtlinien
- Weisen Sie Speicher-Workloads Richtlinien auf der Seite „Workloads“ zu.

Verwandte Informationen

"Richtlinienbasierte Speicherverwaltung"

Übersicht über Workloads

Eine Arbeitslast stellt die Eingabe-/Ausgabevorgänge (E/A) eines Speicherobjekts dar, beispielsweise eines Volumes oder einer LUN. Die Art und Weise der Speicherbereitstellung basiert auf den erwarteten Arbeitslastanforderungen. Workload-Statistiken werden von Active IQ Unified Manager erst verfolgt, wenn Datenverkehr zum und vom Speicherobjekt stattfindet. Beispielsweise sind die IOPS- und Latenzwerte der Arbeitslast verfügbar, nachdem Benutzer mit der Verwendung einer Datenbank- oder E-Mail-Anwendung begonnen haben.

Auf der Seite „Workloads“ wird eine Zusammenfassung der Speicher-Workloads der von Unified Manager verwalteten ONTAP Cluster angezeigt. Es bietet auf einen Blick kumulative Informationen zu den Speicher-Workloads, die dem Performance Service Level entsprechen, sowie zu den nicht konformen Speicher-Workloads. Darüber hinaus können Sie die gesamte, verfügbare und genutzte Kapazität und Leistung (IOPS) der Cluster in Ihrem Rechenzentrum beurteilen.

Es wird empfohlen, die Anzahl der Speicher-Workloads zu ermitteln, die nicht konform, nicht verfügbar oder von keinem Performance Service Level verwaltet werden, und die erforderlichen Maßnahmen zu ergreifen, um ihre Konformität, Kapazitätsnutzung und IOPS sicherzustellen.

Die Seite „Workloads“ enthält die folgenden zwei Abschnitte:

- Übersicht über Workloads: Bietet eine Übersicht über die Anzahl der Speicher-Workloads auf den von Unified Manager verwalteten ONTAP Clustern.
- Rechenzentrumsübersicht: Bietet eine Übersicht über die Kapazität und IOPS der Speicher-Workloads im Rechenzentrum. Die relevanten Daten werden auf Rechenzentrumsebene und für einzelne angezeigt.

Abschnitt „Workloads – Übersicht“

Der Abschnitt „Workloadsübersicht“ bietet auf einen Blick zusammengefasste Informationen zu den Speicher-Workloads. Der Status der Speicher-Workloads wird basierend auf zugewiesenen und nicht zugewiesenen Performance-Service-Levels angezeigt.

- **Zugewiesen**: Für Speicher-Workloads, denen Performance-Service-Level zugewiesen wurden, werden die folgenden Status gemeldet:
  - **Konform**: Die Leistung von Speicher-Workloads basiert auf den ihnen zugewiesenen Performance Service Levels. Wenn die Speicher-Workloads innerhalb der in den zugehörigen Performance Service Levels definierten Schwellenlatenz liegen, werden sie als „konform“ gekennzeichnet. Die konformen Arbeitslasten sind blau markiert.
  - **Nicht konform**: Während der Leistungsüberwachung werden Speicher-Workloads als „nicht konform“ markiert, wenn die Latenz der Speicher-Workloads die im zugehörigen Leistungs-Servicelevel definierte Schwellenlatenz überschreitet. Die nicht konformen Arbeitslasten sind orange markiert.
  - **Nicht verfügbar**: Speicher-Workloads werden als „nicht verfügbar“ markiert, wenn sie offline sind oder der entsprechende Cluster nicht erreichbar ist. Die nicht verfügbaren Workloads sind rot markiert.
- **Nicht zugewiesen**: Speicher-Workloads, denen kein Performance-Service-Level zugewiesen ist, werden als „nicht zugewiesen“ gemeldet. Die Nummer wird durch das Informationssymbol übermittelt.

Die Gesamtzahl der Arbeitslasten ist die Summe der zugewiesenen und nicht zugewiesenen Arbeitslasten.

Sie können auf die Gesamtzahl der in diesem Abschnitt angezeigten Workloads klicken und sie auf der Seite „Workloads“ anzeigen.

Der Unterabschnitt „Konformität nach Leistungsserviceleveln“ zeigt die Gesamtzahl der verfügbaren Speicherarbeitslasten an:

- Konform mit jedem Typ von Performance Service Level
- Bei denen eine Diskrepanz zwischen den zugewiesenen und den empfohlenen Performance Service Levels besteht

Abschnitt „Übersicht über das Rechenzentrum“

Der Abschnitt „Rechenzentrumsübersicht“ stellt die verfügbare und genutzte Kapazität sowie die IOPS für alle Cluster im Rechenzentrum grafisch dar. Mithilfe dieser Daten sollten Sie die Kapazität und IOPS der Speicher-Workloads verwalten. Der Abschnitt zeigt außerdem die folgenden Informationen zu den Speicherarbeitslasten aller Cluster an:

- Die gesamte, verfügbare und genutzte Kapazität für alle Cluster in Ihrem Rechenzentrum
- Die gesamten, verfügbaren und verwendeten IOPS für alle Cluster in Ihrem Rechenzentrum
- Die verfügbare und genutzte Kapazität basierend auf jedem Performance Service Level
- Die verfügbaren und genutzten IOPS basierend auf jedem Performance Service Level
- Der gesamte Speicherplatz und die IOPS, die von den Workloads verwendet werden, denen kein Performance Service Level zugewiesen ist

Wie die Kapazität und Leistung von Rechenzentren basierend auf Performance Service Levels berechnet wird

Die genutzte Kapazität und die IOPS werden im Hinblick auf die insgesamt genutzte Kapazität und Leistung aller Speicher-Workloads in den Clustern abgerufen.

Die verfügbaren IOPS werden basierend auf der erwarteten Latenz und den empfohlenen Leistungsserviceleveln auf den Knoten berechnet. Es umfasst die verfügbaren IOPS für alle Performance-Service-Levels, deren erwartete Latenz kleiner oder gleich ihrer eigenen erwarteten Latenz ist.

Die verfügbare Kapazität wird basierend auf der erwarteten Latenz und den empfohlenen Leistungsserviceleveln für Aggregate berechnet. Es umfasst die verfügbare Kapazität für alle Performance-Service-Levels, deren erwartete Latenz kleiner oder gleich ihrer eigenen erwarteten Latenz ist.

Arbeitslasten anzeigen

Wenn Sie Cluster zu Unified Manager hinzufügen, werden die Speicher-Workloads auf jedem Cluster automatisch erkannt und auf der Seite „Workloads“ angezeigt.

Unified Manager beginnt erst mit der Analyse der Workloads für Empfehlungen (empfohlene PSLs), nachdem die E/A-Vorgänge für die Speicher-Workloads gestartet wurden.

FlexGroup Volumina und ihre Bestandteile sind ausgeschlossen.

Übersicht über Workloads

Auf der Seite „Workloads-Übersicht“ wird die Übersicht über die Workloads im Rechenzentrum sowie die Speicherplatz- und Leistungsübersicht des Rechenzentrums angezeigt.

- **Arbeitslastübersicht**-Bereich: Zeigt die Gesamtzahl der Arbeitslasten und die Anzahl der Arbeitslasten mit oder ohne zugewiesene PSLs an. Außerdem wird die Aufschlüsselung der Arbeitslastanzahl für jede PSL angezeigt. Durch Klicken auf die Zählungen gelangen Sie zur Ansicht **Alle Workloads** mit den gefilterten Workloads. Sie können auch die Anzahl der Workloads anzeigen, die nicht der Systemempfehlung entsprechen, und ihnen die vom System empfohlenen PSLs zuweisen, indem Sie auf die Schaltfläche **Vom System empfohlene PSLs zuweisen** klicken.
- **Rechenzentrumsübersicht**-Bereich: Zeigt den verfügbaren und genutzten Speicherplatz (TiB) und die Leistung (IOPS) des Rechenzentrums an. Außerdem wird eine Aufschlüsselung des verfügbaren und verwendeten Speicherplatzes (TiB) und der Leistung (IOPS) aller Workloads unter jeder PSL angezeigt.

Ansicht „Alle Workloads“

Auf der Seite **Speicher > Workloads > Alle Workloads** werden die Speicher-Workloads aufgelistet, die mit den von Unified Manager verwalteten ONTAP Clustern verknüpft sind.

Für die neu erkannten Speicher-Workloads, bei denen keine E/A-Vorgänge stattgefunden haben, lautet der Status „Warten auf E/A“. Nachdem die E/A-Vorgänge für die Speicher-Workloads begonnen haben, beginnt Unified Manager mit der Analyse und der Workload-Status ändert sich in „Lernen …“. Nach Abschluss der Analyse (innerhalb von 24 Stunden nach Beginn der E/A-Vorgänge) werden die empfohlenen PSLs für die Speicher-Workloads angezeigt.

Auf der Seite können Sie Speicher-Workloads auch Storage Efficiency Policies (SEPs) und Performance Service Levels (PSLs) zuweisen. Sie können mehrere Aufgaben ausführen:

- Hinzufügen oder Bereitstellen von Speicherworkloads
- Anzeigen und Filtern der Liste der Workloads
- Zuweisen von PSLs zu Speicher-Workloads
- Bewerten Sie vom System empfohlene PSLs und weisen Sie sie Arbeitslasten zu
- Zuweisen von SEPs zu Speicher-Workloads

Hinzufügen oder Bereitstellen von Speicher-Workloads

Sie können die Speicher-Workloads zu unterstützten LUNs (die sowohl iSCSI- als auch FCP-Protokolle unterstützen), NFS-Dateifreigaben und SMB-Freigaben hinzufügen oder bereitstellen.

Schritte

1. Klicken Sie auf **Speicher > Workloads > Alle Workloads > Erstellen**.
2. Erstellen Sie Arbeitslasten. Weitere Informationen finden Sie unter"Bereitstellung und Verwaltung von Workloads" .

Anzeigen und Filtern von Workloads

Auf dem Bildschirm „Alle Workloads“ können Sie alle Workloads in Ihrem Rechenzentrum anzeigen oder anhand ihrer PSLs oder Namen nach bestimmten Speicher-Workloads suchen. Über das Filtersymbol können Sie bestimmte Bedingungen für Ihre Suche eingeben. Sie können nach verschiedenen Filterbedingungen suchen, beispielsweise nach dem Hostcluster oder der Speicher-VM. Die Option **Gesamtkapazität** ermöglicht das Filtern nach der Gesamtkapazität der Workloads (in MB). In diesem Fall kann die Anzahl der zurückgegebenen Workloads jedoch variieren, da die Gesamtkapazität auf Byte-Ebene verglichen wird.

Für jede Arbeitslast werden Informationen wie Hostcluster und Speicher-VM zusammen mit den zugewiesenen PSL und SEP angezeigt.

Auf der Seite können Sie auch die Leistungsdetails einer Arbeitslast anzeigen. Sie können detaillierte Informationen zu IOPS, Kapazität und Latenz der Arbeitslast anzeigen, indem Sie auf die Schaltfläche **Spalten auswählen/sortieren** klicken und bestimmte Spalten zur Anzeige auswählen. In der Spalte „Leistungsansicht“ werden die durchschnittlichen und Spitzen-IOPS für eine Arbeitslast angezeigt. Sie können auf das Symbol des Arbeitslastanalysators klicken, um die detaillierte IOPS-Analyse anzuzeigen.

Analysieren von Leistungs- und Kapazitätskriterien für eine Workload

Über die Schaltfläche **Arbeitslast analysieren** im Popup-Fenster **IOPS-Analyse** gelangen Sie zur Seite „Arbeitslastanalyse“, auf der Sie einen Zeitraum auswählen und die Latenz-, Durchsatz- und Kapazitätstrends für die ausgewählte Arbeitslast anzeigen können. Weitere Informationen zum Workload-Analyzer finden Sie unter"Fehlerbehebung bei Workloads mit dem Workload-Analyzer" .

Sie können Leistungsinformationen zu einer Arbeitslast anzeigen, um die Fehlerbehebung zu erleichtern, indem Sie in der Spalte **Leistungsansicht** auf das Balkendiagrammsymbol klicken. Um Leistungs- und Kapazitätsdiagramme auf der Seite „Arbeitslastanalyse“ anzuzeigen und das Objekt zu analysieren, klicken Sie auf die Schaltfläche **Arbeitslast analysieren**.

Weitere Informationen finden Sie unter "Welche Daten zeigt der Workload Analyzer an".

Zuweisen von Richtlinien zu Workloads

Sie können Speicher-Effizienzrichtlinien (SEPs) und Performance Service Levels (PSLs) mithilfe der verschiedenen Navigationsoptionen von der Seite „Alle Workloads“ aus Speicher-Workloads zuweisen.

Zuweisen von Richtlinien zu einer einzelnen Arbeitslast

Sie können einer einzelnen Arbeitslast entweder eine PSL oder eine SEP oder beides zuweisen. Gehen Sie folgendermaßen vor:

1. Wählen Sie die Arbeitslast aus.
2. Klicken Sie auf das Bearbeitungssymbol neben der Zeile und dann auf **Bearbeiten**.

   Die Felder **Zugewiesenes Leistungsservicelevel** und **Speichereffizienzrichtlinie** sind aktiviert.

3. Wählen Sie die gewünschte PSL oder SEP oder beides aus.
4. Klicken Sie auf das Häkchensymbol, um die Änderungen zu übernehmen.

Sie können auch eine Arbeitslast auswählen und auf **Weitere Aktionen** klicken, um die Richtlinien zuzuweisen.

Zuweisen von Richtlinien zu mehreren Speicher-Workloads

Sie können mehreren Speicher-Workloads gleichzeitig eine PSL oder ein SEP zuweisen. Gehen Sie folgendermaßen vor:

1. Aktivieren Sie die Kontrollkästchen für die Workloads, denen Sie die Richtlinie zuweisen möchten, oder wählen Sie alle Workloads in Ihrem Rechenzentrum aus.
2. Klicken Sie auf **Weitere Aktionen**.
3. Wählen Sie zum Zuweisen eines PSL **Performance Service Level zuweisen**. Wählen Sie zum Zuweisen eines SEP **Speichereffizienzrichtlinie zuweisen**. Es wird ein Popup angezeigt, in dem Sie die Richtlinie auswählen können.
4. Wählen Sie die entsprechende Richtlinie aus und klicken Sie auf **Übernehmen**. Die Anzahl der Workloads, denen die Richtlinien zugewiesen sind, wird angezeigt. Die Workloads, denen die Richtlinien nicht zugewiesen sind, werden ebenfalls mit 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 **Im Hintergrund ausführen** klicken und mit anderen Aufgaben fortfahren, während der Vorgang im Hintergrund ausgeführt wird. Wenn die Massenzuweisung abgeschlossen ist, können Sie den Abschlussstatus anzeigen. Wenn Sie eine PSL auf mehrere Workloads anwenden, können Sie keine weitere Anfrage auslösen, während der vorherige Job der Massenzuweisung ausgeführt wird.

Zuweisen von vom System empfohlenen PSLs zu Workloads

Sie können den Speicherarbeitslasten in einem Rechenzentrum, denen keine PSLs zugewiesen sind oder die nicht mit der Systemempfehlung übereinstimmen, vom System empfohlene PSLs zuweisen. Um diese Funktion zu verwenden, klicken Sie auf die Schaltfläche **Vom System empfohlene PSLs zuweisen**. Sie müssen keine bestimmten Workloads auswählen.

Die Empfehlung wird intern durch Systemanalysen ermittelt und für Workloads übersprungen, deren IOPS und andere Parameter nicht mit den Definitionen eines verfügbaren PSL übereinstimmen. Speicher-Workloads mit `Waiting for I/O` und Lernstatus sind ebenfalls ausgeschlossen.

Es gibt spezielle Schlüsselwörter, nach denen Unified Manager im Workload-Namen sucht, um die Systemanalyse zu überschreiben und eine andere PSL für den Workload zu empfehlen. Wenn der Name der Arbeitslast die Buchstaben „`ora`“ enthält, wird die **Extreme Performance**PSL empfohlen. Und wenn der Workload die Buchstaben „vm“ im Namen hat, wird die **Performance**PSL empfohlen.

Siehe auch den Knowledge Base (KB)-Artikel "ActiveIQ Unified Manager „Empfohlene Leistungsserviceebene des Systems zuweisen“ ist nicht anpassungsfähig an eine stark variable Arbeitslast"

Bereitstellen von Dateifreigabevolumes

Sie können auf der Seite „Workload bereitstellen“ Dateifreigabevolumes erstellen, die CIFS/SMB- und NFS-Protokolle auf einem vorhandenen Cluster und einer Storage Virtual Machine (Storage-VM) unterstützen.

Bevor Sie beginnen

- Die Speicher-VM muss über Speicherplatz für die Bereitstellung des Dateifreigabevolumes verfügen.
- Einer oder beide der SMB- und NFS-Dienste sollten auf Ihrer Speicher-VM aktiviert sein.
- Um den Performance Service Level (PSL) und die Storage Efficiency Policy (SEP) für die Arbeitslast auszuwählen und zuzuweisen, müssen die Richtlinien erstellt worden sein, bevor Sie mit der Erstellung der Arbeitslast beginnen.

Schritte

1. Fügen Sie auf der Seite **Workload bereitstellen** den Namen der Workload hinzu, die Sie erstellen möchten, und wählen Sie dann den Cluster aus der verfügbaren Liste aus.
2. Basierend auf dem von Ihnen ausgewählten Cluster filtert das Feld **STORAGE VM** die verfügbaren Speicher-VMs für diesen Cluster. Wählen Sie die erforderliche Speicher-VM aus der Liste aus.

   Basierend auf den auf der Speicher-VM unterstützten SMB- und NFS-Diensten wird die NAS-Option im Abschnitt „Hostinformationen“ aktiviert.

3. Weisen Sie im Abschnitt „Speicher und Optimierung“ die Speicherkapazität und PSL sowie optional einen SEP für die Arbeitslast zu.

   Die Spezifikationen für das SEP werden der LUN zugewiesen und die Definitionen für das PSL werden beim Erstellen auf die Arbeitslast angewendet.

4. Aktivieren Sie das Kontrollkästchen **Leistungsgrenzen erzwingen**, wenn Sie die PSL erzwingen möchten, die Sie der Arbeitslast zugewiesen haben.

   Durch die Zuweisung einer PSL zu einer Arbeitslast wird sichergestellt, dass das Aggregat, auf dem die Arbeitslast erstellt wird, die in der jeweiligen Richtlinie definierten Leistungs- und Kapazitätsziele unterstützen kann. Wenn beispielsweise einer Arbeitslast die PSL „Extreme Performance“ zugewiesen wird, sollte das Aggregat, auf dem die Arbeitslast bereitgestellt werden soll, in der Lage sein, die Leistungs- und Kapazitätsziele der Richtlinie „Extreme Performance“ zu unterstützen, beispielsweise SSD-Speicher.

   > Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird die PSL nicht auf die Arbeitslast angewendet und der Status der Arbeitslast wird auf dem Dashboard als „Nicht zugewiesen“ angezeigt.

5. Wählen Sie die Option **NAS**.

   Wenn die Option **NAS** nicht aktiviert ist, überprüfen Sie, ob die von Ihnen ausgewählte Speicher-VM SMB oder NFS oder beides unterstützt.

Wenn Ihre Speicher-VM sowohl für SMB- als auch für NFS-Dienste aktiviert ist, können Sie die Kontrollkästchen **Freigabe über NFS** und **Freigabe über SMB** aktivieren und eine Dateifreigabe erstellen, die sowohl NFS- als auch SMB-Protokolle unterstützt. Wenn Sie entweder eine SMB- oder eine CIFS-Freigabe erstellen möchten, aktivieren Sie nur das jeweilige Kontrollkästchen.

6. Geben Sie für NFS-Dateifreigabevolumes die IP-Adresse des Hosts oder Netzwerks an, um auf das Dateifreigabevolume zuzugreifen. Sie können durch Kommas getrennte Werte für mehrere Hosts eingeben.

   Beim Hinzufügen der Host-IP-Adresse wird eine interne Prüfung ausgeführt, um die Hostdetails mit der Speicher-VM abzugleichen, und die Exportrichtlinie für diesen Host wird erstellt oder, falls eine vorhandene Richtlinie vorhanden ist, wird sie 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 Funktion zum Festlegen von Regeln einzelner Richtlinien oder zum Wiederverwenden von Richtlinien durch die Bereitstellung bestimmter Richtlinienschlüssel ist verfügbar, wenn Sie die NFS-Freigabe mithilfe von APIs bereitstellen.

7. Geben Sie für eine SMB-Freigabe an, welche Benutzer oder Benutzergruppen auf die SMB-Freigabe zugreifen können, und weisen Sie die erforderlichen Berechtigungen zu. Für jede Benutzergruppe wird während der Erstellung der Dateifreigabe eine neue Zugriffskontrollliste (ACL) generiert.
8. Klicken Sie auf **Speichern**.

   Die Arbeitslast wird der Liste der Speicherarbeitslasten hinzugefügt.

Bereitstellen von LUNs

Sie können auf der Seite „Workload bereitstellen“ LUNs erstellen, die CIFS/SMB- und NFS-Protokolle auf einem vorhandenen Cluster und einer Storage Virtual Machine (Storage-VM) unterstützen.

Bevor Sie beginnen

- Die Speicher-VM muss über Speicherplatz für die Bereitstellung der LUN verfügen.
- Sowohl iSCSI als auch FCP müssen auf der Speicher-VM aktiviert sein, auf der Sie die LUN erstellen.
- Um den Performance Service Level (PSL) und die Storage Efficiency Policy (SEP) für die Arbeitslast auszuwählen und zuzuweisen, müssen die Richtlinien erstellt worden sein, bevor Sie mit der Erstellung der Arbeitslast beginnen.

Schritte

1. Fügen Sie auf der Seite **Workload bereitstellen** den Namen der Workload hinzu, die Sie erstellen möchten, und wählen Sie dann den Cluster aus der verfügbaren Liste aus.

   Basierend auf dem von Ihnen ausgewählten Cluster filtert das Feld **STORAGE VM** die verfügbaren Speicher-VMs für diesen Cluster.

2. Wählen Sie aus der Liste die Speicher-VM aus, die die iSCSI- und FCP-Dienste unterstützt.

   Basierend auf Ihrer Auswahl wird die SAN-Option im Abschnitt „Hostinformationen“ aktiviert.

3. Weisen Sie im Abschnitt **Speicher und Optimierung** die Speicherkapazität und PSL sowie optional den SEP für die Arbeitslast zu.

Die Spezifikationen für das SEP werden der LUN zugewiesen und die Definitionen für das PSL werden beim Erstellen auf die Arbeitslast angewendet.

4. Aktivieren Sie das Kontrollkästchen **Leistungsgrenzen erzwingen**, wenn Sie die zugewiesene PSL für die Arbeitslast erzwingen möchten.

   Durch die Zuweisung einer PSL zu einer Arbeitslast wird sichergestellt, dass das Aggregat, auf dem die Arbeitslast erstellt wird, die in der jeweiligen Richtlinie definierten Leistungs- und Kapazitätsziele unterstützen kann. Wenn beispielsweise einer Arbeitslast die PSL „Extreme Leistung“ zugewiesen wird, sollte das Aggregat, auf dem die Arbeitslast bereitgestellt werden soll, in der Lage sein, die Leistungs- und Kapazitätsziele der Richtlinie „Extreme Leistung“ zu unterstützen, beispielsweise SSD-Speicher.

   Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird die PSL nicht auf die Arbeitslast angewendet und der Status der Arbeitslast wird auf dem Dashboard als `unassigned`.

5. Wählen Sie die Option **SAN**. Wenn die Option **SAN** nicht aktiviert ist, überprüfen Sie, ob die von Ihnen ausgewählte Speicher-VM iSCSI und FCP unterstützt.
6. Wählen Sie das Host-Betriebssystem aus.
7. Geben Sie die Hostzuordnung an, um den Zugriff der Initiatoren auf die LUN zu steuern. Sie können vorhandene Initiatorgruppen (igroups) zuweisen oder neue igroups definieren und zuordnen.

   Wenn Sie beim Bereitstellen der LUN eine neue igroup erstellen, müssen Sie bis zum nächsten Erkennungszyklus (bis zu 15 Minuten) warten, bevor Sie sie verwenden können. Es wird daher empfohlen, eine vorhandene Igroup aus der Liste der verfügbaren Igroups zu verwenden.

   Wenn Sie eine neue Igroup erstellen möchten, wählen Sie die Schaltfläche **Neue Initiatorgruppe erstellen** und geben Sie die Informationen für die Igroup ein.

8. Klicken Sie auf **Speichern**.

   Die LUN wird der Liste der Speicher-Workloads hinzugefügt.

Leistungsservice-Levels

Mit einem Performance Service Level (PSL) können Sie die Leistungs- und Speicherziele für eine Arbeitslast definieren. Sie können einer Arbeitslast beim ersten Erstellen der Arbeitslast oder später durch Bearbeiten der Arbeitslast eine PSL zuweisen.

Die Verwaltung und Überwachung von Speicherressourcen basieren auf Service Level Objectives (SLOs). SLOs werden durch Service Level Agreements definiert, die auf der erforderlichen Leistung und Kapazität basieren. In Unified Manager beziehen sich SLOs auf die PSL-Definitionen der Anwendungen, die auf NetApp -Speicher ausgeführt werden. Speicherdienste unterscheiden sich anhand der Leistung und Nutzung der zugrunde liegenden Ressourcen. Eine PSL ist eine Beschreibung der Speicherdienstziele. Ein PSL ermöglicht dem Speicheranbieter, die Leistungs- und Kapazitätsziele für die Arbeitslast anzugeben. Wenn Sie einer Workload eine PSL zuweisen, wird die entsprechende Workload auf ONTAP anhand ihrer Leistungs- und Kapazitätsziele verwaltet. Jeder PSL wird durch Spitzen-, erwartete und absolute Mindest-IOPs sowie die erwartete Latenz bestimmt.

Unified Manager verfügt über die folgenden PSL-Typen:

- **Systemdefiniert**: Unified Manager bietet einige vorgefertigte Richtlinien, die nicht geändert werden können. Diese vordefinierten PSLs sind:

  - Extreme Leistung
  - Performance
  - Wert

    Die PSLs „Extreme Performance“, „Performance“ und „Value“ sind für die meisten gängigen Speicher-Workloads in einem Rechenzentrum anwendbar.

  Unified Manager bietet außerdem drei Performance Service Levels für Datenbankanwendungen. Dabei handelt es sich um PSLs mit extrem hoher Leistung, die Burst-IOPS unterstützen und für Datenbankanwendungen mit den höchsten Durchsatzanforderungen geeignet sind.

  - Extreme für Datenbankprotokolle
  - Extreme für gemeinsam genutzte Datenbankdaten
  - Extreme für Datenbankdaten
- **Benutzerdefiniert**: Wenn die vordefinierten Performance Service Levels Ihren Anforderungen nicht entsprechen, können Sie neue PSLs erstellen, die Ihren Anforderungen entsprechen. Weitere 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 Arbeitslasten vorgeschlagen werden, die höhere IOPs als Extreme erfordern. Die Workloads werden intern anhand ihrer IOPS, Kapazität und Latenz analysiert und für jeden dieser Workloads wird auf dem Bildschirm **Speicher > Workloads > Alle Workloads** ein Beyond Extreme PSL empfohlen. Sie können die PSLs auf die Workloads anwenden, um eine optimale Leistung sicherzustellen.

  Die IOPs-Parameter für die Workloads werden dynamisch generiert, abhängig vom Workload-Verhalten, und an den Namen der Beyond Extreme PSL im Format angehängt `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`. Wenn das System beispielsweise eine Arbeitslast ermittelt, die die Spitzen- und erwarteten IOPs aufweist, `106345` Und `37929` bzw. die für die Arbeitslast generierte Beyond Extreme PSL wird wie folgt benannt: `Beyond Extreme 106345 37929`. Obwohl diese PSLs vom System empfohlen werden, werden sie bei der Zuweisung zu Workloads als gekennzeichnet. `User-defined` im Typ.

Verwalten Sie Arbeitslasten durch die Zuweisung von PSLs

Sie können auf PSLs über die Seite **Richtlinien** > **Leistungs-Servicelevel** und mithilfe der APIs des Speicheranbieters zugreifen. Die Verwaltung von Speicher-Workloads durch die Zuweisung von PSLs ist praktisch, da Sie die Speicher-Workloads nicht einzeln verwalten müssen. Alle Änderungen können auch durch die Neuzuweisung einer anderen PSL verwaltet werden, anstatt sie einzeln zu verwalten. Unified Manager hilft Ihnen, Ihren Arbeitslasten PSLs basierend auf internen Bewertungen und Empfehlungen zuzuweisen.

Informationen zum Zuweisen systemseitig empfohlener PSLs zu Workloads finden Sie unter"Zuweisen von vom System empfohlenen PSLs zu Workloads"

Auf der Seite „Performance Service Levels“ werden die verfügbaren PSL-Richtlinien aufgelistet und Sie können diese hinzufügen, bearbeiten und löschen.

Sie können keine PSL ändern, die systemdefiniert ist oder die derzeit einer Arbeitslast zugewiesen ist. Sie können keine PSL löschen, die einer Arbeitslast zugewiesen ist oder die einzige verfügbare PSL ist.

Auf dieser Seite werden die folgenden Informationen angezeigt:

Feld	Beschreibung
Name	Name der PSL.
Typ	Ob die Richtlinie systemdefiniert oder benutzerdefiniert ist.
Erwartete IOPS/TB	Mindestanzahl an IOPS, die eine Anwendung voraussichtlich auf einer LUN oder Dateifreigabe ausführen kann. „Erwartete IOPS“ gibt die minimal erwarteten zugewiesenen IOPS basierend auf der zugewiesenen Größe des Speicherobjekts an.
Spitzen-IOPS/TB	Maximale Anzahl von IOPS, die eine Anwendung auf einer LUN oder Dateifreigabe ausführen kann. Peak IOPS gibt die maximal möglichen zugewiesenen IOPS an, basierend auf der Größe des zugewiesenen Speicherobjekts oder der Größe des verwendeten Speicherobjekts. Spitzen-IOPS basieren auf einer Zuweisungsrichtlinie. Die Zuweisungsrichtlinie lautet entweder „zugewiesener Speicherplatz“ oder „verwendeter Speicherplatz“. Wenn die Zuweisungsrichtlinie auf „zugewiesener Speicherplatz“ eingestellt ist, wird der Spitzen-IOPS basierend auf der Größe des Speicherobjekts berechnet. Wenn die Zuweisungsrichtlinie auf „Verwendeter Speicherplatz“ eingestellt ist, wird der Spitzen-IOPS basierend auf der im Speicherobjekt gespeicherten Datenmenge berechnet, wobei die Speichereffizienz berücksichtigt wird. Standardmäßig ist die Zuweisungsrichtlinie auf „genutzter Speicherplatz“ eingestellt.

Feld	Beschreibung
Absolutes Minimum an IOPS	Der absolute Mindest-IOPS-Wert wird als Überschreibung verwendet, wenn der erwartete IOPS-Wert unter diesem Wert liegt. Die Standardwerte der systemdefinierten PSLs sind die folgenden: • Extreme Leistung: Wenn erwartete IOPS >= 6144/TB, dann absolutes Minimum an IOPS = 1000 • Leistung: Wenn erwartete IOPS >= 2048/TB und < 6144/TB, dann absolutes Minimum an IOPS = 500 • Wert: Wenn die erwarteten IOPS >= 128/TB und < 2048/TB sind, dann ist der absolute Mindest-IOPS = 75 Die Standardwerte der systemdefinierten Datenbank-PSLs sind die folgenden: • Extrem für Datenbankprotokolle: Wenn erwartete IOPS >= 22528, dann absolutes Minimum an IOPS = 4000 • Extrem für gemeinsam genutzte Datenbankdaten: Wenn erwartete IOPS >= 16384, dann absolutes Minimum an IOPS = 2000 • Extrem für Datenbankdaten: Wenn erwartete IOPS >= 12288, dann absolutes Minimum an IOPS = 2000 Der höhere Wert des absoluten IOPS-Mindestwerts für benutzerdefinierte PSLs kann maximal 75.000 betragen. Der niedrigere Wert berechnet sich wie folgt: 1000/erwartete Latenz
Erwartete Latenz	Erwartete Latenz für Speicher-IOPS in Millisekunden pro Vorgang (ms/op).
Kapazität	Gesamte verfügbare und genutzte Kapazität in den Clustern.
Arbeitslasten	Anzahl der Speicher-Workloads, denen die PSL zugewiesen wurde.

Informationen dazu, wie die Spitzen-IOPS und die erwarteten IOPs dazu beitragen, eine konsistente differenzierte Leistung auf ONTAP Clustern zu erzielen, finden Sie im folgenden KB-Artikel:https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["Was ist Performance Budgeting?"]

Ereignisse, die für Workloads generiert werden, die den durch PSLs definierten Schwellenwert überschreiten

Beachten Sie, dass Unified Manager eines der folgenden Ereignisse generiert, um Sie auf ein potenzielles Leistungsproblem hinzuweisen, wenn die Arbeitslasten in der letzten Stunde 30 % der Zeit den erwarteten Latenzwert überschritten haben:

- Latenzschwelle für Workload-Volumen überschritten, wie in der Service-Level-Richtlinie für die Leistung definiert
- Der in der Service-Level-Richtlinie für die Leistung definierte Schwellenwert für die Arbeitslast-LUN-Latenz wurde überschritten.

Möglicherweise möchten Sie die Arbeitslast analysieren, um herauszufinden, was die höheren Latenzwerte verursacht.

Weitere Informationen finden Sie unter den folgenden Links:

- "Volumenereignisse"
- "Was passiert, wenn eine Leistungsschwellenrichtlinie verletzt wird?"
- "So nutzt Unified Manager die Workload-Latenz, um Leistungsprobleme zu identifizieren"
- "Was sind Performance-Ereignisse"

Systemdefinierte PSLs

Die folgende Tabelle enthält Informationen zu den systemdefinierten PSLs:

Leistungsservicelevel	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/op)	Spitzen-IOPS	Erwartete IOPS	Absolutes Minimum an IOPS
Extreme Leistung	Bietet extrem hohen Durchsatz bei sehr geringer Latenz Ideal für latenzempfindliche Anwendungen	1	12288	6144	1000
Performance	Bietet hohen Durchsatz bei geringer Latenz Ideal für Datenbank- und virtualisierte Anwendungen	2	4096	2048	500

Leistungsservicelevel	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/op)	Spitzen-IOPS	Erwartete IOPS	Absolutes Minimum an IOPS
Wert	Bietet hohe Speicherkapazität und moderate Latenz Ideal für Anwendungen mit hoher Kapazität wie E-Mail, Webinhalte, Dateifreigaben und Sicherungsziele	17	512	128	75
Extreme für Datenbankprotokolle	Bietet maximalen Durchsatz bei niedrigster Latenz. Ideal für Datenbankanwendungen, die Datenbankprotokolle unterstützen. Diese PSL bietet den höchsten Durchsatz, da Datenbankprotokolle extrem stoßweise auftreten und die Protokollierung ständig erforderlich ist.	1	45056	22528	4000

Leistungsservicelevel	Beschreibung und Anwendungsfall	Erwartete Latenz (ms/op)	Spitzen-IOPS	Erwartete IOPS	Absolutes Minimum an IOPS
Extreme für gemeinsam genutzte Datenbankdaten	Bietet einen sehr hohen Durchsatz bei geringster Latenz. Ideal für Datenbankanwendungen: Daten, die in einem gemeinsamen Datenspeicher gespeichert, aber datenbankübergreifend genutzt werden.	1	32768	16384	2000
Extreme für Datenbankdaten	Bietet hohen Durchsatz bei geringster Latenz. Ideal für Daten aus Datenbankanwendungen, wie Datenbanktabelleninformationen und Metadaten.	1	24576	12288	2000

Erstellen und Bearbeiten von Performance Service Levels

Wenn die systemdefinierten Performance-Service-Levels nicht Ihren Workload-Anforderungen entsprechen, können Sie Ihre eigenen Performance-Service-Levels erstellen, die für Ihre Workloads optimiert sind.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.
- Der Name des Performance Service Level muss eindeutig sein und Sie dürfen die folgenden reservierten Schlüsselwörter nicht verwenden:

  `Prime`, `Extreme` , `Performance` , `Value` , `Unassigned` , `Learning` , `Idle` , `Default` , Und `None` .

Sie erstellen und bearbeiten benutzerdefinierte Performance-Service-Levels auf der Seite „Performance-Service-Levels“, indem Sie die Service-Level-Ziele definieren, die Sie für die Anwendungen benötigen, die auf den Speicher zugreifen.

Sie können einen Performance-Servicelevel nicht ändern, wenn er aktuell einer Arbeitslast zugewiesen ist.

Schritte

1. Wählen Sie im linken Navigationsbereich unter **Einstellungen Richtlinien** > **Leistungsservicelevel** aus.
2. Klicken Sie auf der Seite **Performance-Service-Levels** auf die entsprechende Schaltfläche, je nachdem, ob Sie ein neues Performance-Service-Level erstellen oder ein vorhandenes Performance-Service-Level bearbeiten möchten.

Zu…	Befolgen Sie diese Schritte…
Erstellen eines neuen Performance-Service-Levels	Klicken Sie auf **Hinzufügen**.
Bearbeiten eines vorhandenen Performance-Service-Levels	Wählen Sie ein vorhandenes Performance-Service-Level aus und klicken Sie dann auf **Bearbeiten**.

   Die Seite zum Hinzufügen oder Bearbeiten eines Performance-Service-Levels wird angezeigt.

3. Passen Sie das Performance-Service-Level an, indem Sie die Leistungsziele angeben, und klicken Sie dann auf **Senden**, um das Performance-Service-Level zu speichern.

Sie können das neue oder geänderte Performance-Service-Level auf Workloads (LUNs, NFS-Dateifreigaben, CIFS-Freigaben) von der Seite „Workloads“ oder beim Bereitstellen eines neuen Workloads anwenden.

Verwalten von Speichereffizienzrichtlinien

Mit einer Storage Efficiency Policy (SEP) können Sie die Speichereffizienzmerkmale einer Arbeitslast definieren. Sie können einer Arbeitslast beim ersten Erstellen der Arbeitslast oder später durch Bearbeiten der Arbeitslast einen SEP zuweisen.

Zur Speichereffizienz gehört der Einsatz von Technologien wie Thin Provisioning, Deduplizierung und Datenkomprimierung, die die Speicherauslastung erhöhen und die Speicherkosten senken. Beim Erstellen von SEPs können Sie diese platzsparenden Technologien entweder einzeln oder zusammen verwenden, um maximale Speichereffizienz zu erreichen. Wenn Sie die Richtlinien mit Ihren Speicher-Workloads verknüpfen, werden ihnen die angegebenen Richtlinieneinstellungen zugewiesen. Mit Unified Manager können Sie systemdefinierte und benutzerdefinierte SEPs zuweisen, um die Speicherressourcen in Ihrem Rechenzentrum zu optimieren.

Unified Manager bietet zwei systemdefinierte SEPs: High und Low. Diese SEPs sind auf die meisten Speicher-Workloads in einem Rechenzentrum anwendbar. Sie können jedoch Ihre eigenen Richtlinien erstellen, wenn die systemdefinierten SEPs Ihren Anforderungen nicht entsprechen.

Sie können einen SEP, der systemdefiniert ist oder derzeit einer Arbeitslast zugewiesen ist, nicht ändern. Sie können keinen SEP löschen, der einer Arbeitslast zugewiesen ist oder der einzige verfügbare SEP ist.

Auf der Seite „Speichereffizienzrichtlinien“ werden die verfügbaren SEPs aufgelistet und Sie können benutzerdefinierte SEPs hinzufügen, bearbeiten und löschen. Auf dieser Seite werden die folgenden Informationen angezeigt:

Feld	Beschreibung
Name	Name des SEP.
Typ	Ob die Richtlinie systemdefiniert oder benutzerdefiniert ist.
Platzreserve	Ob das Volume Thin Provisioning oder Thick Provisioning ist.
Deduplizierung	Ob die Deduplizierung für die Arbeitslast aktiviert ist: • Inline: Die Deduplizierung erfolgt während des Schreibens auf die Arbeitslast • Hintergrund: Deduplizierung erfolgt im Workload • Deaktivieren: Die Deduplizierung ist für die Arbeitslast deaktiviert
Komprimierung	Ob die Datenkomprimierung für die Arbeitslast aktiviert ist: • Inline: Die Datenkomprimierung erfolgt während des Schreibens in die Arbeitslast • Hintergrund: Die Datenkomprimierung erfolgt im Workload • Deaktivieren: Die Datenkomprimierung ist für die Arbeitslast deaktiviert
Arbeitslasten	Anzahl der Speicher-Workloads, denen das SEP zugewiesen wurde

Richtlinien zum Erstellen einer benutzerdefinierten Speichereffizienzrichtlinie

Wenn die vorhandenen SEPs die Richtlinienanforderungen für Ihre Speicher-Workloads nicht erfüllen, können Sie ein benutzerdefiniertes SEP erstellen. Es wird jedoch empfohlen, dass Sie versuchen, die systemdefinierten SEPs für Ihre Speicher-Workloads zu verwenden und nur bei Bedarf benutzerdefinierte SEPs zu erstellen.

Sie können den den Workloads zugewiesenen SEP auf der Seite „Alle Workloads“ und auf der Seite „Volume-/Integritätsdetails“ anzeigen. Sie können das Datenreduktionsverhältnis auf Clusterebene (ohne Snapshot-Kopien) basierend auf diesen Speichereffizienzen im Kapazitätsbereich auf dem Dashboard und in der Ansicht „Kapazität: Alle Cluster“ anzeigen.

Erstellen und Bearbeiten von Speichereffizienzrichtlinien

Wenn die systemdefinierten Speichereffizienzrichtlinien nicht Ihren Workload-Anforderungen entsprechen, können Sie Ihre eigenen Speichereffizienzrichtlinien erstellen, die für Ihre Workloads optimiert sind.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.
- Der Name der Speichereffizienzrichtlinie muss eindeutig sein und Sie können die folgenden reservierten Schlüsselwörter nicht verwenden:

  `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 Anwendungen benötigen, die auf den Speicher zugreifen.

Sie können eine Speichereffizienzrichtlinie nicht ändern, wenn sie derzeit einer Arbeitslast zugewiesen ist.

Schritte

1. Wählen Sie im linken Navigationsbereich unter **Einstellungen Richtlinien** > **Speichereffizienz** aus.
2. Klicken Sie auf der Seite **Speichereffizienzrichtlinien** auf die entsprechende Schaltfläche, je nachdem, ob Sie eine neue Speichereffizienzrichtlinie erstellen oder eine vorhandene Speichereffizienzrichtlinie bearbeiten möchten.

Zu…	Befolgen Sie diese Schritte…
Erstellen einer neuen Speichereffizienzrichtlinie	Klicken Sie auf **Hinzufügen**
Bearbeiten einer vorhandenen Speichereffizienzrichtlinie	Wählen Sie eine vorhandene Speichereffizienzrichtlinie aus und klicken Sie auf **Bearbeiten**

   Die Seite zum Hinzufügen oder Bearbeiten einer Speichereffizienzrichtlinie wird angezeigt.

3. Passen Sie die Speichereffizienzrichtlinie an, indem Sie die Speichereffizienzmerkmale angeben, und klicken Sie dann auf **Senden**, um die Speichereffizienzrichtlinie zu speichern.

Sie können die neue oder geänderte Speichereffizienzrichtlinie auf Workloads (LUNs, NFS-Dateifreigaben, CIFS-Freigaben) von der Seite „Workloads“ oder beim Bereitstellen eines neuen Workloads anwenden.

Verwalten und Überwachen von MetroCluster -Konfigurationen

Die Überwachungsunterstützung für MetroCluster -Konfigurationen in der Unified Manager-Web-Benutzeroberfläche ermöglicht es Ihnen, Ihre MetroCluster Konfigurationen über FC und IP auf Verbindungsprobleme zu überprüfen. Durch die frühzeitige Erkennung eines Konnektivitätsproblems können Sie Ihre MetroCluster -Konfigurationen effektiv verwalten.

Lautstärkeverhalten beim Umschalten und Zurückschalten

Ereignisse, die ein Switchover oder Switchback auslösen, führen dazu, dass aktive

Volumes von einem Cluster in den anderen Cluster in der Disaster Recovery-Gruppe verschoben werden. Die Volumes auf dem Cluster, die aktiv waren und Daten an Clients übermittelt haben, werden gestoppt, und die Volumes auf dem anderen Cluster werden aktiviert und beginnen mit der Datenübermittlung. Unified Manager überwacht nur die Volumes, die aktiv und aktiv sind.

Da Volumes von einem Cluster in einen anderen verschoben werden, wird empfohlen, beide Cluster zu überwachen. Eine einzelne Instanz von Unified Manager kann beide Cluster in einer MetroCluster -Konfiguration überwachen, aber manchmal erfordert die Entfernung zwischen den beiden Standorten die Verwendung von zwei Unified Manager-Instanzen zur Überwachung beider Cluster. Die folgende Abbildung zeigt eine einzelne Instanz von Unified Manager:

Die Volumes mit p im Namen geben die primären Volumes an, und die Volumes mit b im Namen sind gespiegelte Sicherungsvolumes, die von SnapMirror erstellt werden.

Während des Normalbetriebs:

- Cluster A hat zwei aktive Volumes: Vol1p und Vol2p.
- Cluster B hat zwei aktive Volumes: Vol3p und Vol4p.
- Cluster A hat zwei inaktive Volumes: Vol3b und Vol4b.
- Cluster B hat zwei inaktive Volumes: Vol1b und Vol2b.

Informationen zu jedem der aktiven Volumes (Statistiken, Ereignisse usw.) werden von Unified Manager gesammelt. Vol1p- und Vol2p-Statistiken werden von Cluster A und Vol3p- und Vol4p-Statistiken von Cluster B gesammelt.

Nach einem katastrophalen Fehler kommt es zu einer Umschaltung der aktiven Volumes von Cluster B zu Cluster A:

- Cluster A hat vier aktive Volumes: Vol1p, Vol2p, Vol3b und Vol4b.
- Cluster B hat vier inaktive Volumes: Vol3p, Vol4p, Vol1b und Vol2b.

Wie im Normalbetrieb werden Informationen zu jedem der aktiven Volumes vom Unified Manager erfasst. In diesem Fall werden die Statistiken zu Vol1p und Vol2p jedoch von Cluster A erfasst, und die Statistiken zu Vol3b und Vol4b werden ebenfalls von Cluster A erfasst.

Beachten Sie, dass Vol3p und Vol3b nicht dieselben Volumes sind, da sie sich auf unterschiedlichen Clustern befinden. Die Informationen im Unified Manager für Vol3p sind nicht dieselben wie für Vol3b:

- Während der Umstellung auf Cluster A sind Vol3p-Statistiken und -Ereignisse nicht sichtbar.
- Beim allerersten Umschalten sieht Vol3b wie ein neuer Band ohne historische Informationen aus.

Wenn Cluster B repariert ist und ein Switchback durchgeführt wird, ist Vol3p auf Cluster B wieder aktiv, mit den historischen Statistiken und einer Statistiklücke für den Zeitraum während der Umschaltung. Vol3b kann von Cluster A aus erst angezeigt werden, wenn eine weitere Umschaltung erfolgt:

- Inaktive MetroCluster Volumes, beispielsweise Vol3b auf Cluster A nach dem Switchback, werden mit der Meldung „Dieses Volume wurde gelöscht“ gekennzeichnet. Das Volume wird nicht wirklich 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, gibt die Volume-Suche Informationen zu dem Volume zurück, das zu diesem Zeitpunkt aktiv ist. Beispielsweise würde eine Suche nach „Vol3“ Statistiken und Ereignisse für Vol3b auf Cluster A zurückgeben, wenn eine Umschaltung stattgefunden hat und Vol3 auf Cluster A aktiv geworden ist.

Cluster-Konnektivitätsstatusdefinitionen für die MetroCluster über-FC-Konfiguration

Die Konnektivität zwischen den Clustern in einer MetroCluster -über-FC-Konfiguration kann einen der folgenden Status aufweisen: Optimal, Beeinträchtigt oder Ausgefallen. Wenn Sie den Verbindungsstatus verstehen, können Sie Ihre MetroCluster -Konfigurationen effektiv verwalten.

Verbindungsstatus	Beschreibung	Angezeigtes Symbol
Optimal	Die Konnektivität zwischen den Clustern in der MetroCluster -Konfiguration ist normal.	
Betroffen	Ein oder mehrere Fehler beeinträchtigen den Status der Failover-Verfügbarkeit; beide Cluster in der MetroCluster -Konfiguration sind jedoch noch aktiv. Zum Beispiel, wenn die ISL-Verbindung ausgefallen ist, wenn die IP-Verbindung zwischen den Clustern ausgefallen ist oder wenn der Partnercluster nicht erreichbar ist.	
Runter	Die Konnektivität zwischen den Clustern in der MetroCluster -Konfiguration ist unterbrochen, weil einer oder beide Cluster ausgefallen sind oder sich die Cluster im Failover-Modus befinden. Beispielsweise, wenn der Partnercluster aufgrund einer Katastrophe ausfällt oder wenn eine Umstellung zu Testzwecken geplant ist.	Umschaltung mit Fehlern: Umschaltung erfolgreich:

Datenspiegelungsstatusdefinitionen für MetroCluster über FC

MetroCluster über FC-Konfigurationen bieten Datenspiegelung und die zusätzliche Möglichkeit, ein Failover einzuleiten, wenn ein ganzer Standort nicht verfügbar ist. Der Status der Datenspiegelung zwischen den Clustern in einer MetroCluster über-FC-Konfiguration kann entweder „Normal“ oder „Spiegelung nicht verfügbar“ sein. Wenn Sie den Status kennen, können Sie Ihre MetroCluster -Konfigurationen effektiv verwalten.

Datenspiegelungsstatus	Beschreibung	Angezeigtes Symbol
Normal	Die Datenspiegelung zwischen den Clustern in der MetroCluster -Konfiguration ist normal.	
Spiegelung nicht verfügbar	Die Datenspiegelung zwischen den Clustern in der MetroCluster -Konfiguration ist aufgrund einer Umschaltung nicht verfügbar. Beispielsweise, wenn der Partnercluster aufgrund einer Katastrophe ausfällt oder wenn eine Umstellung zu Testzwecken geplant ist.	Umschaltung mit Fehlern: Umschaltung erfolgreich:

Überwachen Sie MetroCluster -Konfigurationen

Sie können Konnektivitätsprobleme in Ihrer MetroCluster -Konfiguration überwachen. Zu den Details gehören der Status der Komponenten und der Konnektivität innerhalb eines Clusters sowie der Konnektivitätsstatus zwischen den Clustern in der MetroCluster -Konfiguration. Hier erfahren Sie, wie Sie Konnektivitätsprobleme in Clustern überwachen, die durch MetroCluster over FC- und MetroCluster over IP-Konfigurationen geschützt sind.

Sie können die MetroCluster -Konfigurationen aus den folgenden Ansichten im linken Navigationsbereich des Active IQ Unified Manager überwachen:

- **Speicher** > **Cluster** > **Schutz: MetroCluster** anzeigen
- **Schutz** > **Beziehungen** > **Beziehung: MetroCluster** anzeigen

Unified Manager verwendet Systemzustandswarnungen, 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.

- Wenn in einer MetroCluster -over-IP-Konfiguration ein Mediator unterstützt werden soll, muss der Mediator konfiguriert und über die entsprechende API zum Cluster hinzugefügt werden.
- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Überwachen Sie Konnektivitätsprobleme in der MetroCluster über-FC-Konfiguration

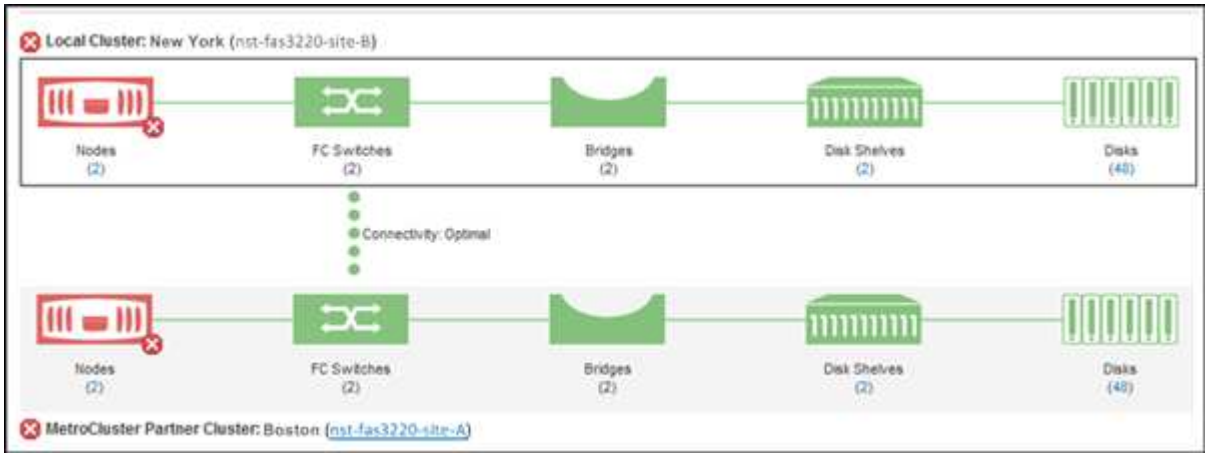
Für Cluster in einer MetroCluster -über-FC-Konfiguration werden die Konnektivitätsdiagramme auf der Detailseite **Cluster/Integrität** angezeigt. Befolgen Sie diese Schritte.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Cluster**.

   Es wird eine Liste aller überwachten Cluster angezeigt.

2. Klicken Sie in der Ansicht **Schutz: MetroCluster** auf den Namen des Clusters, für den Sie die Konfigurationsdetails von MetroCluster über FC anzeigen möchten. Alternativ können Sie in einer MetroCluster -Konfiguration nach Clustern filtern.
3. Klicken Sie auf der Detailseite **Cluster/Integrität** auf die Registerkarte * MetroCluster -Konnektivität*. Die Registerkarte * MetroCluster -Konnektivität* ist nur für MetroCluster über-FC-Konfigurationen verfügbar.



   Die Topologie der MetroCluster -Konfiguration wird im entsprechenden Cluster-Objektbereich angezeigt. Sie können die auf der Seite „Cluster-/Integritätsdetails“ angezeigten Informationen verwenden, um etwaige Verbindungsprobleme zu beheben. Wenn beispielsweise die Verbindung zwischen dem Knoten und dem Switch in einem Cluster unterbrochen ist, wird das folgende Symbol angezeigt:

Wenn Sie den Zeiger über das Symbol bewegen, können Sie detaillierte Informationen zum generierten Ereignis anzeigen.

Wenn Sie Konnektivitätsprobleme in Ihrer MetroCluster -Konfiguration feststellen, müssen Sie sich beim System Manager anmelden oder auf die ONTAP CLI zugreifen, um die Probleme zu beheben.

Weitere Informationen zum Bestimmen der Clusterintegrität finden Sie unter"Bestimmen Sie die Clusterintegrität in der MetroCluster -über-FC-Konfiguration" .

Überwachen Sie Konnektivitätsprobleme in der MetroCluster -over-IP-Konfiguration

Für Cluster in einer MetroCluster -over-IP-Konfiguration werden die Konnektivitätsdiagramme auf der Seite **Cluster** angezeigt. Befolgen Sie diese Schritte.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Cluster**.

   Es wird eine Liste aller überwachten Cluster angezeigt.

2. Klicken Sie in der Ansicht **Schutz: MetroClusters** auf den Namen des Clusters, für den Sie die Konfigurationsdetails von MetroCluster over IP anzeigen möchten. Alternativ können Sie in einer MetroCluster -Konfiguration nach Clustern filtern.
3. Erweitern Sie die Zeile, indem Sie auf das Caret-Symbol klicken ⌄ Symbol. Das Caret-Symbol wird nur für einen Cluster angezeigt, der durch die MetroCluster over-IP-Konfiguration geschützt ist.

   Sie können die Topologie der Quell- und Spiegelsites sowie den Mediator (sofern vorhanden) anzeigen, der für die Verbindung verwendet wird. Sie können die folgenden Informationen anzeigen:

   - Konnektivität zwischen den Standorten
   - Gesundheits- und Verfügbarkeitsprobleme, falls vorhanden, auf beiden Websites
   - Mediatorbezogene Probleme
   - Replikationsbezogene Probleme.

   > Die folgenden Status werden gemeldet: Kritisch ( ), Fehler ( ) oder Normal ( ). Sie können auch den aggregierten Datenreplikationsstatus der Primär- und Spiegeldaten in derselben Topologie anzeigen.

   Im folgenden Diagramm können Sie sehen, dass die standortübergreifende Konnektivität zwischen den Quell- und Zielclustern nicht verfügbar ist und der Mediator zwischen ihnen nicht konfiguriert ist.

4. Klicken Sie auf das Statussymbol. Es wird eine Meldung mit der Fehlerdefinition angezeigt. Wenn für das Problem in Ihrer MetroCluster over IP-Konfiguration ein Ereignis ausgelöst wurde, können Sie in der Nachricht auf die Schaltfläche **Ereignis anzeigen** klicken und die Ereignisdetails anzeigen. Wenn Sie das

Problem und das Ereignis behoben haben, wechselt das Statussymbol in dieser Topologie zu „Normal“ ( ).

5. Weitere Konfigurationsdetails können Sie in den Abschnitten * MetroCluster -Übersicht* und **Schutz** auf der Registerkarte **Konfiguration** der Detailseite **Cluster/Integrität** anzeigen.

> Nur bei einer MetroCluster -over-IP-Konfiguration können Sie die Clustertopologie auf der Seite **Cluster** anzeigen. Für Cluster in einer MetroCluster über-FC-Konfiguration wird die Topologie auf der Registerkarte * MetroCluster Konnektivität* auf der Detailseite **Cluster/Integrität** angezeigt.

Verwandte Informationen

- "Cluster-/Integritätsdetailseite"
- Informationen zur Ansicht **Relationship: MetroCluster** finden Sie unter"Überwachen Sie MetroCluster -Konfigurationen" .
- Informationen zur Ansicht **Beziehung: Transferstatus des letzten Monats** finden Sie unter"Beziehung: Ansicht des Übertragungsstatus des letzten Monats" .
- Informationen zur Ansicht **Beziehung: Übertragungsrate des letzten Monats** finden Sie unter"Beziehung: Ansicht der Übertragungsrate des letzten Monats" .
- Informationen zur Ansicht **Beziehung: Alle Beziehungen** finden Sie unter"Beziehung: Ansicht „Alle Beziehungen“" .

Überwachen der MetroCluster -Replikation

Sie können den Gesamtzustand der logischen Verbindungen überwachen und diagnostizieren, während Sie die Daten spiegeln. Sie können die Probleme oder Risiken identifizieren, die die Spiegelung von Clusterkomponenten wie Aggregaten, Knoten und virtuellen Speichermaschinen unterbrechen.

Unified Manager verwendet Systemzustandswarnungen, um den Status der Komponenten und der 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

Anzeigen der Replikation für MetroCluster über IP-Konfigurationen

Bei MetroCluster over IP-Konfigurationen wird der Datenreplikationsstatus in der Topologie-Vorschauansicht für einen durch MetroCluster over IP geschützten Cluster aus den folgenden Ansichten im linken Navigationsbereich des Unified Manager angezeigt:

- **Speicher** > **Cluster** > **Schutz: MetroCluster** anzeigen
- **Schutz** > **Beziehungen** > **Beziehung: MetroCluster** anzeigen

Weitere Informationen finden Sie unter"Überwachen Sie Konnektivitätsprobleme in MetroCluster über IP" .

Anzeigen der Replikation für MetroCluster über FC-Konfigurationen

Befolgen Sie diese Schritte, um etwaige Probleme bei der Datenreplikation für die MetroCluster über-FC-

Konfiguration zu ermitteln.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Cluster**.

   Es wird eine Liste der überwachten Cluster angezeigt.

2. Klicken Sie in der Ansicht **Health: All Clusters** auf den Namen des Clusters, für den Sie die MetroCluster Replikationsdetails anzeigen möchten. Klicken Sie auf der Seite **Cluster-/Integritätsdetails** auf die Registerkarte * MetroCluster -Replikation*.

   Die Topologie der zu replizierenden MetroCluster Konfiguration wird am lokalen Standort im entsprechenden Cluster-Objektbereich mit den Informationen zum Remote-Standort angezeigt, an dem die Daten gespiegelt werden. Wenn Sie den Zeiger über das Symbol bewegen, können Sie detaillierte Informationen zum generierten Ereignis anzeigen.

Sie können die auf der Seite „Cluster-/Integritätsdetails“ angezeigten Informationen verwenden, um etwaige Replikationsprobleme zu beheben. Wenn Sie Spiegelungsprobleme in Ihrer MetroCluster -Konfiguration feststellen, müssen Sie sich beim System Manager anmelden oder auf die ONTAP CLI zugreifen, um die Probleme zu beheben.

Verwandte Informationen

"Cluster-/Integritätsdetailseite"

Verwalten von Kontingenten

Mithilfe von Benutzer- und Gruppenkontingenten können Sie den Speicherplatz oder die Anzahl der Dateien begrenzen, die ein Benutzer oder eine Benutzergruppe verwenden kann. Sie können Kontingentinformationen zu Benutzern und Benutzergruppen anzeigen, beispielsweise die Festplatten- und Dateinutzung und die verschiedenen für Festplatten festgelegten Beschränkungen.

Welche Kontingentgrenzen gibt es

Benutzerkontingentgrenzen sind Werte, die der Unified Manager-Server verwendet, um zu bewerten, ob sich der Speicherplatzverbrauch eines Benutzers der Grenze nähert oder die durch die Benutzerkontingentgrenze festgelegte Grenze erreicht hat. Wenn das weiche Limit überschritten oder das harte Limit erreicht wird, 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 harte Kontingentlimit erreicht haben und für die Benutzerkontingentereignisse konfiguriert sind. Benutzer mit der Rolle „Anwendungsadministrator“ können Warnmeldungen konfigurieren, die die angegebenen Empfänger über Benutzer- oder Benutzergruppenkontingentereignisse benachrichtigen.

Sie können Kontingentgrenzen entweder mit dem ONTAP System Manager oder der ONTAP CLI festlegen.

Anzeigen von Benutzer- und Benutzergruppenkontingenten

Auf der Seite „Storage VM / Health Details“ werden Informationen zu den Benutzer- und Benutzergruppenkontingenten angezeigt, die auf der SVM konfiguriert sind. Sie können den Namen des Benutzers oder der Benutzergruppe, die für die Datenträger und Dateien festgelegten Beschränkungen, den verwendeten Datenträger- und Dateispeicherplatz sowie die E-Mail-Adresse für Benachrichtigungen anzeigen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Speicher-VMs**.
2. Wählen Sie in der Ansicht **Integrität: Alle Storage-VMs** eine Storage-VM aus und klicken Sie dann auf die Registerkarte **Benutzer- und Gruppenkontingente**.

Verwandte Informationen

"Benutzer hinzufügen"

Erstellen Sie Regeln zum Generieren von E-Mail-Adressen

Sie können Regeln erstellen, um die E-Mail-Adresse basierend auf dem Benutzerkontingent anzugeben, das Clustern, virtuellen Speichermaschinen (SVMs), Volumes, Qtrees, Benutzern oder Benutzergruppen zugeordnet ist. Bei einer Quotenüberschreitung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Richtlinien auf der Seite „Regeln zum Generieren von E-Mail-Adressen für Benutzer- und Gruppenkontingente“ gelesen haben.

Sie müssen die Regeln für Kontingent-E-Mail-Adressen definieren und sie in der Reihenfolge eingeben, in der Sie sie ausführen möchten. Wenn Sie beispielsweise die E-Mail-Adresse abc@xyz.com verwenden möchten, um Benachrichtigungen über Kontingentverletzungen für abc zu erhalten, und die E-Mail-Adresse dl-$GROUP@$DOMAIN für alle anderen Gruppen verwenden möchten, müssen die Regeln in der folgenden Reihenfolge aufgeführt werden:

- wenn ($USER == 'abc') dann abc@xyz.com
- wenn ($GROUP == *) dann dl-$GROUP@$DOMAIN

Wenn keines der Kriterien der von Ihnen angegebenen Regeln erfüllt ist, wird die Standardregel verwendet:

wenn ($USER_OR_GROUP == *) dann $USER_OR_GROUP@$DOMAIN

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Kontingent-E-Mail-Regeln**.
2. Geben Sie die Regel basierend auf Ihren Kriterien ein.

3. Klicken Sie auf **Validieren**, um die Syntax der Regel zu validieren.

   Wenn die Syntax der Regel falsch ist, wird eine Fehlermeldung angezeigt. Sie müssen die Syntax korrigieren und erneut auf **Validieren** klicken.

4. Klicken Sie auf **Speichern**.
5. Überprüfen Sie, ob die von Ihnen erstellte E-Mail-Adresse auf der Registerkarte „Benutzer- und Gruppenkontingente“ der Detailseite „Speicher-VM/Integrität“ angezeigt wird.

Erstellen Sie ein E-Mail-Benachrichtigungsformat für Benutzer- und Benutzergruppenkontingente

Sie können ein Benachrichtigungsformat für die E-Mails erstellen, die an einen Benutzer oder eine Benutzergruppe gesendet werden, wenn ein kontingentbezogenes Problem vorliegt (weiches Limit überschritten oder hartes Limit erreicht).

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Kontingent-E-Mail-Format**.
2. Geben Sie die Details in den Feldern **Von**, **Betreff** und **E-Mail-Details** ein oder ändern Sie sie.
3. Klicken Sie auf **Vorschau**, um eine Vorschau der E-Mail-Benachrichtigung anzuzeigen.
4. Klicken Sie auf **Schließen**, um das Vorschaufenster zu schließen.
5. Ändern Sie bei Bedarf den Inhalt der E-Mail-Benachrichtigung.
6. Klicken Sie auf **Speichern**.

Bearbeiten Sie die E-Mail-Adressen der Benutzer- und Gruppenkontingente

Sie können die E-Mail-Adressen basierend auf dem Benutzerkontingent ändern, das Clustern, virtuellen Speichermaschinen (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“ angegebenen Regeln generiert wurde.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die"Richtlinien zum Erstellen von Regeln" .

Wenn Sie eine E-Mail-Adresse bearbeiten, gelten die Regeln zum Generieren der E-Mail-Adressen für Benutzer- und Gruppenkontingente nicht mehr für das Kontingent. Damit Benachrichtigungen an die durch die angegebenen Regeln generierte E-Mail-Adresse gesendet werden, müssen Sie die E-Mail-Adresse löschen und die Änderung speichern.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **SVMs**.

2. Wählen Sie in der Ansicht **Health: All Storage VMs** eine SVM aus und klicken Sie dann auf die Registerkarte **User and Group Quotas**.
3. Klicken Sie unterhalb der Registerkartenreihe auf **E-Mail-Adresse bearbeiten**.
4. Führen Sie im Dialogfeld **E-Mail-Adresse bearbeiten** die entsprechende Aktion aus:

Wenn…	Dann…
Sie möchten, dass Benachrichtigungen an die E-Mail-Adresse gesendet werden, die durch die angegebenen Regeln generiert wurde	a. Löschen Sie die E-Mail-Adresse im Feld **E-Mail-Adresse**. b. Klicken Sie auf **Speichern**. c. Aktualisieren Sie den Browser, indem Sie F5 drücken, um das Dialogfeld „E-Mail-Adresse bearbeiten“ neu zu laden. Die von der angegebenen 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. Ändern Sie die E-Mail-Adresse im Feld **E-Mail-Adresse**. b. Klicken Sie auf **Speichern**. Die Regeln zum Generieren der E-Mail-Adressen für Benutzer- und Gruppenkontingente sind auf das Kontingent nicht mehr anwendbar.

Erfahren Sie mehr über Quoten

Wenn Sie die Konzepte zu Kontingenten verstehen, können Sie Ihre Benutzerkontingente und Benutzergruppenkontingente effizient verwalten.

Überblick über den Quotenprozess

Quoten können weich oder hart sein. Weiche Kontingente veranlassen ONTAP , eine Benachrichtigung zu senden, wenn bestimmte Grenzwerte überschritten werden, und harte Kontingente verhindern, dass ein Schreibvorgang erfolgreich ist, wenn bestimmte Grenzwerte überschritten werden.

Wenn ONTAP von einem Benutzer oder einer Benutzergruppe eine Anforderung zum Schreiben auf ein FlexVol volume erhält, prüft es, ob auf diesem Volume Kontingente für den Benutzer oder die Benutzergruppe aktiviert sind, und ermittelt Folgendes:

- Ob die harte Grenze erreicht wird

  Wenn ja, schlägt der Schreibvorgang fehl, wenn das harte Limit erreicht ist und die Benachrichtigung zum harten Kontingent gesendet wird.

- Ob das Soft-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 Soft-Limit nicht überschreitet

  Wenn ja, ist der Schreibvorgang erfolgreich und es wird keine Benachrichtigung gesendet.

Informationen zu Kontingenten

Kontingente bieten eine Möglichkeit, den Speicherplatz und die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien einzuschränken oder zu verfolgen. Sie legen Quoten fest, indem Sie `/etc/quotas` Datei. Kontingente werden auf ein bestimmtes Volume oder einen bestimmten Qtree angewendet.

Warum Sie Kontingente verwenden

Sie können Kontingente verwenden, um die Ressourcennutzung in FlexVol -Volumes zu begrenzen, eine Benachrichtigung zu senden, wenn die Ressourcennutzung bestimmte Werte erreicht, oder um 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
- Um den Speicherplatz oder die Anzahl der von einem Benutzer, einer Gruppe oder einem Qtree verwendeten Dateien zu verfolgen, ohne eine Begrenzung festzulegen
- Um Benutzer zu warnen, wenn ihre Festplatten- oder Dateinutzung hoch ist

Beschreibung der Kontingentdialogfelder

Sie können die entsprechende Option auf der Registerkarte „Benutzer- und Gruppenkontingente“ in der Ansicht „Integrität: Alle Speicher-VMs“ verwenden, um das Format der E-Mail-Benachrichtigung zu konfigurieren, die gesendet wird, wenn ein kontingentbezogenes Problem auftritt, und um Regeln zum Angeben von E-Mail-Adressen basierend auf dem Benutzerkontingent zu konfigurieren.

Seite „E-Mail-Benachrichtigungsformat“

Auf der Seite „E-Mail-Benachrichtigungsformat“ werden die Regeln der E-Mail angezeigt, die an einen Benutzer oder eine Benutzergruppe gesendet wird, wenn ein kontingentbezogenes Problem vorliegt (weiches Limit überschritten oder hartes Limit erreicht).

Die E-Mail-Benachrichtigung wird nur gesendet, wenn die folgenden Benutzer- oder Benutzergruppenkontingentereignisse generiert werden: Weiches Limit für Speicherplatz des Benutzer- oder Gruppenkontingents überschritten, Weiches Limit für Dateianzahl des Benutzer- oder Gruppenkontingents überschritten, Hartes Limit für Speicherplatz des Benutzer- oder Gruppenkontingents erreicht oder Hartes Limit für Dateianzahl des Benutzer- oder Gruppenkontingents erreicht.

- **Aus**

  Zeigt die E-Mail-Adresse an, von der die E-Mail gesendet wird. Sie können diese Adresse ändern.

Standardmäßig ist dies die auf der Benachrichtigungsseite angegebene E-Mail-Adresse.

- **Thema**

  Zeigt den Betreff der Benachrichtigungs-E-Mail an.

- **E-Mail-Details**

  Zeigt den Text der Benachrichtigungs-E-Mail an. Sie können den Text Ihren Anforderungen entsprechend ändern. Sie können beispielsweise Informationen zu den Quotenattributen bereitstellen und die Anzahl der Schlüsselwörter reduzieren. Sie sollten die Schlüsselwörter jedoch nicht ändern.

  Gültige Schlüsselwörter sind wie folgt:

  - $EVENT_NAME

    Gibt den Ereignisnamen an, der die E-Mail-Benachrichtigung verursacht hat.

  - $QUOTA_TARGET

    Gibt den Qtree oder das Volume an, auf das das Kontingent anwendbar ist.

  - $QUOTA_USED_PERCENT

    Gibt den Prozentsatz des Festplatten-Hardlimits, des Festplatten-Softlimits, des Datei-Hardlimits oder des Datei-Softlimits an, der vom Benutzer oder der Benutzergruppe verwendet wird.

  - $QUOTA_LIMIT

    Gibt das Festplattenlimit oder das Dateilimit an, das vom Benutzer oder der Benutzergruppe erreicht wird. Dabei wird eines der folgenden Ereignisse generiert:

    - Hartes Limit für Benutzer- oder Gruppenkontingentspeicherplatz erreicht
    - Soft-Limit für Benutzer- oder Gruppenkontingent-Festplattenspeicher erreicht
    - Festes Limit für die Anzahl der Benutzer- oder Gruppenkontingentedateien erreicht
    - Soft-Limit für die Anzahl der Benutzer- oder Gruppenkontingentedateien erreicht

  - $QUOTA_USED

    Gibt den belegten Speicherplatz oder die Anzahl der vom Benutzer oder der Benutzergruppe erstellten Dateien an.

  - $QUOTA_USER

    Gibt den Benutzer- oder Benutzergruppennamen an.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die am E-Mail-Benachrichtigungsformat vorgenommenen Änderungen in der Vorschau anzeigen, speichern oder abbrechen:

- **Vorschau**

  Zeigt eine Vorschau der Benachrichtigungs-E-Mail an.

- **Auf Werkseinstellungen zurücksetzen**

  Ermöglicht Ihnen, das Benachrichtigungsformat auf die werkseitigen Standardwerte zurückzusetzen.

- **Speichern**

  Speichert die am Benachrichtigungsformat vorgenommenen Änderungen.

Regeln zum Generieren der Seite „Benutzer- und Gruppenkontingent-E-Mail-Adressen“

Auf der Seite „Regeln zum Generieren von E-Mail-Adressen mit Benutzer- und Gruppenkontingenten“ können Sie Regeln zum Angeben von E-Mail-Adressen basierend auf dem mit Clustern, SVMs, Volumes, Qtrees, Benutzern oder Benutzergruppen verknüpften Benutzerkontingent erstellen. Bei einer Quotenüberschreitung wird eine Benachrichtigung an die angegebene E-Mail-Adresse gesendet.

Regelbereich

Sie müssen die Regeln für eine Kontingent-E-Mail-Adresse definieren. Sie können auch Kommentare hinzufügen, um die Regeln zu erläutern.

So definieren Sie Regeln

Sie müssen die Regeln in der Reihenfolge eingeben, in der Sie sie ausführen möchten. Wenn das Kriterium der ersten Regel erfüllt ist, wird die E-Mail-Adresse basierend auf dieser Regel generiert. Wenn das Kriterium nicht erfüllt ist, wird das Kriterium für die nächste Regel berücksichtigt und so weiter. Jede Zeile listet eine separate Regel auf. Die Standardregel ist die letzte Regel in der Liste. Sie können die Prioritätsreihenfolge der Regeln ändern. Sie können die Reihenfolge der Standardregel jedoch nicht ändern.

Wenn Sie beispielsweise die E-Mail-Adresse qtree1@xyz.com verwenden möchten, um Benachrichtigungen über Kontingentverletzungen 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 aufgeführt werden:

- wenn ($QTREE == 'qtree1') dann qtree1@xyz.com
- wenn ($QTREE == *) dann admin@xyz.com

Wenn keines der Kriterien der von Ihnen angegebenen Regeln erfüllt ist, wird die Standardregel verwendet:

wenn ($USER_OR_GROUP == *) dann $USER_OR_GROUP@$DOMAIN

Wenn mehrere Benutzer über dasselbe Kontingent verfügen, werden die Namen der Benutzer als durch Kommas getrennte Werte angezeigt und die Regeln gelten nicht für das Kontingent.

So fügen Sie Kommentare hinzu

Sie können Kommentare hinzufügen, um die Regeln zu erläutern. Sie sollten am Anfang jedes Kommentars # verwenden und jede Zeile einen separaten Kommentar auflisten.

Regelsyntax

Die Syntax der Regel muss eine der folgenden sein:

- Wenn (`valid variableoperator *`) Dann `email ID@domain name`

if ist ein Schlüsselwort und wird in Kleinbuchstaben geschrieben. 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 Domänenname kann ein beliebiges Zeichen, die gültige Variable $DOMAIN oder eine Kombination aus einem beliebigen Zeichen und der gültigen Variable $DOMAIN enthalten. Gültige Variablen können in Groß- oder Kleinbuchstaben geschrieben sein, dürfen aber keine Kombination aus beiden 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 in Kleinbuchstaben geschrieben. Der Operator kann „enthält“ oder „==“ sein. Die E-Mail-ID kann ein beliebiges Zeichen, die gültigen Variablen $USER_OR_GROUP, $USER oder $GROUP oder eine Kombination aus einem beliebigen Zeichen und den gültigen Variablen $USER_OR_GROUP, $USER oder $GROUP enthalten. Der Domänenname kann ein beliebiges Zeichen, die gültige Variable $DOMAIN oder eine Kombination aus einem beliebigen Zeichen und der gültigen Variable $DOMAIN enthalten. Gültige Variablen können in Groß- oder Kleinbuchstaben geschrieben sein, dürfen aber keine Kombination aus beiden sein. Beispielsweise sind $domain und $DOMAIN gültig, aber $Domain ist keine gültige Variable.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die erstellten Regeln speichern, bestätigen oder abbrechen:

- **Bestätigen**

  Validiert die Syntax der erstellten Regel. Wenn bei der Validierung Fehler auftreten, wird die Regel, die den Fehler erzeugt, zusammen mit einer Fehlermeldung angezeigt.

- **Auf Werkseinstellungen zurücksetzen**

  Ermöglicht Ihnen, die Adressregeln auf die werkseitigen Standardwerte zurückzusetzen.

- **Speichern**

  Überprüft die Syntax der Regel und speichert die Regel, wenn keine Fehler vorliegen. Wenn bei der Validierung Fehler auftreten, wird die Regel, die den Fehler generiert, zusammen mit einer Fehlermeldung angezeigt.

Fehlerbehebung

Informationen zur Fehlerbehebung helfen Ihnen, Probleme zu identifizieren und zu lösen, die bei der Verwendung von Unified Manager auftreten.

Fügen Sie dem Unified Manager-Datenbankverzeichnis Speicherplatz hinzu

Das Unified Manager-Datenbankverzeichnis enthält alle von ONTAP -Systemen erfassten Integritäts- und Leistungsdaten. Unter bestimmten Umständen kann es erforderlich sein, dass Sie die Größe des Datenbankverzeichnisses erhöhen.

Beispielsweise kann das Datenbankverzeichnis voll werden, wenn Unified Manager Daten aus einer großen Anzahl von Clustern sammelt, wobei jeder Cluster viele Knoten hat. Sie erhalten ein Warnereignis, wenn das Datenbankverzeichnis zu 90 % voll ist, und ein kritisches Ereignis, wenn das Verzeichnis zu 95 % voll ist.

Wenn das Verzeichnis zu 95 % gefüllt ist, werden keine weiteren Daten mehr aus den Clustern erfasst.

Die zum Hinzufügen von Kapazität zum Datenverzeichnis 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.

Fügen Sie Speicherplatz zur Datenfestplatte der virtuellen VMware-Maschine hinzu

Wenn Sie den Speicherplatz auf der Datenfestplatte für die Unified Manager-Datenbank erhöhen müssen, können Sie nach der Installation Kapazität hinzufügen, indem Sie den Speicherplatz mithilfe der Unified Manager-Wartungskonsole erhöhen.

Bevor Sie beginnen

- Sie müssen Zugriff auf den vSphere-Client haben.
- Auf der virtuellen Maschine dürfen keine Snapshots lokal gespeichert sein.
- Sie müssen über die Anmeldeinformationen des Wartungsbenutzers verfügen.

Wir empfehlen Ihnen, Ihre virtuelle Maschine zu sichern, bevor Sie die Größe virtueller Festplatten erhöhen.

Schritte

1. Wählen Sie im vSphere-Client die virtuelle Maschine Unified Manager aus und fügen Sie dann mehr Festplattenkapazität zu Daten hinzu `disk 3` . Weitere Informationen finden Sie in der VMware-Dokumentation.

   In einigen seltenen Fällen verwendet die Unified Manager-Bereitstellung „Festplatte 2“ für die Datenfestplatte anstelle von „Festplatte 3“. Wenn dies bei Ihrer Bereitstellung der Fall ist, erhöhen Sie den Speicherplatz auf der größeren Festplatte. Auf der Datenfestplatte ist immer mehr Speicherplatz vorhanden als auf der anderen Festplatte.

2. Wählen Sie im vSphere-Client die virtuelle Maschine Unified Manager und dann die Registerkarte **Konsole** aus.
3. Klicken Sie in das Konsolenfenster und melden Sie sich dann mit Ihrem Benutzernamen und Kennwort bei der Wartungskonsole an.
4. Geben Sie im **Hauptmenü** die Nummer für die Option **Systemkonfiguration** ein.
5. Geben Sie im **Systemkonfigurationsmenü** die Zahl für die Option **Datenträgergröße erhöhen** ein.

Fügen Sie dem Datenverzeichnis des Linux-Hosts Speicherplatz hinzu

Wenn Sie nicht genügend Speicherplatz für die `/opt/netapp/data` Verzeichnis zur Unterstützung von Unified Manager, wenn Sie den Linux-Host ursprünglich eingerichtet und dann Unified Manager installiert haben, können Sie nach der Installation Speicherplatz hinzufügen, indem Sie den Speicherplatz auf dem `/opt/netapp/data` Verzeichnis.

Bevor Sie beginnen

Sie müssen über Root-Benutzerzugriff auf die Red Hat Enterprise Linux-Maschine verfügen, auf der Unified Manager installiert ist.

Wir empfehlen, dass Sie die Unified Manager-Datenbank sichern, bevor Sie die Größe des Datenverzeichnisses erhöhen.

Schritte

1. Melden Sie sich als Root-Benutzer bei der Linux-Maschine an, auf der Sie Speicherplatz hinzufügen möchten.
2. Stoppen Sie den Unified Manager-Dienst und die zugehörige MySQL-Software in der angezeigten Reihenfolge: `systemctl stop ocieau ocie mysqld`
3. Erstellen Sie einen temporären Sicherungsordner (z. B. `/backup-data`) mit ausreichend Speicherplatz, um die Daten im aktuellen `/opt/netapp/data` Verzeichnis.
4. Kopieren Sie den Inhalt und die Berechtigungskonfiguration des bestehenden `/opt/netapp/data` Verzeichnis in das Sicherungsdatenverzeichnis:

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

5. Wenn SE Linux aktiviert ist:

   a. Holen Sie sich den SE Linux-Typ für Ordner auf 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 ähnlich der folgenden zurück:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Führen Sie den `chcon` Befehl zum Festlegen des SE Linux-Typs für das Sicherungsverzeichnis:

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. Entfernen Sie den Inhalt des `/opt/netapp/data` Verzeichnis:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. Erweitern Sie die Größe des `/opt/netapp/data` Verzeichnis auf mindestens 150 GB durch LVM-Befehle oder durch Hinzufügen zusätzlicher Festplatten.

   Wenn Sie erstellt haben `/opt/netapp/data` von einer Festplatte, dann sollten Sie nicht versuchen, zu mounten `/opt/netapp/data` als NFS- oder CIFS-Freigabe. Denn in diesem Fall, wenn Sie versuchen, den Speicherplatz zu erweitern, einige LVM-Befehle, wie zum Beispiel `resize` Und `extend` funktioniert möglicherweise nicht wie erwartet.

8. Bestätigen Sie, dass die `/opt/netapp/data` Verzeichnisbesitzer (mysql) und Gruppe (root) bleiben unverändert:

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

   Das System gibt eine Bestätigung ähnlich der folgenden zurück:

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

9. Wenn SE Linux aktiviert ist, bestätigen Sie, dass der Kontext für die `/opt/netapp/data` Verzeichnis ist immer noch auf mysqld_db_t eingestellt:

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

   Das System gibt eine Bestätigung ähnlich der folgenden zurück:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Löschen Sie die Datei `abc` damit diese überflüssige Datei in Zukunft keinen Datenbankfehler verursacht.

11. Kopieren Sie den Inhalt von `backup-data` zurück zur erweiterten `/opt/netapp/data` Verzeichnis:

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

12. Wenn SE Linux aktiviert ist, führen Sie den folgenden Befehl aus:

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

13. Starten Sie den MySQL-Dienst:

    `systemctl start mysqld`

14. Nachdem der MySQL-Dienst gestartet wurde, starten Sie die Dienste ocie und ocieau in der angezeigten Reihenfolge:

    `systemctl start ocie ocieau`

15. Nachdem alle Dienste gestartet sind, löschen Sie den Sicherungsordner `/backup-data` :

    `rm -rf /backup-data`

Fügen Sie dem logischen Laufwerk des Microsoft Windows-Servers Speicherplatz hinzu

Wenn Sie den Speicherplatz für die Unified Manager-Datenbank erhöhen müssen, können Sie die Kapazität des logischen Laufwerks erhöhen, auf dem Unified Manager installiert ist.

Bevor Sie beginnen

Sie müssen über Windows-Administratorrechte verfügen.

Wir empfehlen Ihnen, die Unified Manager-Datenbank zu sichern, bevor Sie Speicherplatz hinzufügen.

Schritte

1. Melden Sie sich als Administrator bei dem Windows-Server an, auf dem Sie Speicherplatz hinzufügen möchten.
2. Führen Sie den Schritt aus, der der Methode entspricht, mit der Sie mehr Speicherplatz hinzufügen möchten:

Option	Beschreibung
Erhöhen Sie auf einem physischen Server die Kapazität des logischen Laufwerks, auf dem der Unified Manager-Server installiert ist.	Befolgen Sie die Schritte im Microsoft-Thema: "Erweitern eines Basisvolumes"
Fügen Sie auf einem physischen Server ein Festplattenlaufwerk hinzu.	Befolgen Sie die Schritte im Microsoft-Thema: "Hinzufügen von Festplattenlaufwerken"
Erhöhen Sie auf einer virtuellen Maschine die Größe einer Festplattenpartition.	Befolgen Sie die Schritte im VMware-Thema: "Erhöhen der Größe einer Festplattenpartition"

Ändern des Erfassungsintervalls für Leistungsstatistiken

Das Standarderfassungsintervall für Leistungsstatistiken beträgt 5 Minuten. Sie können dieses Intervall auf 10 oder 15 Minuten ändern, wenn Sie feststellen, dass Sammlungen aus großen Clustern nicht innerhalb der Standardzeit abgeschlossen werden. Diese Einstellung wirkt sich auf die Erfassung von Statistiken aus allen Clustern aus, die diese Instanz von Unified Manager überwacht.

Bevor Sie beginnen

Sie müssen über eine Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.

Das Problem, dass die Erfassung von Leistungsstatistiken nicht rechtzeitig abgeschlossen wird, wird durch die Bannermeldungen angezeigt `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>.`

Sie sollten das Erfassungsintervall nur ändern, wenn dies aufgrund eines Problems bei der Statistikerfassung erforderlich ist. Ändern Sie diese Einstellung aus keinem anderen Grund.

> Das Ändern dieses Werts von der Standardeinstellung von 5 Minuten kann sich auf die Anzahl und Häufigkeit der von Unified Manager gemeldeten Leistungsereignisse auswirken. Beispielsweise lösen systemdefinierte Leistungsschwellenwerte Ereignisse aus, wenn die Richtlinie 30 Minuten lang überschritten wird. Bei der Verwendung von 5-Minuten-Sammlungen muss die Richtlinie bei sechs aufeinanderfolgenden Sammlungen überschritten werden. Bei 15-Minuten-Abholungen darf die Richtlinie nur für zwei Abholperioden überschritten werden.

Eine Meldung unten auf der Seite „Cluster-Setup“ gibt das aktuelle Intervall zur Erfassung statistischer Daten an.

Schritte

1. Melden Sie sich per SSH als Wartungsbenutzer beim Unified Manager-Host an.

   Die Eingabeaufforderungen der Unified Manager-Wartungskonsole werden angezeigt.

2. Geben Sie die Nummer der Menüoption mit der Bezeichnung **Konfiguration des Leistungsabfrageintervalls** ein und drücken Sie dann die Eingabetaste.
3. Geben Sie bei entsprechender Aufforderung das Wartungsbenutzerkennwort erneut ein.
4. Geben Sie die Zahl für das neue Abfrageintervall ein, das Sie festlegen möchten, und drücken Sie dann die Eingabetaste.

Wenn Sie das Erfassungsintervall des Unified Managers auf 10 oder 15 Minuten geändert haben und über eine aktuelle Verbindung zu einem externen Datenanbieter (z. B. Graphite) verfügen, müssen Sie das Übertragungsintervall des Datenanbieters so ändern, dass es gleich oder größer als das Erfassungsintervall des Unified Managers ist.

Ändern Sie die Dauer, für die Unified Manager Ereignis- und Leistungsdaten speichert

Standardmäßig speichert Unified Manager Ereignisdaten und Leistungsdaten für alle überwachten Cluster 6 Monate lang. Nach Ablauf dieser Zeit werden ältere Daten automatisch gelöscht, um Platz für neue Daten zu schaffen. Dieser Standardzeitrahmen funktioniert für die meisten Konfigurationen gut, aber bei sehr großen Konfigurationen mit vielen Clustern und Knoten muss der Aufbewahrungszeitraum möglicherweise verkürzt werden, damit Unified Manager optimal funktioniert.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Sie können die Aufbewahrungszeiträume für diese beiden Datentypen auf der Seite „Datenaufbewahrung“ ändern. Diese Einstellungen wirken sich auf die Aufbewahrung von Daten aus allen Clustern aus, die diese Instanz von Unified Manager überwacht.

> Unified Manager sammelt alle 5 Minuten Leistungsstatistiken. Jeden Tag werden die 5-Minuten-Statistiken zu stündlichen Leistungsstatistiken zusammengefasst. Es speichert 30 Tage lang 5-minütige historische Leistungsdaten und 6 Monate lang stündlich zusammengefasste Leistungsdaten (standardmäßig).

Sie sollten die Aufbewahrungsfrist nur dann verkürzen, wenn der Speicherplatz knapp wird oder die Sicherung und andere Vorgänge sehr lange dauern. Die Verkürzung der Aufbewahrungsfrist hat folgende Auswirkungen:

- Alte Leistungsdaten werden nach Mitternacht aus der Unified Manager-Datenbank gelöscht.
- Alte Ereignisdaten werden sofort aus der Unified Manager-Datenbank gelöscht.
- Ereignisse vor Ablauf der Aufbewahrungsfrist können in der Benutzeroberfläche nicht mehr angezeigt werden.
- Stellen in der Benutzeroberfläche, an denen stündliche Leistungsstatistiken angezeigt werden, sind vor Ablauf der Aufbewahrungsfrist leer.
- Wenn die Aufbewahrungsdauer des Ereignisses die Aufbewahrungsdauer der Leistungsdaten überschreitet, wird unter dem Leistungsschieberegler eine Meldung angezeigt, die darauf hinweist, dass für ältere Leistungsereignisse möglicherweise keine Hintergrunddaten in den zugehörigen Diagrammen vorhanden sind.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Richtlinien** > **Datenaufbewahrung**.
2. Wählen Sie auf der Seite **Datenaufbewahrung** das Schieberegler-Tool im Bereich „Ereignisaufbewahrung“ oder „Aufbewahrung von Leistungsdaten“ aus, verschieben Sie es auf die Anzahl der Monate, für die die Daten aufbewahrt werden sollen, und klicken Sie auf **Speichern**.

Unbekannter Authentifizierungsfehler

Wenn Sie einen authentifizierungsbezogenen Vorgang ausführen, z. B. Remotebenutzer oder -gruppen hinzufügen, bearbeiten, löschen oder testen, wird möglicherweise die folgende Fehlermeldung angezeigt: `Unknown authentication error.`

Ursache

Dieses Problem kann auftreten, wenn Sie für die folgenden Optionen einen falschen Wert festgelegt haben:

- Administratorname des Active Directory-Authentifizierungsdienstes
- Bind Distinguished Name des OpenLDAP-Authentifizierungsdienstes

Korrekturmaßnahme

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Geben Sie basierend auf dem von Ihnen ausgewählten Authentifizierungsdienst die entsprechenden Informationen für den Administratornamen oder den Bind Distinguished Name ein.
3. Klicken Sie auf **Authentifizierung testen**, um die Authentifizierung mit den von Ihnen angegebenen Details zu testen.
4. Klicken Sie auf **Speichern**.

Benutzer nicht gefunden

Wenn Sie einen authentifizierungsbezogenen Vorgang ausführen, z. B. Remotebenutzer oder -gruppen hinzufügen, bearbeiten, löschen oder testen, 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 Sie den Basis-Distinguished Name auf einen falschen Wert festgelegt haben.

Korrekturmaßnahme

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Geben Sie die entsprechenden Informationen für den Basis-Distinguished Name ein.
3. Klicken Sie auf **Speichern**.

Problem beim Hinzufügen von LDAP mithilfe anderer Authentifizierungsdienste

Wenn Sie „Andere“ als Authentifizierungsdienst auswählen, behalten die Benutzer- und Gruppenobjektklassen 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 richtig konfiguriert.

Korrekturmaßnahme

Sie können dieses Problem manuell beheben, indem Sie eine der folgenden Problemumgehungen verwenden.

Wenn Ihre LDAP-Benutzerobjektklasse und Gruppenobjektklasse „Benutzer“ bzw. „Gruppe“ sind, führen Sie die folgenden Schritte aus:

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Wählen Sie im Dropdown-Menü **Authentifizierungsdienst** die Option **Active Directory** und dann **Andere** aus.
3. Füllen Sie die Textfelder aus.

Wenn Ihre LDAP-Benutzerobjektklasse und Gruppenobjektklasse „posixAccount“ bzw. „posixGroup“ sind, führen Sie die folgenden Schritte aus:

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote-Authentifizierung**.
2. Wählen Sie im Dropdown-Menü **Authentifizierungsdienst** die Option **OpenLDAP** und dann **Andere** aus.
3. Füllen Sie die Textfelder aus.

Wenn die ersten beiden Workarounds nicht funktionieren, rufen Sie den `option-set` API und legen Sie die `auth.ldap.userObjectClass` Und `auth.ldap.groupObjectClass` Optionen auf die richtigen Werte.

Problem mit der Protokollrotation des NetApp Manageability SDK auf Windows-Systemen

Nachdem Sie einen ONTAPI API-basierten Cluster zu Unified Manager auf einem Windows-Betriebssystem hinzugefügt haben, `nmsdk.log` Die Dateigröße nimmt zu und überschreitet die Größenbeschränkung von 10 MB.

Ursache

Dieses Problem kann auftreten, wenn keine Protokollrotation stattfindet.

Korrekturmaßnahme

1. Stoppen Sie Unified Manager.
2. Wenn Sie Unified Manager unter Windows installieren, installieren Sie Logrotate Version 0.0.0.18. Weitere Informationen finden Sie im"Leitfaden zur Sicherheitshärtung für den technischen Bericht zum NetApp Manageability SDK" .
3. Starten Sie Unified Manager.

Verwalten von Ereignissen und Warnungen

Ereignisse verwalten

Ereignisse helfen Ihnen, Probleme in den überwachten Clustern zu identifizieren.

Was sind Active IQ Plattformereignisse?

Unified Manager kann Ereignisse anzeigen, die von der Active IQ Plattform erkannt wurden. Diese Ereignisse werden erstellt, indem ein Regelsatz für AutoSupport -Nachrichten ausgeführt wird, die von allen von Unified Manager überwachten Speichersystemen generiert werden.

Weitere Informationen finden Sie unter "So werden Active IQ Plattformereignisse generiert".

Unified Manager sucht automatisch nach einer neuen Regeldatei und lädt nur dann eine neue Datei herunter, wenn neuere Regeln vorhanden sind. An Standorten ohne externen Netzwerkzugriff müssen Sie die Regeln manuell über **Speicherverwaltung** > **Ereigniseinrichtung** > **Regeln hochladen** hochladen.

Diese Active IQ -Ereignisse überschneiden sich nicht mit vorhandenen Unified Manager-Ereignissen und identifizieren Vorfälle oder Risiken in Bezug auf Systemkonfiguration, Verkabelung, bewährte Methoden und Verfügbarkeitsprobleme.

Weitere Informationen zum Aktivieren von Plattformereignissen finden Sie unter"Aktivieren von Active IQ Portalereignissen" . Weitere Informationen zum Hochladen von Regeldateien finden Sie unter"Hochladen einer neuen Active IQ Regeldatei" .

NetApp Active IQ ist ein Cloud-basierter Service, der prädiktive Analysen und proaktiven Support zur Optimierung des Speichersystembetriebs in der NetApp Hybrid Cloud bietet. Sehen "NetApp Active IQ" für weitere Informationen.

Was sind Event Management System-Ereignisse?

Das Event Management System (EMS) sammelt Ereignisdaten aus verschiedenen Teilen des ONTAP Kernels und stellt Mechanismen zur Ereignisweiterleitung bereit. Diese ONTAP -Ereignisse können als EMS-Ereignisse im Unified Manager gemeldet werden. Zentralisierte Überwachung und Verwaltung erleichtern die Konfiguration kritischer EMS-Ereignisse und Warnbenachrichtigungen basierend auf diesen EMS-Ereignissen.

Die Unified Manager-Adresse wird dem Cluster als Benachrichtigungsziel hinzugefügt, wenn Sie den Cluster zu Unified Manager hinzufügen. Ein EMS-Ereignis wird gemeldet, sobald das Ereignis im Cluster auftritt.

Es gibt zwei Methoden zum Empfangen von EMS-Ereignissen in Unified Manager:

- Eine bestimmte Anzahl wichtiger EMS-Ereignisse wird automatisch gemeldet.
- Sie können den Empfang einzelner 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-Nachrichten	Abonnierte EMS-Nachrichten
Verfügbare EMS-Ereignisse	Teilmenge der EMS-Ereignisse	Alle EMS-Veranstaltungen
Name der EMS-Nachricht bei Auslösung	Unified Manager-Ereignisname (konvertiert vom EMS-Ereignisnamen)	Unspezifisch im Format „Fehler EMS empfangen“. Die detaillierte Meldung enthält das Punktnotationsformat des tatsächlichen EMS-Ereignisses
Empfangene Nachrichten	Sobald der Cluster entdeckt 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“, „Gelöst“ und „Veraltet“	Das EMS-Ereignis wird nach der Aktualisierung des Clusters, 15 Minuten nach der Erstellung des Ereignisses, obsolet.
Erfasst Ereignisse während der Ausfallzeit von Unified Manager	Ja, wenn das System startet, kommuniziert es mit jedem Cluster, um fehlende Ereignisse abzurufen	Nein
Veranstaltungsdetails	Vorgeschlagene Korrekturmaßnahmen werden direkt aus ONTAP importiert, um konsistente Lösungen zu gewährleisten	Korrekturmaßnahmen sind auf der Seite „Ereignisdetails“ nicht verfügbar

Einige der neuen automatischen EMS-Ereignisse sind Informationsereignisse, die darauf hinweisen, dass ein vorheriges Ereignis behoben wurde. Beispielsweise zeigt das Informationsereignis „FlexGroup -Bestandteile – Speicherplatzstatus alles in Ordnung“ an, dass das Fehlerereignis „FlexGroup -Bestandteile haben Speicherplatzprobleme“ behoben wurde. Informationsereignisse können nicht mit demselben Ereignislebenszyklus wie andere Ereignisschweretypen verwaltet werden. Das Ereignis wird jedoch automatisch verworfen, wenn auf demselben Datenträger ein weiteres Fehlerereignis vom Typ „Speicherplatzprobleme“ auftritt.

EMS-Ereignisse, die automatisch zu 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 mit ONTAP 9.5 oder höher verfügbar:

Unified Manager-Ereignisname	EMS-Ereignisname	Betroffene Ressource	Unified Manager-Schweregrad
Zugriff auf Cloud-Ebene für Aggregatverlagerung verweigert	arl.netra.ca.check.failed	Aggregat	Fehler
Zugriff auf Cloud-Ebene für Aggregatverlagerung während Speicher-Failover verweigert	gb.netra.ca.check.failed	Aggregat	Fehler
Neusynchronisierung der FabricPool -Spiegelreplikation abgeschlossen	wafl.ca.resync.complete	Cluster	Fehler
FabricPool -Speicherplatz fast voll	fabricpool.nearly.full	Cluster	Fehler
NVMe-oF-Karenzzeitraum gestartet	nvmf.graceperiod.start	Cluster	Warnung
NVMe-oF-Gnadenfrist aktiv	nvmf.graceperiod.active	Cluster	Warnung
NVMe-oF-Karenzzeit abgelaufen	nvmf.graceperiod.expired	Cluster	Warnung
LUN zerstört	lun.destroy	LUN	Information
Cloud AWS MetaDataConnFail	cloud.aws.metadataConnFail	Node	Fehler
Cloud AWS IAMCredsAbgelaufen	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	Information
Cloud AWS IAMRoleInvalid	cloud.aws.iamRoleInvalid	Node	Fehler

Unified Manager-Ereignisname	EMS-Ereignisname	Betroffene Ressource	Unified Manager-Schweregrad
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
Anforderung stimmt nicht mit Cloud-Tier-Signatur überein	osc.signatureMismatch	Node	Fehler
Einer der NFSv4-Pools ist erschöpft	Nblade.nfsV4PoolExhaust	Node	Kritisch
QoS-Monitor-Speicher maximal	qos.monitor.memory.maxed	Node	Fehler
QoS-Monitor-Speicher verringert	qos.monitor.memory.abated	Node	Information
NVMeNS zerstören	NVMeNS.destroy	Namensraum	Information
NVMeNS Online	NVMeNS.offline	Namensraum	Information
NVMeNS Offline	NVMeNS.online	Namensraum	Information
NVMeNS hat keinen Platz mehr	Kein Speicherplatz mehr für NVMeNS	Namensraum	Warnung
Synchrone Replikation nicht synchron	SMS-Status nicht synchron	SnapMirror -Beziehung	Warnung
Synchrone Replikation wiederhergestellt	sms.status.in.sync	SnapMirror -Beziehung	Information
Automatische Neusynchronisierung der synchronen Replikation fehlgeschlagen	SMS-Neusynchronisierungsversuch fehlgeschlagen	SnapMirror -Beziehung	Fehler
Viele CIFS-Verbindungen	Nblade.cifsManyAuths	SVM	Fehler

Unified Manager-Ereignisname	EMS-Ereignisname	Betroffene Ressource	Unified Manager-Schweregrad
Maximale CIFS-Verbindung 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, eine nicht vorhandene CIFS-Freigabe zu verbinden	Nblade.cifsNoPrivShare	SVM	Kritisch
CIFS-Schattenkopie-Vorgang fehlgeschlagen	cifs.shadowcopy.failure	SVM	Fehler
Vom AV-Server gefundener Virus	Nblade.vscanVirusDetected	SVM	Fehler
Keine AV-Serververbindung für Virenscan	Nblade.vscanNoScannerConn	SVM	Kritisch
Kein AV-Server registriert	Nblade.vscanNoRegdScanner	SVM	Fehler
Keine reagierende AV-Serververbindung	Nblade.vscanConnInactive	SVM	Information
AV-Server zu beschäftigt, um neue Scan-Anforderungen anzunehmen	Nblade.vscanConnBackPressure	SVM	Fehler
Versuch eines nicht autorisierten Benutzers, den AV-Server zu beschädigen	Nblade.vscanBadUserPrivAccess	SVM	Fehler
FlexGroup -Bestandteile haben Platzprobleme	Flexgroup-Bestandteile haben Platzprobleme	Volumen	Fehler
FlexGroup -Bestandteile Raumstatus Alles OK	flexgroup.constituents.space.status.all.ok	Volumen	Information

Unified Manager-Ereignisname	EMS-Ereignisname	Betroffene Ressource	Unified Manager-Schweregrad
FlexGroup -Bestandteile haben Inodes-Probleme	Flexgroup.Bestandteile.haben.Inodes.Probleme	Volumen	Fehler
FlexGroup -Bestandteile Inodes Status Alle OK	flexgroup.constituents.inodes.status.all.ok	Volumen	Information
Logischer Speicherplatz des Volumes fast voll	monitor.vol.nearFull.inc.sav	Volumen	Warnung
Logischer Speicherplatz des Volumes voll	monitor.vol.full.inc.sav	Volumen	Fehler
Volumen Logischer Speicherplatz Normal	monitor.vol.one.ok.inc.sav	Volumen	Information
WAFL -Volume-AutoSize -Fehler	wafl.vol.autoSize.fail	Volumen	Fehler
WAFL Volume AutoSize Fertig	wafl.vol.autoSize.done	Volumen	Information
WAFL READDIR-Dateivorgang-Timeout	wafl.readdir.expired	Volumen	Fehler

Abonnieren Sie ONTAP EMS-Events

Sie können den Empfang von Event Management System (EMS)-Ereignissen abonnieren, die von Systemen generiert werden, auf denen ONTAP -Software installiert ist. Eine Teilmenge der EMS-Ereignisse wird automatisch an Unified Manager gemeldet, zusätzliche EMS-Ereignisse werden jedoch nur gemeldet, wenn Sie diese Ereignisse abonniert haben.

Bevor Sie beginnen

Abonnieren Sie keine EMS-Ereignisse, die bereits automatisch zu Unified Manager hinzugefügt wurden, da dies zu Verwirrung führen kann, wenn Sie zwei Ereignisse für dasselbe Problem erhalten.

Sie können beliebig viele EMS-Events 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* bietet detaillierte Informationen zu allen EMS-Nachrichten für die angegebene Version der ONTAP 9-Software. Suchen Sie auf der Seite „ONTAP 9-Produktdokumentation“ nach der entsprechenden Version des *EMS-Ereigniskatalogs*, um eine Liste der entsprechenden Ereignisse zu erhalten.

"ONTAP 9 Produktbibliothek"

Sie können Warnmeldungen für die ONTAP EMS-Ereignisse konfigurieren, die Sie abonnieren, und Sie können benutzerdefinierte Skripte erstellen, die für diese Ereignisse ausgeführt werden.

Wenn Sie die abonnierten ONTAP EMS-Ereignisse nicht erhalten, liegt möglicherweise ein Problem mit der DNS-Konfiguration des Clusters vor, das verhindert, dass der Cluster den Unified Manager-Server erreicht. Um dieses Problem zu beheben, muss der Clusteradministrator die DNS-Konfiguration des Clusters korrigieren und anschließend Unified Manager neu starten. Dadurch werden die ausstehenden EMS-Ereignisse auf den Unified Manager-Server übertragen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Ereigniseinrichtung**.
2. Klicken Sie auf der Seite „Ereigniseinrichtung“ auf die Schaltfläche **EMS-Ereignisse abonnieren**.
3. Geben Sie im Dialogfeld „EMS-Ereignisse abonnieren“ den Namen des ONTAP EMS-Ereignisses ein, das Sie abonnieren möchten.

   Um die Namen der EMS-Ereignisse anzuzeigen, die Sie abonnieren können, können Sie in der ONTAP Cluster-Shell die folgenden Befehle verwenden: `event route show` Befehl (vor ONTAP 9) oder der `event catalog show` Befehl (ONTAP 9 oder höher).

   "So konfigurieren und empfangen Sie Warnungen vom ONTAP EMS Event Subscription in Active IQ Unified Manager"

4. Klicken Sie auf **Hinzufügen**.

   Das EMS-Ereignis wird der Liste „Abonnierte EMS-Ereignisse“ hinzugefügt, aber in der Spalte „Gilt für Cluster“ wird für das von Ihnen hinzugefügte EMS-Ereignis der Status „Unbekannt“ angezeigt.

5. Klicken Sie auf **Speichern und schließen**, um das EMS-Ereignisabonnement beim Cluster zu registrieren.
6. Klicken Sie erneut auf **EMS-Events abonnieren**.

   Für das von Ihnen hinzugefügte EMS-Ereignis wird in der Spalte „Gilt für Cluster“ der Status „Ja“ angezeigt.

   Wenn der Status nicht „Ja“ lautet, überprüfen Sie die Schreibweise des ONTAP EMS-Ereignisnamens. Wenn der Name falsch eingegeben wurde, müssen Sie das falsche Ereignis entfernen und das Ereignis anschließend erneut hinzufügen.

Wenn das ONTAP EMS-Ereignis eintritt, wird das Ereignis auf der Seite „Ereignisse“ angezeigt. Sie können das Ereignis auswählen, um Details zum EMS-Ereignis auf der Seite „Ereignisdetails“ anzuzeigen. Sie können auch die Disposition des Ereignisses verwalten oder Warnungen für das Ereignis erstellen.

Was passiert, wenn ein Ereignis empfangen wird?

Wenn Unified Manager ein Ereignis empfängt, wird es auf der Dashboard-Seite, auf der Inventarseite „Event Management“, auf den Registerkarten „Zusammenfassung“ und „Explorer“ der Seite „Cluster/Leistung“ und auf der objektspezifischen Inventarseite (z. B. der Inventarseite „Volumes/Health“) angezeigt.

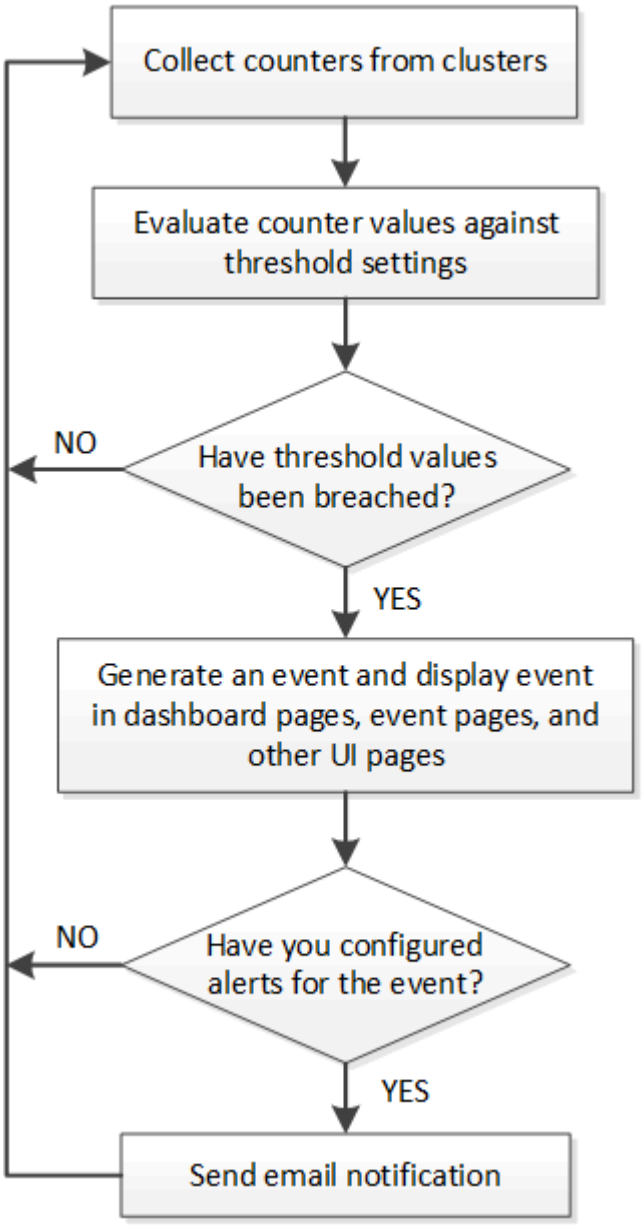
Wenn Unified Manager mehrere aufeinanderfolgende Vorkommen derselben Ereignisbedingung für dieselbe Clusterkomponente erkennt, behandelt es alle Vorkommen als ein einzelnes Ereignis und nicht als separate Ereignisse. Die Dauer des Ereignisses wird erhöht, um anzuzeigen, dass das Ereignis noch aktiv ist.

Je nachdem, wie Sie die Einstellungen auf der Seite „Alarm-Setup“ konfigurieren, können Sie andere Benutzer

über diese Ereignisse benachrichtigen. Der Alarm führt dazu, dass die folgenden Aktionen eingeleitet werden:

- Eine E-Mail über das Ereignis kann an alle Unified Manager Administrator-Benutzer gesendet werden.
- Das Ereignis kann an zusätzliche E-Mail-Empfänger gesendet werden.
- An den Trap-Empfänger kann ein SNMP-Trap gesendet werden.
- Zur Durchführung einer Aktion kann ein benutzerdefiniertes Skript ausgeführt werden.

Dieser Arbeitsablauf ist im folgenden Diagramm dargestellt.



Anzeigen von Ereignissen und Ereignisdetails

Sie können Details zu einem Ereignis anzeigen, das von Unified Manager ausgelöst wird, um Korrekturmaßnahmen zu ergreifen. Wenn beispielsweise ein Integritätsereignis „Volume offline“ vorliegt, können Sie auf dieses Ereignis klicken, um die Details anzuzeigen und Korrekturmaßnahmen durchzuführen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die Ereignisdetails umfassen Informationen wie die Quelle des Ereignisses, die Ursache des Ereignisses und alle Hinweise zum Ereignis.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.

   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 „Vorfall“ oder „Risiko“ aufweisen.

2. Wenn Sie eine bestimmte Kategorie von Ereignissen anzeigen möchten, beispielsweise Kapazitätsereignisse oder Leistungsereignisse, klicken Sie auf **Anzeigen** und wählen Sie aus dem Menü der Ereignistypen aus.
3. Klicken Sie auf den Namen des Ereignisses, dessen Details Sie anzeigen möchten.

   Die Ereignisdetails werden auf der Seite „Ereignisdetails“ angezeigt.

Nicht zugewiesene Ereignisse anzeigen

Sie können nicht zugewiesene Ereignisse anzeigen und dann jedes davon einem Benutzer zuweisen, der sie lösen kann.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.

   Standardmäßig werden neue und bestätigte Ereignisse auf der Inventarseite der Ereignisverwaltung angezeigt.

2. Wählen Sie im Bereich **Filter** im Bereich **Zugewiesen an** die Filteroption **Nicht zugewiesen** aus.

Ereignisse bestätigen und beheben

Sie sollten ein Ereignis bestätigen, bevor Sie mit der Arbeit an dem Problem beginnen, das das Ereignis verursacht hat, damit Sie nicht weiterhin wiederholt Warnmeldungen erhalten. Nachdem Sie Korrekturmaßnahmen für ein bestimmtes Ereignis ergriffen haben, sollten Sie das Ereignis als gelöst markieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können mehrere Ereignisse gleichzeitig bestätigen und beheben.

Sie können Informationsereignisse nicht bestätigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.
2. Führen Sie in der Ereignisliste die folgenden Aktionen aus, um die Ereignisse zu bestätigen:

Wenn Sie wollen…	Machen Sie Folgendes…
Bestätigen und markieren Sie ein einzelnes Ereignis als gelöst	a. Klicken Sie auf den Ereignisnamen. b. Ermitteln Sie auf der Seite „Ereignisdetails“ die Ursache des Ereignisses. c. Klicken Sie auf **Bestätigen**. d. Ergreifen Sie entsprechende Korrekturmaßnahmen. e. Klicken Sie auf **Als gelöst markieren**.
Mehrere Ereignisse bestätigen und als gelöst markieren	a. Ermitteln Sie die Ursache der Ereignisse auf der jeweiligen Seite mit den Ereignisdetails. b. Wählen Sie die Ereignisse aus. c. Klicken Sie auf **Bestätigen**. d. Ergreifen Sie entsprechende Korrekturmaßnahmen. e. Klicken Sie auf **Als gelöst markieren**.

   Nachdem das Ereignis als gelöst markiert wurde, wird es in die Liste der gelösten Ereignisse verschoben.

3. **Optional**: Fügen Sie im Bereich **Notizen und Aktualisierungen** eine Notiz darüber hinzu, wie Sie auf das Ereignis reagiert haben, und klicken Sie dann auf **Posten**.

Zuweisen von Ereignissen zu bestimmten Benutzern

Sie können nicht zugewiesene Ereignisse sich selbst oder anderen Benutzern, einschließlich Remotebenutzern, zuweisen. Sie können zugewiesene Ereignisse bei Bedarf einem anderen Benutzer neu zuweisen. Wenn beispielsweise bei einem Speicherobjekt 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-ID des Benutzers müssen korrekt konfiguriert sein.
- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.
2. Wählen Sie auf der Inventarseite **Event Management** ein oder mehrere Events aus, die Sie zuweisen möchten.
3. Weisen Sie das Ereignis zu, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie das Ereignis zuweisen möchten an…	Dann tun Sie Folgendes …
Selbst	Klicken Sie auf **Zuweisen an** > **Mir**.
Ein anderer Benutzer	a. Klicken Sie auf **Zuweisen an** > **Anderer Benutzer**. b. Geben Sie im Dialogfeld „Besitzer zuweisen“ den Benutzernamen ein oder wählen Sie einen Benutzer aus der Dropdownliste aus. c. Klicken Sie auf **Zuweisen**. Dem Benutzer wird eine E-Mail-Benachrichtigung gesendet. Wenn Sie keinen Benutzernamen eingeben oder keinen Benutzer aus der Dropdown-Liste auswählen und auf **Zuweisen** klicken, bleibt das Ereignis unzugeordnet.

Deaktivieren Sie unerwünschte Ereignisse

Alle Ereignisse sind standardmäßig aktiviert. Sie können Ereignisse global deaktivieren, um die Generierung von Benachrichtigungen für Ereignisse zu verhindern, die in Ihrer Umgebung nicht wichtig sind. Sie können deaktivierte Ereignisse aktivieren, wenn Sie den Empfang von Benachrichtigungen dafür wieder aufnehmen möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn Sie Ereignisse deaktivieren, werden die zuvor generierten Ereignisse im System als veraltet markiert und die für diese Ereignisse konfigurierten Warnungen werden nicht ausgelöst. Wenn Sie deaktivierte Ereignisse 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 Sie das Ereignis später aktivieren, generiert Unified Manager keine neuen Ereignisse für Objekte, die offline gingen, als das Ereignis deaktiviert war. Unified Manager generiert nur dann ein neues Ereignis, wenn sich der Objektstatus ändert, nachdem das Ereignis erneut aktiviert wurde.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Ereigniseinrichtung**.
2. Deaktivieren oder aktivieren Sie Ereignisse auf der Seite **Ereignis-Setup**, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Ereignisse deaktivieren	a. Klicken Sie auf **Deaktivieren**. b. Wählen Sie im Dialogfeld „Ereignisse deaktivieren“ den Schweregrad des Ereignisses aus. c. Wählen Sie in der Spalte „Übereinstimmende Ereignisse“ die Ereignisse aus, die Sie basierend auf dem Schweregrad des Ereignisses deaktivieren möchten, und klicken Sie dann auf den Rechtspfeil, um diese Ereignisse in die Spalte „Ereignisse deaktivieren“ zu verschieben. d. Klicken Sie auf **Speichern und schließen**. e. Überprüfen Sie, ob die von Ihnen deaktivierten Ereignisse in der Listenansicht der Seite „Ereigniseinrichtung“ angezeigt werden.
Ereignisse aktivieren	a. Aktivieren Sie das Kontrollkästchen für das oder die Ereignisse, die Sie aktivieren möchten. b. Klicken Sie auf **Aktivieren**.

Beheben Sie Probleme mit der automatischen Korrektur durch Unified Manager

Es gibt bestimmte Ereignisse, die Unified Manager gründlich diagnostizieren und mithilfe der Schaltfläche **Fix It** eine einzige Lösung bereitstellen kann. Sofern verfügbar, werden diese Lösungen im Dashboard, auf der Seite mit den Ereignisdetails und in der Auswahl „Workload-Analyse“ im linken Navigationsmenü angezeigt.

Für die meisten Ereignisse gibt es eine Reihe möglicher Lösungen, die auf der Seite mit den Ereignisdetails angezeigt werden, sodass Sie mit dem ONTAP System Manager oder der ONTAP CLI die beste Lösung implementieren können. Eine **Fix It**-Aktion ist verfügbar, wenn Unified Manager festgestellt hat, dass es eine einzige Lösung zur Behebung des Problems gibt und dass es mit einem ONTAP CLI-Befehl behoben werden kann.

Schritte

1. Um Ereignisse anzuzeigen, die über das **Dashboard** behoben werden können, klicken Sie auf **Dashboard**.
2. Um alle Probleme zu beheben, die Unified Manager beheben kann, klicken Sie auf die Schaltfläche **Fix It**. Um ein Problem zu beheben, das bei mehreren Objekten auftritt, klicken Sie auf die Schaltfläche **Alle beheben**.

Informationen zu den Problemen, die durch automatische Korrektur behoben werden können, finden Sie unter"Welche Probleme kann Unified Manager beheben?" .

Aktivieren und Deaktivieren der Active IQ -Ereignisberichterstattung

Active IQ Plattformereignisse werden standardmäßig generiert und in der Benutzeroberfläche des Unified Managers angezeigt. Wenn Sie feststellen, dass diese Ereignisse zu „laut“ sind oder Sie diese Ereignisse nicht in Unified Manager anzeigen möchten, können Sie die Generierung dieser Ereignisse deaktivieren. Sie können sie zu einem späteren Zeitpunkt aktivieren, wenn Sie diese Benachrichtigungen weiterhin erhalten möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Wenn Sie diese Funktion deaktivieren, empfängt Unified Manager sofort keine Active IQ Plattformereignisse mehr.

Wenn Sie diese Funktion aktivieren, beginnt Unified Manager, basierend auf der Zeitzone des Clusters, kurz nach Mitternacht mit dem Empfang von Active IQ -Plattformereignissen. Die Startzeit basiert darauf, wann Unified Manager AutoSupport Nachrichten von jedem Cluster empfängt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Funktionseinstellungen**.
2. Deaktivieren oder aktivieren Sie auf der Seite **Funktionseinstellungen** Active IQ -Plattformereignisse, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Deaktivieren von Active IQ Plattformereignissen	Bewegen Sie im Bereich * Active IQ Portalereignisse* den Schieberegler nach links.
Aktivieren von Active IQ Plattformereignissen	Bewegen Sie im Bereich * Active IQ Portalereignisse* den Schieberegler nach rechts.

Laden Sie eine neue Active IQ Regeldatei hoch

Unified Manager sucht automatisch nach einer neuen Active IQ Ereignisdatei (Regeln) und lädt eine neue Datei herunter, wenn neuere Regeln vorhanden sind. An Standorten ohne externen Netzwerkzugriff müssen Sie die Regeldatei jedoch manuell hochladen.

Active IQ Regeln werden auch als sichere Config Advisor (CA)-Regeln bezeichnet.

Wenn Sie Unified Manager an einem Standort ohne Netzwerkverbindung installieren oder auf eine bestimmte Version aktualisieren, stehen die gebündelten Active IQ Regeln automatisch zum Hochladen zur Verfügung. 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 Speichersysteme weiterhin optimal funktionieren.

Bevor Sie beginnen

- Die Ereignisberichterstattung des Active IQ Portals muss aktiviert sein. Diese Funktion ist standardmäßig aktiviert. Weitere Informationen finden Sie unter"Aktivieren von Active IQ Portalereignissen" .

- Sie müssen die Regeldatei von der NetApp Support-Site herunterladen.

  Die Regeldatei befindet sich unter: https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

Schritte

1. Navigieren Sie auf einem Computer mit Netzwerkzugriff zur NetApp -Support-Site und laden Sie die aktuellen Regeln herunter `.zip` Datei.

   Das gebündelte Regelpaket umfasst das Regelrepository, Datenquellen und einen NetApp -KB-Artikel.

   > Auf Windows-Systemen ist der NetApp -KB-Artikel an einem Standort ohne Netzwerkkonnektivität nicht standardmäßig im Installationsprogramm enthalten. Sie können die Datei *secure_rules.zip* von der Support-Site herunterladen und hochladen, um den KB-Artikel mit allen Regeln anzuzeigen.

2. Übertragen Sie die Regeldatei auf ein Medium, das Sie in den sicheren Bereich bringen können, und kopieren Sie es dann auf ein System im sicheren Bereich.
3. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Ereigniseinrichtung**.
4. Klicken Sie auf der Seite **Ereigniseinrichtung** auf die Schaltfläche **Regeln hochladen**.
5. Navigieren Sie im Dialogfeld **Upload-Regeln** zu den Regeln und wählen Sie sie aus `.zip` Datei, die Sie heruntergeladen haben, und klicken Sie auf **Hochladen**.

   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 Vorfallereignisse.

Weitere Informationen finden Sie in diesem Knowledge Base-Artikel (KB): "So aktualisieren Sie AIQCASecure-Regeln manuell in Active IQ Unified Manager" .

So werden Active IQ Plattformereignisse generiert

Vorfälle und Risiken der Active IQ -Plattform werden in Unified Manager-Ereignisse umgewandelt, wie im folgenden Diagramm dargestellt.

Wie Sie sehen, wird die auf der Active IQ Plattform kompilierte Regeldatei auf dem neuesten Stand gehalten, Cluster- AutoSupport -Nachrichten werden täglich generiert und Unified Manager aktualisiert die Liste der Ereignisse täglich.

Beheben Sie Active IQ Plattformereignisse

Vorfälle und Risiken der Active IQ -Plattform ähneln anderen Unified Manager-Ereignissen, da sie zur Lösung anderen Benutzern zugewiesen werden können und über dieselben verfügbaren Status verfügen. Wenn Sie diese Art von Ereignissen jedoch mit der Schaltfläche **Fix It** beheben, können Sie die Lösung innerhalb weniger Stunden überprüfen.

Das folgende Diagramm zeigt die Aktionen, die Sie ausführen müssen (in Grün) und die Aktion, die Unified Manager ausführt (in Schwarz), wenn Ereignisse aufgelöst werden, die von der Active IQ Plattform generiert wurden.

Wenn Sie eine manuelle Lösung durchführen, müssen Sie sich beim System Manager oder der ONTAP Befehlszeilenschnittstelle anmelden, um das Problem zu beheben. Sie können das Problem erst überprüfen, nachdem der Cluster um Mitternacht eine neue AutoSupport -Nachricht generiert hat.

Wenn Sie eine halbautomatische Lösung mit der Schaltfläche **Fix It** durchführen, können Sie innerhalb weniger Stunden überprüfen, ob die Lösung erfolgreich war.

Konfigurieren der Ereignisaufbewahrungseinstellungen

Sie können die Anzahl der Monate angeben, die ein Ereignis auf dem Unified Manager-Server aufbewahrt wird, bevor es automatisch gelöscht wird.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Das Aufbewahren von Ereignissen für mehr als 6 Monate kann die Serverleistung beeinträchtigen und wird nicht empfohlen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Datenaufbewahrung**.
2. Wählen Sie auf der Seite **Datenaufbewahrung** den Schieberegler im Bereich „Ereignisaufbewahrung“ aus, verschieben Sie ihn auf die Anzahl der Monate, die Ereignisse aufbewahrt werden sollen, und klicken Sie auf **Speichern**.

Was ein Unified Manager-Wartungsfenster ist

Sie definieren ein Unified Manager-Wartungsfenster, um Ereignisse und Warnungen 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 der Ereignisverwaltung ein Ereignis „Wartungsfenster für Objekte gestartet“ veröffentlicht. Dieses Ereignis wird automatisch verworfen, wenn das Wartungsfenster endet.

Während eines Wartungsfensters werden die Ereignisse im Zusammenhang mit allen Objekten in diesem Cluster weiterhin generiert, sie werden jedoch auf keiner der UI-Seiten angezeigt und es werden keine Warnungen oder andere Arten von Benachrichtigungen für diese Ereignisse gesendet. Sie können jedoch die Ereignisse anzeigen, die während eines Wartungsfensters für alle Speicherobjekte generiert wurden, indem Sie auf der Inventarseite der Ereignisverwaltung eine der Anzeigeoptionen auswählen.

Sie können ein Wartungsfenster für die Zukunft planen, Sie können die Start- und Endzeiten für ein geplantes Wartungsfenster ändern und Sie können ein geplantes Wartungsfenster abbrechen.

Planen Sie ein Wartungsfenster, um Cluster-Ereignisbenachrichtigungen zu deaktivieren

Wenn Sie für einen Cluster eine Ausfallzeit planen, beispielsweise um den Cluster zu aktualisieren oder einen der Knoten zu verschieben, können Sie die Ereignisse und

Warnungen unterdrücken, die normalerweise während dieses Zeitraums generiert würden, indem Sie ein Wartungsfenster für Unified Manager planen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Während eines Wartungsfensters werden die Ereignisse, die sich auf alle Objekte in diesem Cluster beziehen, weiterhin generiert, sie werden jedoch nicht auf der Ereignisseite angezeigt und es werden keine Warnungen oder andere Arten von Benachrichtigungen für diese Ereignisse gesendet.

Die von Ihnen für das Wartungsfenster eingegebene Zeit basiert auf der Zeit auf dem Unified Manager-Server.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.
2. Wählen Sie in der Spalte **Wartungsmodus** für den Cluster den Schieberegler aus und verschieben Sie ihn nach rechts.

   Das Kalenderfenster wird angezeigt.

3. Wählen Sie Start- und Enddatum sowie -uhrzeit für das Wartungsfenster aus und klicken Sie auf **Übernehmen**.

   Neben dem Schieberegler erscheint die Meldung „Geplant“.

Wenn die Startzeit erreicht ist, wechselt der Cluster in den Wartungsmodus und ein Ereignis „Object Maintenance Window Started“ wird generiert.

Ändern oder Abbrechen eines geplanten Wartungsfensters

Wenn Sie ein zukünftiges Wartungsfenster für Unified Manager konfiguriert haben, können Sie die Start- und Endzeiten ändern oder das Wartungsfenster abbrechen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Das Abbrechen eines aktuell laufenden Wartungsfensters ist nützlich, wenn Sie die Clusterwartung vor dem geplanten Ende des Wartungsfensters abgeschlossen haben und wieder Ereignisse und Warnungen vom Cluster empfangen möchten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Cluster-Setup**.
2. In der Spalte **Wartungsmodus** für den Cluster:

Wenn Sie wollen…	Führen Sie diesen Schritt aus…
Ändern des Zeitrahmens für ein geplantes Wartungsfenster	a. Klicken Sie neben dem Schieberegler auf den Text „Geplant“. b. Ändern Sie das Start- und/oder Enddatum und die Uhrzeit und klicken Sie auf **Übernehmen**.

Wenn Sie wollen…	Führen Sie diesen Schritt aus…
Verlängern Sie die Länge eines aktiven Wartungsfensters	a. Klicken Sie neben dem Schieberegler auf den Text „Aktiv“. b. Ändern Sie das Enddatum und die Endzeit und klicken Sie auf **Übernehmen**.
Abbrechen eines geplanten Wartungsfensters	Wählen Sie den Schieberegler aus und verschieben Sie ihn nach links.
Abbrechen eines aktiven Wartungsfensters	Wählen Sie den Schieberegler aus und verschieben Sie ihn nach links.

Anzeigen von Ereignissen, die während eines Wartungsfensters aufgetreten sind

Bei Bedarf können Sie die Ereignisse anzeigen, die während eines Unified Manager-Wartungsfensters für alle Speicherobjekte generiert wurden. Die meisten Ereignisse werden im Status „Veraltet“ angezeigt, sobald das Wartungsfenster abgeschlossen ist und alle Systemressourcen wieder betriebsbereit sind.

Bevor Sie beginnen

Es muss mindestens ein Wartungsfenster abgeschlossen sein, bevor Ereignisse verfügbar sind.

Ereignisse, die während eines Wartungsfensters aufgetreten sind, werden standardmäßig nicht auf der Inventarseite der Ereignisverwaltung angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisse**.

   Standardmäßig werden alle aktiven (neuen und bestätigten) Ereignisse auf der Inventarseite der Ereignisverwaltung angezeigt.

2. Wählen Sie im Ansichtsbereich die Option **Alle während der Wartung generierten Ereignisse**.

   Die Liste der Ereignisse, die in den letzten 7 Tagen von allen Wartungsfenstersitzungen und von allen Clustern ausgelöst wurden, wird angezeigt.

3. Wenn für einen einzelnen Cluster mehrere Wartungsfenster vorhanden waren, können Sie auf das Kalendersymbol **Ausgelöste Zeit** klicken und den Zeitraum für die Wartungsfensterereignisse auswählen, die Sie anzeigen möchten.

Verwalten von Hostsystemressourcenereignissen

Unified Manager enthält einen Dienst, der Ressourcenprobleme auf dem Hostsystem überwacht, auf dem Unified Manager installiert ist. Probleme wie fehlender verfügbarer Speicherplatz oder Speichermangel auf dem Hostsystem können Verwaltungsstationsereignisse auslösen, die als Bannermeldungen oben auf der Benutzeroberfläche angezeigt werden.

Ereignisse der Verwaltungsstation weisen auf ein Problem mit dem Hostsystem hin, auf dem Unified Manager installiert ist. Zu den Problemen der Verwaltungsstation zählen beispielsweise zu wenig Speicherplatz auf dem Hostsystem, ein fehlender regelmäßiger Datenerfassungszyklus von Unified Manager und die Nichterfüllung oder verspätete Durchführung der Statistikanalyse, weil die nächste Datenerfassungsabfrage eingeleitet wurde.

Im Gegensatz zu allen anderen Ereignismeldungen des Unified Manager werden diese speziellen Warnungen und kritischen Ereignisse der Verwaltungsstation in Bannermeldungen angezeigt.

Schritt

1. Um Ereignisinformationen zur Verwaltungsstation anzuzeigen, führen Sie die folgenden Aktionen aus:

Wenn Sie wollen…	Machen Sie Folgendes…
Details zur Veranstaltung anzeigen	Klicken Sie auf das Ereignisbanner, um die Seite mit den Ereignisdetails anzuzeigen, die Lösungsvorschläge für das Problem enthält.
Alle Ereignisse der Verwaltungsstation anzeigen	a. Klicken Sie im linken Navigationsbereich auf **Event Management**. b. Klicken Sie im Bereich „Filter“ auf der Inventarseite der Ereignisverwaltung in der Liste „Quelltyp“ auf das Kontrollkästchen für die Verwaltungsstation.

Erfahren Sie mehr über Ereignisse

Wenn Sie die Konzepte zu Ereignissen verstehen, können Sie Ihre Cluster und Clusterobjekte effizienter verwalten und Warnmeldungen entsprechend definieren.

Ereignisstatusdefinitionen

Anhand des Status eines Ereignisses können Sie feststellen, ob eine entsprechende Korrekturmaßnahme erforderlich ist. Ein Ereignis kann „Neu“, „Bestätigt“, „Gelöst“ oder „Veraltet“ sein. Beachten Sie, 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 Status eines Ereignisses, wenn Sie es bestätigt haben.

- **Gelöst**

  Der Status eines Ereignisses, wenn es als gelöst markiert ist.

- **Veraltet**

  Der Status eines Ereignisses, wenn es automatisch korrigiert wird oder wenn die Ursache des Ereignisses nicht mehr gültig ist.

  Sie können ein veraltetes Ereignis weder bestätigen noch beheben.

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 in „Bestätigt“. Wenn Sie eine entsprechende Korrekturmaßnahme ergriffen haben, müssen Sie das Ereignis als gelöst markieren. Der Ereignisstatus ändert sich dann in „Gelöst“.

Wenn das Ereignis „Cluster nicht erreichbar“ aufgrund eines Stromausfalls generiert wird, nimmt der Cluster nach Wiederherstellung der Stromversorgung seinen Betrieb ohne Eingriff des Administrators wieder auf. Daher ist das Ereignis „Cluster nicht erreichbar“ nicht mehr gültig und der Ereignisstatus ändert sich im nächsten Überwachungszyklus in „Veraltet“.

Unified Manager sendet eine Warnung, wenn ein Ereignis den Status „Veraltet“ oder „Gelöst“ hat. Die Betreffzeile und der Inhalt einer E-Mail-Benachrichtigung geben Auskunft über den Ereignisstatus. Ein SNMP-Trap enthält auch Informationen zum Ereignisstatus.

Beschreibung der Ereignisschweregrade

Jedem Ereignis ist ein Schweregrad zugeordnet, der Ihnen dabei hilft, die Ereignisse zu priorisieren, die sofortige Korrekturmaßnahmen erfordern.

- **Kritisch**

  Es ist ein Problem aufgetreten, das zu einer Dienstunterbrechung führen kann, wenn nicht sofort Abhilfemaßnahmen ergriffen werden.

  Leistungskritische Ereignisse werden nur ab benutzerdefinierten Schwellenwerten gesendet.

- **Fehler**

  Die Ereignisquelle funktioniert noch, es sind jedoch Korrekturmaßnahmen erforderlich, um eine Dienstunterbrechung zu vermeiden.

- **Warnung**

  Bei der Ereignisquelle ist ein Vorfall aufgetreten, den Sie kennen sollten, oder ein Leistungsindikator für ein Clusterobjekt liegt außerhalb des normalen Bereichs und sollte überwacht werden, um sicherzustellen, dass er nicht den kritischen Schweregrad erreicht. Ereignisse dieses Schweregrads verursachen keine Dienstunterbrechung und es sind möglicherweise keine sofortigen Korrekturmaßnahmen erforderlich.

  Leistungswarnungsereignisse werden von benutzerdefinierten, systemdefinierten oder dynamischen Schwellenwerten gesendet.

- **Information**

Das Ereignis tritt ein, wenn ein neues Objekt erkannt oder eine Benutzeraktion ausgeführt wird. Wenn beispielsweise ein Speicherobjekt gelöscht wird oder Konfigurationsänderungen vorgenommen werden, wird das Ereignis mit dem Schweregrad „Informationen“ generiert.

Informationsereignisse werden direkt von ONTAP gesendet, wenn eine Konfigurationsänderung erkannt wird.

Beschreibung der Ereignisauswirkungsstufen

Jedem Ereignis ist eine Auswirkungsstufe (Vorfall, Risiko, Ereignis oder Upgrade) zugeordnet, damit Sie die Ereignisse priorisieren können, die sofortige Korrekturmaßnahmen erfordern.

- **Vorfall**

  Ein Vorfall ist eine Reihe von Ereignissen, die dazu führen können, dass ein Cluster dem Client keine Daten mehr bereitstellt und nicht mehr genügend Speicherplatz für die Daten zur Verfügung steht. Ereignisse mit der Auswirkungsstufe „Vorfall“ sind die schwerwiegendsten. Um eine Unterbrechung des Dienstes zu vermeiden, sollten umgehend Korrekturmaßnahmen ergriffen werden.

- **Risiko**

  Ein Risiko ist eine Reihe von Ereignissen, die möglicherweise dazu führen können, dass ein Cluster keine Daten mehr an den Client liefert und nicht mehr genügend Speicherplatz für die Daten zur Verfügung steht. Ereignisse mit der Auswirkungsstufe „Risiko“ können zu Dienstunterbrechungen führen. Möglicherweise sind Korrekturmaßnahmen erforderlich.

- **Ereignis**

  Ein Ereignis ist eine Zustands- oder Statusänderung von Speicherobjekten und ihren Attributen. Ereignisse mit der Auswirkungsstufe „Ereignis“ haben informativen Charakter und erfordern keine Korrekturmaßnahmen.

- **Upgrade**

  Upgrade-Ereignisse sind ein bestimmter Ereignistyp, der von der Active IQ Plattform gemeldet wird. Diese Ereignisse identifizieren Probleme, für deren Lösung Sie ein Upgrade der ONTAP -Software, der Knoten-Firmware oder der Betriebssystemsoftware (für Sicherheitshinweise) benötigen. Bei einigen dieser Probleme möchten Sie möglicherweise sofort Abhilfemaßnahmen ergreifen, während andere Probleme möglicherweise bis zu Ihrer nächsten planmäßigen Wartung warten können.

Beschreibung der Ereignisauswirkungsbereiche

Ereignisse werden in sechs Auswirkungsbereiche (Verfügbarkeit, Kapazität, Konfiguration, Leistung, Schutz und Sicherheit) kategorisiert, damit Sie sich auf die Ereignistypen konzentrieren können, für die Sie verantwortlich sind.

- **Verfügbarkeit**

  Verfügbarkeitsereignisse benachrichtigen Sie, wenn ein Speicherobjekt offline geht, ein Protokolldienst ausfällt, ein Problem mit dem Speicherfailover auftritt oder ein Problem mit der Hardware auftritt.

- **Kapazität**

Kapazitätsereignisse benachrichtigen Sie, wenn Ihre Aggregate, Volumes, LUNs oder Namespaces sich einem Größenschwellenwert nähern oder diesen bereits erreicht haben oder wenn die Wachstumsrate für Ihre Umgebung ungewöhnlich ist.

- **Konfiguration**

  Konfigurationsereignisse informieren Sie über die Erkennung, Löschung, Hinzufügung, Entfernung oder Umbenennung Ihrer Speicherobjekte. Konfigurationsereignisse haben die Auswirkungsstufe „Ereignis“ und den Schweregrad „Information“.

- **Leistung**

  Leistungsereignisse benachrichtigen Sie über Ressourcen-, Konfigurations- oder Aktivitätsbedingungen in Ihrem Cluster, die sich negativ auf die Geschwindigkeit der Datenspeichereingabe oder des Datenabrufs Ihrer überwachten Speicherobjekte auswirken können.

- **Schutz**

  Schutzereignisse benachrichtigen Sie über Vorfälle oder Risiken im Zusammenhang mit SnapMirror -Beziehungen, Problemen mit der Zielkapazität, Problemen mit SnapVault -Beziehungen oder Problemen mit Schutzaufträgen. Alle ONTAP Objekte (insbesondere Aggregate, Volumes und SVMs), die sekundäre Volumes und Schutzbeziehungen hosten, werden im Bereich „Schutzauswirkungen“ kategorisiert.

- **Sicherheit**

  Sicherheitsereignisse informieren Sie darüber, wie sicher Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes sind, basierend auf den im "NetApp Security Hardening Guide für ONTAP 9" .

  Darüber hinaus enthält dieser Bereich Upgrade-Ereignisse, die von der Active IQ Plattform gemeldet werden.

So wird der Objektstatus berechnet

Der Objektstatus wird durch das schwerwiegendste Ereignis bestimmt, das derzeit den Status „Neu“ oder „Bestätigt“ aufweist. Wenn beispielsweise der Status eines Objekts „Fehler“ lautet, weist eines der Ereignisse des Objekts den Schweregrad „Fehler“ auf. Wenn Korrekturmaßnahmen ergriffen wurden, wechselt der Ereignisstatus zu „Gelöst“.

Details zum dynamischen Leistungsereignisdiagramm

Bei dynamischen Leistungsereignissen werden im Abschnitt „Systemdiagnose“ der Seite „Ereignisdetails“ die wichtigsten Workloads mit der höchsten Latenz oder Nutzung der umkämpften Clusterkomponente aufgelistet.

Die Leistungsstatistiken basieren auf dem Zeitpunkt, zu dem das Leistungsereignis erkannt wurde, bis zum Zeitpunkt der letzten Ereignisanalyse. Die Diagramme zeigen auch historische Leistungsstatistiken für die umstrittene Clusterkomponente an.

Sie können beispielsweise Workloads mit hoher Auslastung einer Komponente identifizieren, um zu bestimmen, welche Workload auf eine weniger ausgelastete Komponente verschoben werden soll. Durch die Verschiebung der Arbeitslast würde der Arbeitsaufwand für die aktuelle Komponente verringert und die Komponente möglicherweise aus dem Wettbewerb genommen. Oben in diesem Abschnitt stehen der Zeit- und Datumsbereich, in dem ein Ereignis erkannt und zuletzt analysiert wurde. Bei aktiven Ereignissen (neu oder

bestätigt) wird die letzte analysierte Zeit aktualisiert.

Die Latenz- und Aktivitätsdiagramme zeigen die Namen der wichtigsten Workloads an, wenn Sie mit dem Cursor über das Diagramm fahren. Wenn Sie auf das Menü „Workload-Typ“ rechts neben dem Diagramm klicken, können Sie die Workloads nach ihrer Rolle im Ereignis sortieren, einschließlich *Haie*, *Mobber* oder *Opfer*. Außerdem werden Details zu ihrer Latenz und ihrer Nutzung der umstrittenen Clusterkomponente angezeigt. Sie können den tatsächlichen Wert mit dem erwarteten Wert vergleichen, um zu sehen, wann die Arbeitslast außerhalb des erwarteten Latenz- oder Nutzungsbereichs lag. Weitere Informationen finden Sie unter"Von Unified Manager überwachte Workloadtypen" .

Wenn Sie nach der Spitzenabweichung der Latenz sortieren, werden systemdefinierte Workloads nicht in der Tabelle angezeigt, da die Latenz nur für benutzerdefinierte Workloads gilt. Workloads mit sehr niedrigen Latenzwerten werden in der Tabelle nicht angezeigt.

Weitere Informationen zu den dynamischen Leistungsschwellenwerten finden Sie unter"Analysieren von Ereignissen anhand dynamischer Leistungsschwellenwerte" .

Informationen dazu, wie Unified Manager die Arbeitslasten bewertet und die Sortierreihenfolge bestimmt, finden Sie unter"So ermittelt Unified Manager die Leistungsauswirkungen eines Ereignisses" .

Die Daten in den Diagrammen zeigen Leistungsstatistiken der letzten 24 Stunden vor der letzten Ereignisanalyse. Die tatsächlichen und erwarteten Werte für jede Arbeitslast basieren auf der Zeit, in der die Arbeitslast am Ereignis beteiligt war. Beispielsweise kann eine Arbeitslast in ein Ereignis verwickelt werden, nachdem das Ereignis erkannt wurde, sodass ihre Leistungsstatistiken möglicherweise nicht mit den Werten zum Zeitpunkt der Ereigniserkennung übereinstimmen. Standardmäßig werden die Workloads nach der Spitzenabweichung (höchsten Abweichung) bei der Latenz sortiert.

Da Unified Manager maximal 30 Tage lang 5-minütige historische Leistungs- und Ereignisdaten speichert, werden keine Leistungsdaten angezeigt, wenn das Ereignis älter als 30 Tage ist.

- **Spalte „Workload sortieren“**
  - **Latenzdiagramm**

    Zeigt die Auswirkungen des Ereignisses auf die Latenz der Arbeitslast während der letzten Analyse an.
  - **Spalte „Komponentennutzung“**

    Zeigt Details zur Arbeitslastnutzung der konkurrierenden Clusterkomponente an. In den Diagrammen ist die tatsächliche Nutzung als blaue Linie dargestellt. Ein roter Balken hebt die Ereignisdauer vom Erkennungszeitpunkt bis zum letzten analysierten Zeitpunkt hervor. Weitere Informationen finden Sie unter "Messwerte für die Workload-Leistung".

    Für die Netzwerkkomponente wird diese Spalte nicht angezeigt, da die Netzwerkleistungsstatistiken aus Aktivitäten außerhalb des Clusters stammen.
  - **Komponentenverwendung**

    Zeigt den Nutzungsverlauf in Prozent für die Netzwerkverarbeitung, Datenverarbeitung und Aggregatkomponenten oder den Aktivitätsverlauf in Prozent für die QoS-Richtliniengruppenkomponente an. Für die Netzwerk- oder Verbindungskomponenten wird das Diagramm nicht angezeigt. Sie können auf die Statistiken zeigen, um die Nutzungsstatistiken zu einem bestimmten Zeitpunkt anzuzeigen.

- **Gesamtverlauf der Schreibvorgänge in MB/s**

  Zeigt nur für die MetroCluster -Ressourcenkomponente den gesamten Schreibdurchsatz in Megabyte pro Sekunde (MBps) für alle Volume-Workloads an, die in einer MetroCluster -Konfiguration auf den Partnercluster gespiegelt werden.

- **Ereignisverlauf**

  Zeigt rot schattierte Linien an, um die historischen Ereignisse für die umstrittene Komponente anzuzeigen. Bei veralteten Ereignissen zeigt das Diagramm Ereignisse an, die vor der Erkennung des ausgewählten Ereignisses und nach seiner Lösung aufgetreten sind.

Von Unified Manager erkannte Konfigurationsänderungen

Unified Manager überwacht Ihre Cluster auf Konfigurationsänderungen, damit Sie feststellen können, ob eine Änderung ein Leistungsereignis verursacht oder dazu beigetragen hat. Auf den Seiten des Performance Explorers wird ein Symbol für Änderungsereignisse angezeigt ( ), um das Datum und die Uhrzeit anzugeben, wann die Änderung erkannt wurde.

Sie können die Leistungsdiagramme auf den Seiten des Leistungs-Explorers und auf der Seite „Arbeitslastanalyse“ überprüfen, um zu sehen, ob sich das Änderungsereignis auf die Leistung des ausgewählten Clusterobjekts ausgewirkt hat. Wenn die Änderung ungefähr zur gleichen Zeit wie ein Leistungsereignis erkannt wurde, hat die Änderung möglicherweise zu dem Problem beigetragen, das zur Auslösung der Ereigniswarnung geführt hat.

Unified Manager kann die folgenden Änderungsereignisse erkennen, die als Informationsereignisse kategorisiert werden:

- Ein Volumen wird zwischen Aggregaten verschoben.

  Unified Manager kann erkennen, wann die Verschiebung läuft, abgeschlossen ist oder fehlgeschlagen ist. Wenn Unified Manager während einer Volumeverschiebung ausfällt, erkennt es die Volumeverschiebung, wenn es wieder verfügbar ist, und zeigt ein Änderungsereignis dafür an.

- Die Durchsatzgrenze (MB/s oder IOPS) einer QoS-Richtliniengruppe, die eine oder mehrere überwachte Workloads enthält, ändert sich.

  Das Ändern eines Richtliniengruppenlimits kann zu zeitweiligen Spitzen in der Latenz (Reaktionszeit) führen, die auch Ereignisse für die Richtliniengruppe auslösen können. Die Latenz normalisiert sich allmählich und alle durch die Spitzen verursachten Ereignisse werden obsolet.

- Ein Knoten in einem HA-Paar übernimmt den Speicher seines Partnerknotens oder gibt ihn zurück.

  Unified Manager kann erkennen, wann die Übernahme-, Teilübernahme- oder Rückgabeoperation abgeschlossen ist. Wenn die Übernahme durch einen in Panik geratenen Knoten verursacht wird, erkennt Unified Manager das Ereignis nicht.

- Ein ONTAP -Upgrade- oder Wiederherstellungsvorgang wurde erfolgreich abgeschlossen.

  Es werden die vorherige und die neue Version angezeigt.

Liste der Ereignisse und Schweregrade

Sie können die Ereignisliste verwenden, um sich mit den Ereigniskategorien, Ereignisnamen und dem Schweregrad jedes Ereignisses vertraut zu machen, die Sie möglicherweise in Unified Manager sehen. Ereignisse werden in alphabetischer Reihenfolge nach Objektkategorie aufgelistet.

Aggregierte Ereignisse

Aggregatereignisse liefern Ihnen Informationen zum Status von Aggregaten, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungsstufe	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
Aggregat herabgestuft (ocumEvtAggregateRaidStateDegraded)	Risiko	Aggregat	Warnung
Cloud-Ebene teilweise erreichbar (ocumEventCloudTierPartiallyReachable)	Risiko	Aggregat	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Cloud-Ebene nicht erreichbar (ocumEventCloudTierUnreachable)	Risiko	Aggregat	Fehler
Zugriff auf Cloud-Ebene für Aggregatverlagerung verweigert *(arlNetraCaCheckFailed)	Risiko	Aggregat	Fehler
Zugriff auf Cloud-Ebene für Aggregatverlagerung während Speicher-Failover verweigert *(gbNetraCaCheckFailed)	Risiko	Aggregat	Fehler
Zurückgelassenes MetroCluster -Aggregat (ocumEvtMetroClusterAggregateLeftBehind)	Risiko	Aggregat	Fehler
MetroCluster -Aggregatspiegelung beeinträchtigt (ocumEvtMetroClusterAggregateMirrorDegraded)	Risiko	Aggregat	Fehler

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Aggregatspeicherplatz fast voll (ocumEvtAggregateNearlyFull)	Risiko	Aggregat	Warnung
Aggregatspeicher voll (ocumEvtAggregateFull)	Risiko	Aggregat	Fehler
Aggregierte Tage bis zur Vollendung (ocumEvtAggregateDaysUntilFullSoon)	Risiko	Aggregat	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Aggregat überbelegt (ocumEvtAggregateOvercommitted)	Risiko	Aggregat	Fehler
Aggregat fast überlastet (ocumEvtAggregateAlmostOvercommitted)	Risiko	Aggregat	Warnung
Aggregierte Snapshot-Reserve voll (ocumEvtAggregateSnapReserveFull)	Risiko	Aggregat	Warnung
Anormale Gesamtwachstumsrate (ocumEvtAggregateGrowthRateAbnormal)	Risiko	Aggregat	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Aggregat entdeckt (Nicht zutreffend)	Ereignis	Aggregat	Information
Aggregat umbenannt (Nicht zutreffend)	Ereignis	Aggregat	Information
Aggregat gelöscht (Nicht zutreffend)	Ereignis	Node	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für aggregierte IOPS überschritten (ocumAggregateIopsIncident)	Vorfall	Aggregat	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Warnschwelle für aggregierte IOPS überschritten (ocumAggregateIopsWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für aggregierte MB/s überschritten (ocumAggregateMbpsIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für aggregierte MB/s überschritten (ocumAggregateMbpsWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für aggregierte Latenz überschritten (ocumAggregateLatencyIncident)	Vorfall	Aggregat	Kritisch
Schwellenwert für Warnung vor aggregierter Latenz überschritten (ocumAggregateLatencyWarning)	Risiko	Aggregat	Warnung
Kritischer Schwellenwert für genutzte Gesamtleistungskapazität überschritten (ocumAggregatePerfCapacityUsedIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für genutzte Gesamtleistungskapazität überschritten (ocumAggregatePerfCapacityUsedWarning)	Risiko	Aggregat	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für Gesamtauslastung überschritten (ocumAggregateUtilizationIncident)	Vorfall	Aggregat	Kritisch
Warnschwelle für aggregierte Auslastung überschritten (ocumAggregateUtilizationWarning)	Risiko	Aggregat	Warnung
Schwellenwert für Überauslastung aggregierter Datenträger überschritten (ocumAggregateDisksOverUtilizedWarning)	Risiko	Aggregat	Warnung
Aggregierter dynamischer Schwellenwert überschritten (ocumAggregateDynamicEventWarning)	Risiko	Aggregat	Warnung

Cluster-Ereignisse

Clusterereignisse liefern Informationen zum Status von Clustern, sodass Sie die Cluster auf potenzielle Probleme überwachen können. Die Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignisnamen, den Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Im Cluster fehlen Ersatzfestplatten (ocumEvtDisksNoSpares)	Risiko	Cluster	Warnung
Cluster nicht erreichbar (ocumEvtClusterUnreachable)	Risiko	Cluster	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Clusterüberwachung fehlgeschlagen (ocumEvtClusterMonitoringFailed)	Risiko	Cluster	Warnung
Lizenzkapazitätsgrenzen des Cluster FabricPool überschritten (ocumEvtExternalCapacityTierSpaceFull)	Risiko	Cluster	Warnung
NVMe-oF-Karenzzeitraum gestartet *(nvmfGracePeriodStart)	Risiko	Cluster	Warnung
NVMe-oF-Karenzzeitraum aktiv *(nvmfGracePeriodActive)	Risiko	Cluster	Warnung
NVMe-oF-Karenzzeit abgelaufen *(nvmfGracePeriodExpired)	Risiko	Cluster	Warnung
Objektwartungsfenster gestartet (objectMaintenanceWindowStarted)	Ereignis	Cluster	Kritisch
Objektwartungsfenster beendet (objectMaintenanceWindowEnded)	Ereignis	Cluster	Information
Zurückgelassene MetroCluster -Ersatzfestplatten (ocumEvtSpareDiskLeftBehind)	Risiko	Cluster	Fehler
Automatische ungeplante Umschaltung von MetroCluster deaktiviert (ocumEvtMccAutomaticUnplannedSwitchOverDisabled)	Risiko	Cluster	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Cluster-Benutzerkennwort geändert *(cluster.passwd.changed)	Ereignis	Cluster	Information

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Schwellenwert für Cluster-Kapazitätsungleichgewicht überschritten (ocumConformanceNodeImbalanceWarning)	Risiko	Cluster	Warnung
Cluster-Cloud-Tier-Planung (clusterCloudTierPlanningWarning)	Risiko	Cluster	Warnung
Neusynchronisierung der FabricPool -Spiegelreplikation abgeschlossen *(waflCaResyncComplete)	Ereignis	Cluster	Warnung
FabricPool -Speicherplatz fast voll *(fabricpoolNearlyFull)	Risiko	Cluster	Fehler

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Knoten hinzugefügt (nicht zutreffend)	Ereignis	Cluster	Information
Knoten entfernt (Nicht zutreffend)	Ereignis	Cluster	Information
Cluster entfernt (Nicht zutreffend)	Ereignis	Cluster	Information

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Cluster hinzufügen fehlgeschlagen (Nicht zutreffend)	Ereignis	Cluster	Fehler
Clustername geändert (Nicht zutreffend)	Ereignis	Cluster	Information
Notfall-EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Kritisch
Kritischer EMS-Einsatz empfangen (Nicht zutreffend)	Ereignis	Cluster	Kritisch
EMS-Alarm erhalten (Nicht zutreffend)	Ereignis	Cluster	Fehler
Fehler EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Warnung
Warnung EMS erhalten (Nicht zutreffend)	Ereignis	Cluster	Warnung
Debug-EMS empfangen (Nicht zutreffend)	Ereignis	Cluster	Warnung
EMS-Benachrichtigung erhalten (Nicht zutreffend)	Ereignis	Cluster	Warnung
Informatives EMS erhalten (Nicht zutreffend)	Ereignis	Cluster	Warnung

ONTAP EMS-Ereignisse werden in drei Unified Manager-Ereignisschweregrade eingeteilt.

Unified Manager-Ereignisschweregrad	ONTAP EMS-Ereignisschweregrad
Kritisch	Notfall Kritisch
Fehler	Alarm

Warnung	Fehler Warnung Debuggen Beachten Informativ

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Schwellenwert für Cluster-Lastungleichgewicht überschritten()	Risiko	Cluster	Warnung
Kritischer Cluster-IOPS-Schwellenwert überschritten (ocumClusterIopsIncident)	Vorfall	Cluster	Kritisch
Cluster-IOPS-Warnschwelle überschritten (ocumClusterIopsWarning)	Risiko	Cluster	Warnung
Kritischer Schwellenwert für Cluster-MB/s überschritten (ocumClusterMbpsIncident)	Vorfall	Cluster	Kritisch
Cluster-MB/s-Warnschwelle überschritten (ocumClusterMbpsWarning)	Risiko	Cluster	Warnung
Dynamischer Cluster-Schwellenwert überschritten (ocumClusterDynamicEventWarning)	Risiko	Cluster	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
AutoSupport HTTPS-Transport deaktiviert (ocumClusterASUPHttpsConfiguredDisabled)	Risiko	Cluster	Warnung
Protokollweiterleitung nicht verschlüsselt (ocumClusterAuditLogUnencrypted)	Risiko	Cluster	Warnung
Standardmäßiger lokaler 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
Ziele für die Protokollweiterleitung geändert (ocumLogForwardDestinationsChanged)	Risiko	Cluster	Warnung
NTP-Servernamen geändert (ocumNtpServerNamesChanged)	Risiko	Cluster	Warnung
Die Anzahl der NTP-Server ist niedrig (securityConfigNTPServerCountLowRisk)	Risiko	Cluster	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Cluster-Peer-Kommunikation nicht verschlüsselt (ocumClusterPeerEncryptionDisabled)	Risiko	Cluster	Warnung
SSH verwendet unsichere Chiffren (ocumClusterSSHInsecure)	Risiko	Cluster	Warnung
Telnet-Protokoll aktiviert (ocumClusterTelnetEnabled)	Risiko	Cluster	Warnung
Passwörter einiger ONTAP Benutzerkonten verwenden die weniger sichere MD5-Hash-Funktion (ocumClusterMD5PasswordHashUsed).	Risiko	Cluster	Warnung
Cluster verwendet selbstsigniertes Zertifikat (ocumClusterSelfSignedCertificate)	Risiko	Cluster	Warnung
Cluster-Remote-Shell ist aktiviert (ocumClusterRshDisabled)	Risiko	Cluster	Warnung
Cluster-Zertifikat läuft bald ab (ocumEvtClusterCertificateAboutToExpire)	Risiko	Cluster	Warnung
Cluster-Zertifikat abgelaufen (ocumEvtClusterCertificateExpired)	Risiko	Cluster	Fehler

Datenträgerereignisse

Datenträgerereignisse liefern Ihnen Informationen zum Status von Datenträgern, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach

Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Flash-Festplatten – Ersatzblöcke fast aufgebraucht (ocumEvtClusterFlashDiskFewerSpareBlockError)	Risiko	Cluster	Fehler
Flash-Disks – Keine Ersatzblöcke (ocumEvtClusterFlashDiskNoSpareBlockCritical)	Vorfall	Cluster	Kritisch
Einige nicht zugewiesene Datenträger (ocumEvtClusterUnassignedDisksSome)	Risiko	Cluster	Warnung
Einige ausgefallene Datenträger (ocumEvtDisksSomeFailed)	Vorfall	Cluster	Kritisch

Anlagen Veranstaltungen

Gehäuseereignisse liefern Ihnen Informationen zum Status der Festplattengehäuse in Ihrem Rechenzentrum, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Festplatten-Shelf-Lüfter ausgefallen (ocumEvtShelfFanFailed)	Vorfall	Ablageboden	Kritisch
Ausfall der Stromversorgung des Festplattenregals (ocumEvtShelfPowerSupplyFailed)	Vorfall	Ablageboden	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	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
Disk Shelf-Pfadfehler (ocumDiskShelfConnectivityPathFailure)	Risiko	Lagerregal	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Disk Shelf erkannt (Nicht zutreffend)	Ereignis	Node	Information
Festplattenregale entfernt (nicht zutreffend)	Ereignis	Node	Information

Fan-Events

Lüfterereignisse liefern Ihnen Informationen zum Status der Lüfter auf Knoten in Ihrem Rechenzentrum, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Ein oder mehrere ausgefallene Lüfter (ocumEvtFansOneOrMoreFailed)	Vorfall	Node	Kritisch

Flashkartenereignisse

Flashkartenereignisse liefern Ihnen Informationen zum Status der auf den Knoten in Ihrem Rechenzentrum installierten Flashkarten, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Karteikarten offline (ocumEvtFlashCardOffline)	Vorfall	Node	Kritisch

Inodes-Ereignisse

Inode-Ereignisse liefern Informationen, wenn der Inode voll oder fast voll ist, sodass Sie ihn auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Inodes fast voll (ocumEvtInodesAlmostFull)	Risiko	Volumen	Warnung
Inodes voll (ocumEvtInodesFull)	Risiko	Volumen	Fehler

Netzwerkschnittstellenereignisse (LIF)

Netzwerkschnittstellenereignisse liefern Informationen zum Status Ihrer Netzwerkschnittstelle (LIFs), sodass Sie diese auf potenzielle Probleme überwachen

können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Netzwerkschnittstellenstatus „Down“ (ocumEvtLifStatusDown)	Risiko	Schnittstelle	Fehler
FC/FCoE-Netzwerkschnittstellenstatus „Down“ (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)	Auswirkungsstufe	Quellentyp	Schwere
Netzwerkschnittstellenroute nicht konfiguriert (Nicht zutreffend)	Ereignis	Schnittstelle	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für Netzwerkschnittstelle MB/s überschritten (ocumNetworkLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Warnschwelle für Netzwerkschnittstelle in MB/s überschritten (ocumNetworkLifMbpsWarning)	Risiko	Schnittstelle	Warnung
Kritischer Schwellenwert für FC-Netzwerkschnittstelle MB/s überschritten (ocumFcpLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
Warnschwelle für FC-Netzwerkschnittstelle (MB/s) überschritten (ocumFcpLifMbpsWarning)	Risiko	Schnittstelle	Warnung
NVMf FC-Netzwerkschnittstelle MB/s kritischer Schwellenwert überschritten (ocumNvmfFcLifMbpsIncident)	Vorfall	Schnittstelle	Kritisch
NVMf FC-Netzwerkschnittstelle MB/s-Warnschwelle überschritten (ocumNvmfFcLifMbpsWarning)	Risiko	Schnittstelle	Warnung

LUN-Ereignisse

LUN-Ereignisse liefern Ihnen Informationen zum Status Ihrer LUNs, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
LUN offline (ocumEvtLunOffline)	Vorfall	LUN	Kritisch
LUN zerstört *(lunDestroy)	Ereignis	LUN	Information
LUN mit nicht unterstütztem Betriebssystem in igroup (igroupUnsupportedOsType) zugeordnet	Vorfall	LUN	Warnung
Einzelner aktiver Pfad zum Zugriff auf LUN (ocumEvtLunSingleActivePath)	Risiko	LUN	Warnung
Keine aktiven Pfade zum Zugriff auf LUN (ocumEvtLunNotReachable)	Vorfall	LUN	Kritisch
Keine optimierten Pfade für den Zugriff auf LUN (ocumEvtLunOptimizedPathInactive)	Risiko	LUN	Warnung
Keine Pfade für den Zugriff auf LUN vom HA-Partner (ocumEvtLunHaPathInactive)	Risiko	LUN	Warnung
Kein Pfad zum Zugriff auf LUN von einem Knoten im HA-Paar (ocumEvtLunNodePathStatusDown)	Risiko	LUN	Fehler

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Nicht genügend Speicherplatz für LUN-Snapshot-Kopie (ocumEvtLunSnapshotNotPossible)	Risiko	Volumen	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
LUN mit nicht unterstütztem Betriebssystem in igroup (igroupUnsupportedOsType) zugeordnet	Risiko	LUN	Warnung

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer LUN-IOPS-Schwellenwert überschritten (ocumLunIopsIncident)	Vorfall	LUN	Kritisch
LUN-IOPS-Warnschwelle überschritten (ocumLunIopsWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN MB/s überschritten (ocumLunMbpsIncident)	Vorfall	LUN	Kritisch
LUN-MB/s-Warnschwelle überschritten (ocumLunMbpsWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz ms/op überschritten (ocumLunLatencyIncident)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
LUN-Latenz ms/op-Warnschwelle überschritten (ocumLunLatencyWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und IOPS überschritten (ocumLunLatencyIopsIncident)	Vorfall	LUN	Kritisch
Schwellenwert für LUN-Latenz und IOPS-Warnung 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
Kritischer Schwellenwert für LUN-Latenz und genutzte Gesamtleistungskapazität überschritten (ocumLunLatencyAggregatePerfCapacityUsedIncident)	Vorfall	LUN	Kritisch
Warnschwelle für LUN-Latenz und genutzte Gesamtleistungskapazität überschritten (ocumLunLatencyAggregatePerfCapacityUsedWarning)	Risiko	LUN	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für LUN-Latenz und Gesamtauslastung überschritten (ocumLunLatencyAggregateUtilizationIncident)	Vorfall	LUN	Kritisch
Warnschwelle für LUN-Latenz und Gesamtauslastung überschritten (ocumLunLatencyAggregateUtilizationWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und genutzte Knotenleistungskapazität überschritten (ocumLunLatencyNodePerfCapacityUsedIncident)	Vorfall	LUN	Kritisch
Warnschwelle für LUN-Latenz und Knotenleistung bei genutzter Kapazität überschritten (ocumLunLatencyNodePerfCapacityUsedWarning)	Risiko	LUN	Warnung
Verwendete LUN-Latenz und Knotenleistungskapazität – kritischer Übernahmeschwellenwert überschritten (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Vorfall	LUN	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Verwendete LUN-Latenz und Knotenleistungskapazität – Schwellenwert für Übernahmewarnung überschritten (ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risiko	LUN	Warnung
Kritischer Schwellenwert für LUN-Latenz und Knotenauslastung überschritten (ocumLunLatencyNodeUtilizationIncident)	Vorfall	LUN	Kritisch
Warnschwelle für LUN-Latenz und Knotenauslastung überschritten (ocumLunLatencyNodeUtilizationWarning)	Risiko	LUN	Warnung
Warnschwelle für maximale IOPS von QoS LUN überschritten (ocumQosLunMaxIopsWarning)	Risiko	LUN	Warnung
QoS LUN Max MB/s-Warnschwelle überschritten (ocumQosLunMaxMbpsWarning)	Risiko	LUN	Warnung
Der Latenzschwellenwert der Workload-LUN wurde gemäß der Leistungs-Servicelevel-Richtlinie überschritten (ocumConformanceLatencyWarning).	Risiko	LUN	Warnung

Ereignisse der Verwaltungsstation

Ereignisse der Verwaltungsstation liefern Ihnen Informationen zum Status des Servers, auf dem Unified Manager installiert ist, sodass Sie ihn auf potenzielle Probleme

überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Speicherplatz des Verwaltungsservers fast voll (ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Risiko	Verwaltungsstation	Warnung
Verwaltungsserver-Festplattenspeicher voll (ocumEvtUnifiedManagerDiskSpaceFull)	Vorfall	Verwaltungsstation	Kritisch
Wenig Arbeitsspeicher auf dem Verwaltungsserver (ocumEvtUnifiedManagerMemoryLow)	Risiko	Verwaltungsstation	Warnung
Verwaltungsserver hat fast keinen Speicher mehr (ocumEvtUnifiedManagerMemoryAlmostOut)	Vorfall	Verwaltungsstation	Kritisch
Größe der MySQL-Protokolldatei erhöht; Neustart erforderlich (ocumEvtMysqlLogFileSizeWarning)	Vorfall	Verwaltungsstation	Warnung
Die Gesamtzuweisungsgröße für das Überwachungsprotokoll ist fast erschöpft	Risiko	Verwaltungsstation	Warnung
Syslog-Server-Zertifikat läuft bald ab	Risiko	Verwaltungsstation	Warnung
Syslog-Server-Zertifikat abgelaufen	Risiko	Verwaltungsstation	Fehler
Audit-Protokolldatei manipuliert	Risiko	Verwaltungsstation	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Audit-Protokolldatei gelöscht	Risiko	Verwaltungsstation	Warnung
Syslog-Server-Verbindungsfehler	Risiko	Verwaltungsstation	Fehler
Syslog-Serverkonfiguration geändert	Ereignis	Verwaltungsstation	Warnung

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Die Analyse der Leistungsdaten ist beeinträchtigt (ocumEvtUnifiedManagerDataMissingAnalyze)	Risiko	Verwaltungsstation	Warnung
Die Leistungsdatenerfassung ist beeinträchtigt (ocumEvtUnifiedManagerDataMissingCollection)	Vorfall	Verwaltungsstation	Kritisch

Diese letzten beiden Leistungsereignisse waren nur für Unified Manager 7.2 verfügbar. Wenn eines dieser Ereignisse im Status „Neu“ vorhanden ist und Sie dann 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.

MetroCluster Bridge-Ereignisse

MetroCluster Bridge-Ereignisse liefern Ihnen Informationen zum Status der Bridges, sodass Sie potenzielle Probleme in einer MetroCluster über-FC-Konfiguration überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Brücke nicht erreichbar (ocumEvtBridgeUnreachable)	Vorfall	MetroCluster Brücke	Kritisch
Brückentemperatur anormal (ocumEvtBridgeTemperatureAbnormal)	Vorfall	MetroCluster Brücke	Kritisch

MetroCluster -Konnektivitätsereignisse

Konnektivitätsereignisse liefern Ihnen Informationen zur Konnektivität zwischen den Komponenten eines Clusters und zwischen Clustern in MetroCluster over FC- und MetroCluster over IP-Konfigurationen, sodass Sie potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

In beiden Konfigurationen gemeinsame Ereignisse

Diese Konnektivitätsereignisse sind sowohl für MetroCluster über FC- als auch für MetroCluster über IP-Konfigurationen üblich.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Alle Links zwischen MetroCluster Partnern ausgefallen (ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Vorfall	MetroCluster -Beziehung	Kritisch
MetroCluster Partner über Peering-Netzwerk nicht erreichbar (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Vorfall	MetroCluster -Beziehung	Kritisch
MetroCluster Disaster-Recovery-Funktion beeinträchtigt (ocumEvtMetroClusterDRStatusImpacted)	Risiko	MetroCluster -Beziehung	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
MetroCluster -Konfiguration umgeschaltet (ocumEvtMetroClusterDRStatusImpacted)	Risiko	MetroCluster -Beziehung	Warnung

MetroCluster über FC-Konfiguration

Diese Ereignisse beziehen sich auf MetroCluster über FC-Konfigurationen.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Alle Inter-Switch-Verbindungen ausgefallen (ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Vorfall	MetroCluster Inter-Switch-Verbindung	Kritisch
FC-SAS-Bridge zum Speicherstapel-Link Down (ocumEvtBridgeSasPortDown)	Vorfall	MetroCluster Bridge-Stack-Verbindung	Kritisch
MetroCluster -Konfiguration teilweise umgeschaltet (ocumEvtMetroClusterDRStatusPartiallyImpacted)	Risiko	MetroCluster -Beziehung	Fehler
Knoten zum FC-Switch: Alle FC-VI-Verbindungsverbindungen unterbrochen (ocumEvtMccNodeSwitchFcviLinksDown)	Vorfall	MetroCluster -Knoten -Switch-Verbindung	Kritisch
Knoten zum FC-Switch: Eine oder mehrere FC-Initiator-Verbindungen ausgefallen (ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Risiko	MetroCluster -Knoten -Switch-Verbindung	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Knoten zum FC-Switch: Alle FC-Initiator-Verbindungen unterbrochen (ocumEvtMccNodeSwitchFcLinksDown)	Vorfall	MetroCluster -Knoten -Switch-Verbindung	Kritisch
Wechseln Sie zur FC-SAS-Bridge. FC-Link ausgefallen (ocumEvtMccSwitchBridgeFcLinksDown)	Vorfall	MetroCluster -Switch -Bridge-Verbindung	Kritisch
Zwischen Knoten: Alle FC VI-InterConnect-Verbindungen ausgefallen (ocumEvtMccInterNodeLinksDown)	Vorfall	Verbindung zwischen Knoten	Kritisch
Zwischen Knoten: Eine oder mehrere FC VI-InterConnect-Verbindungen ausgefallen (ocumEvtMccInterNodeLinksOneOrMoreDown)	Risiko	Verbindung zwischen Knoten	Warnung
Knoten zur Bridge-Verbindung unterbrochen (ocumEvtMccNodeBridgeLinksDown)	Vorfall	Knotenbrückenverbindung	Kritisch
Knoten zum Speicherstapel: Alle SAS-Verbindungen unterbrochen (ocumEvtMccNodeStackLinksDown)	Vorfall	Knotenstapelverbindung	Kritisch
Knoten zum Speicherstapel: Eine oder mehrere SAS-Verbindungen unterbrochen (ocumEvtMccNodeStackLinksOneOrMoreDown)	Risiko	Knotenstapelverbindung	Warnung

MetroCluster über IP-Konfiguration

Diese Ereignisse beziehen sich auf MetroCluster -over-IP-Konfigurationen.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Der Status der IP-Verbindung zwischen den Standorten von MetroCluster ist deaktiviert (mccIntersiteconnectivityStatusDown).	Risiko	MetroCluster -Beziehung	Kritisch
MetroCluster– IP-Knoten zum Offline-Schalten der Verbindung (mccIpPortStatusOffline)	Risiko	Node	Fehler

MetroCluster -Switch-Ereignisse

MetroCluster Switch-Ereignisse für MetroCluster über FC-Konfigurationen liefern Ihnen Informationen zum Status der MetroCluster -Switches, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Schaltertemperatur abnormal (ocumEvtSwitchTemperatureAbnormal)	Vorfall	MetroCluster Switch	Kritisch
Switch nicht erreichbar (ocumEvtSwitchUnreachable)	Vorfall	MetroCluster Switch	Kritisch
Lüfterschalter ausgefallen (ocumEvtSwitchFansOneOrMoreFailed)	Vorfall	MetroCluster Switch	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Fehler bei der Stromversorgung des Switches (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Vorfall	MetroCluster Switch	Kritisch
Schaltertemperatursensoren ausgefallen (ocumEvtSwitchTemperatureSensorFailed) Dieses Ereignis gilt nur für Cisco -Switches.	Vorfall	MetroCluster Switch	Kritisch

NVMe-Namespace-Ereignisse

NVMe-Namespace-Ereignisse liefern Ihnen Informationen zum Status Ihrer Namespaces, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
NVMeNS Offline *(nvmeNamespaceStatusOffline)	Ereignis	Namensraum	Information
NVMeNS Online *(nvmeNamespaceStatusOnline)	Ereignis	Namensraum	Information
Nicht genügend Speicherplatz für NVMeNS *(nvmeNamespaceSpaceOutOfSpace)	Risiko	Namensraum	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
NVMeNS zerstören *(nvmeNamespaceDestroy)	Ereignis	Namensraum	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer IOPS-Schwellenwert für NVMe-Namespace überschritten (ocumNvmeNamespaceIopsIncident)	Vorfall	Namensraum	Kritisch
NVMe-Namespace-IOPS-Warnschwelle überschritten (ocumNvmeNamespaceIopsWarning)	Risiko	Namensraum	Warnung
Kritischer Schwellenwert für NVMe-Namespace MB/s überschritten (ocumNvmeNamespaceMbpsIncident)	Vorfall	Namensraum	Kritisch
NVMe-Namespace MB/s-Warnschwelle überschritten (ocumNvmeNamespaceMbpsWarning)	Risiko	Namensraum	Warnung
NVMe-Namespace-Latenz ms/op – kritischer Schwellenwert überschritten (ocumNvmeNamespaceLatencyIncident)	Vorfall	Namensraum	Kritisch
NVMe-Namespace-Latenz-ms/op-Warnschwelle überschritten (ocumNvmeNamespaceLatencyWarning)	Risiko	Namensraum	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	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
NVMe-Namespace-Latenz und kritischer MB/s-Schwellenwert überschritten (ocumNvmeNamespaceLatencyMbpsIncident)	Vorfall	Namensraum	Kritisch
NVMe-Namespace-Latenz und MB/s-Warnschwelle überschritten (ocumNvmeNamespaceLatencyMbpsWarning)	Risiko	Namensraum	Warnung

Knotenereignisse

Knotenereignisse liefern Ihnen Informationen zum Knotenstatus, sodass Sie potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Speicherplatz des Knotenstammvolumes fast voll (ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Risiko	Node	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Cloud AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	Risiko	Node	Fehler
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	Information
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

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Einer der NFSv4-Pools erschöpft *(nbladeNfsv4PoolEXhaust)	Vorfall	Node	Kritisch
Anforderung stimmt nicht mit Cloud-Tier-Signatur überein *(oscSignatureMismatch)	Risiko	Node	Fehler

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
QoS-Monitor-Speicher maximal *(ocumQosMonitorMemoryMaxed)	Risiko	Node	Fehler
QoS-Monitor-Speicher verringert *(ocumQosMonitorMemoryAbated)	Ereignis	Node	Information

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Knoten umbenannt (Nicht zutreffend)	Ereignis	Node	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Knoten-IOPS-Schwellenwert überschritten (ocumNodeIopsIncident)	Vorfall	Node	Kritisch
Knoten-IOPS-Warnschwelle überschritten (ocumNodeIopsWarning)	Risiko	Node	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Knoten-MB/s-Schwellenwert überschritten (ocumNodeMbpsIncident)	Vorfall	Node	Kritisch
Knoten-MB/s-Warnschwelle überschritten (ocumNodeMbpsWarning)	Risiko	Node	Warnung
Knotenlatenz ms/op – kritischer Schwellenwert überschritten (ocumNodeLatencyIncident)	Vorfall	Node	Kritisch
Knotenlatenz ms/op-Warnschwelle überschritten (ocumNodeLatencyWarning)	Risiko	Node	Warnung
Kritischer Schwellenwert für genutzte Knotenleistungskapazität überschritten (ocumNodePerfCapacityUsedIncident)	Vorfall	Node	Kritisch
Warnschwelle für genutzte Knotenleistungskapazität überschritten (ocumNodePerfCapacityUsedWarning)	Risiko	Node	Warnung
Ausgenutzte Knotenleistungskapazität – kritischer Übernahmeschwellenwert überschritten (ocumNodePerfCapacityUsedTakeoverIncident)	Vorfall	Node	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Ausgenutzte Knotenleistungskapazität – Schwellenwert für Übernahmewarnung überschritten (ocumNodePerfCapacityUsedTakeoverWarning)	Risiko	Node	Warnung
Kritischer Schwellenwert für Knotenauslastung überschritten (ocumNodeUtilizationIncident)	Vorfall	Node	Kritisch
Warnschwelle für Knotenauslastung überschritten (ocumNodeUtilizationWarning)	Risiko	Node	Warnung
Schwellenwert für überbeanspruchtes Knoten-HA-Paar überschritten (ocumNodeHaPairOverUtilizedInformation)	Ereignis	Node	Information
Schwellenwert für die Fragmentierung der Knotenfestplatte überschritten (ocumNodeDiskFragmentationWarning)	Risiko	Node	Warnung
Schwellenwert für genutzte Leistungskapazität überschritten (ocumNodeOverUtilizedWarning)	Risiko	Node	Warnung
Dynamischer Knotenschwellenwert überschritten (ocumNodeDynamicEventWarning)	Risiko	Node	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Hinweis-ID: NTAP-<*advisory ID*>(ocumx)	Risiko	Node	Kritisch

NVRAM -Batterieereignisse

NVRAM Batterieereignisse liefern Ihnen Informationen zum Status Ihrer Batterien, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
NVRAM -Batterie schwach (ocumEvtNvramBatteryLow)	Risiko	Node	Warnung
NVRAM -Batterie entladen (ocumEvtNvramBatteryDischarged)	Risiko	Node	Fehler
NVRAM -Batterie überladen (ocumEvtNvramBatteryOverCharged)	Vorfall	Node	Kritisch

Hafenereignisse

Portereignisse liefern Ihnen den Status von Cluster-Ports, sodass Sie Änderungen oder Probleme am Port überwachen können, beispielsweise ob der Port ausgefallen ist.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Portstatus deaktiviert (ocumEvtPortStatusDown)	Vorfall	Node	Kritisch

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für Netzwerkport MB/s überschritten (ocumNetworkPortMbpsIncident)	Vorfall	Hafen	Kritisch
Warnschwelle für Netzwerkport MB/s überschritten (ocumNetworkPortMbpsWarning)	Risiko	Hafen	Warnung
FCP-Port MB/s kritischer Schwellenwert überschritten (ocumFcpPortMbpsIncident)	Vorfall	Hafen	Kritisch
FCP-Port MB/s-Warnschwelle überschritten (ocumFcpPortMbpsWarning)	Risiko	Hafen	Warnung
Kritischer Schwellenwert für Netzwerk-Port-Auslastung überschritten (ocumNetworkPortUtilizationIncident)	Vorfall	Hafen	Kritisch
Warnschwelle für Netzwerk-Port-Auslastung überschritten (ocumNetworkPortUtilizationWarning)	Risiko	Hafen	Warnung
Kritischer Schwellenwert für FCP-Portauslastung überschritten (ocumFcpPortUtilizationIncident)	Vorfall	Hafen	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Warnschwelle für FCP-Portauslastung überschritten (ocumFcpPortUtilizationWarning)	Risiko	Hafen	Warnung

Netzteilereignisse

Netzteilereignisse liefern Ihnen Informationen zum Status Ihrer Hardware, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Ein oder mehrere Netzteile ausgefallen (ocumEvtPowerSupplyOneOrMoreFailed)	Vorfall	Node	Kritisch

Schutzereignisse

Schutzereignisse informieren Sie darüber, ob ein Job fehlgeschlagen ist oder abgebrochen wurde, sodass Sie ihn auf Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Schutzauftrag fehlgeschlagen (ocumEvtProtectionJobTaskFailed)	Vorfall	Volumen- oder Speicherdienst	Kritisch
Schutzauftrag abgebrochen (ocumEvtProtectionJobAborted)	Risiko	Volumen- oder Speicherdienst	Warnung

Qtree-Ereignisse

Qtree-Ereignisse liefern Ihnen Informationen zur Qtree-Kapazität und den Datei- und Festplattenlimits, sodass Sie potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Qtree-Speicherplatz fast voll (ocumEvtQtreeSpaceNearlyFull)	Risiko	Qtree	Warnung
Qtree-Speicherplatz voll (ocumEvtQtreeSpaceFull)	Risiko	Qtree	Fehler
Qtree Space Normal (ocumEvtQtreeSpaceThresholdOk)	Ereignis	Qtree	Information
Qtree-Dateien-Hardlimit erreicht (ocumEvtQtreeFilesHardLimitReached)	Vorfall	Qtree	Kritisch
Qtree-Dateien Soft-Limit überschritten (ocumEvtQtreeFilesSoftLimitBreached)	Risiko	Qtree	Warnung
Qtree-Speicherplatz-Hartgrenze erreicht (ocumEvtQtreeSpaceHardLimitReached)	Vorfall	Qtree	Kritisch
Qtree Space Soft Limit überschritten (ocumEvtQtreeSpaceSoftLimitBreached)	Risiko	Qtree	Warnung

Serviceprozessorereignisse

Serviceprozessorereignisse liefern Ihnen Informationen zum Status Ihres Prozessors, sodass Sie ihn auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die

Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Serviceprozessor nicht konfiguriert (ocumEvtServiceProcessorNotConfigured)	Risiko	Node	Warnung
Serviceprozessor offline (ocumEvtServiceProcessorOffline)	Risiko	Node	Fehler

SnapMirror -Beziehungsereignisse

SnapMirror Beziehungsereignisse liefern Ihnen Informationen zum Status Ihrer asynchronen und synchronen SnapMirror Beziehungen, sodass Sie diese auf potenzielle Probleme überwachen können. Asynchrone SnapMirror Beziehungsereignisse werden sowohl für Storage-VMs als auch für Volumes generiert, synchrone SnapMirror -Beziehungsereignisse werden jedoch nur für Volume-Beziehungen generiert. Für Bestandteilvolumes, die Teil von Storage-VM-Notfallwiederherstellungsbeziehungen sind, werden keine Ereignisse generiert. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Aufprallbereich: Schutz

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Die SnapMirror -Beziehungsereignisse werden für Storage-VMs generiert, die durch die Notfallwiederherstellung von Storage-VMs geschützt sind, jedoch nicht für Beziehungen zwischen Bestandteilobjekten.

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Spiegelreplikation fehlerhaft (ocumEvtSnapmirrorRelationshipUnhealthy)	Risiko	SnapMirror -Beziehung	Warnung
Abgebrochene Spiegelreplikation (ocumEvtSnapmirrorRelationshipStateBrokenoff)	Risiko	SnapMirror -Beziehung	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Initialisierung der Spiegelreplikation fehlgeschlagen (ocumEvtSnapmirrorRelationshipInitializeFailed)	Risiko	SnapMirror -Beziehung	Fehler
Aktualisierung der Spiegelreplikation fehlgeschlagen (ocumEvtSnapmirrorRelationshipUpdateFailed)	Risiko	SnapMirror -Beziehung	Fehler
Verzögerungsfehler bei der Spiegelreplikation (ocumEvtSnapMirrorRelationshipLagError)	Risiko	SnapMirror -Beziehung	Fehler
Warnung bei Verzögerung bei Spiegelreplikation (ocumEvtSnapMirrorRelationshipLagWarning)	Risiko	SnapMirror -Beziehung	Warnung
Neusynchronisierung der Spiegelreplikation fehlgeschlagen (ocumEvtSnapmirrorRelationshipResyncFailed)	Risiko	SnapMirror -Beziehung	Fehler
Synchrone Replikation nicht synchron *(syncSnapmirrorRelationshipOutofsync)	Risiko	SnapMirror -Beziehung	Warnung
Synchrone Replikation wiederhergestellt *(syncSnapmirrorRelationshipInSync)	Ereignis	SnapMirror -Beziehung	Information
Automatische Neusynchronisierung der synchronen Replikation fehlgeschlagen *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Risiko	SnapMirror -Beziehung	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Ontap Mediator wird zum Cluster hinzugefügt (snapmirrorMediatorAdded)	Ereignis	Cluster	Information
Ontap Mediator wird aus dem Cluster entfernt (snapmirrorMediatorRemoved)	Ereignis	Cluster	Information
Ontap Mediator ist vom Cluster aus nicht erreichbar (snapmirrorMediatorUnreachable)	Risiko	Vermittler	Warnung
Auf Ontap Mediator kann vom Cluster aus nicht zugegriffen werden (SnapmirrorMediator falsch konfiguriert).	Risiko	Vermittler	Fehler
Die Ontap Mediator-Konnektivität wurde wiederhergestellt, ist neu synchronisiert und bereit für die aktive Synchronisierung mit SnapMirror (snapmirrorMediatorInQuorum).	Ereignis	Vermittler	Information

Asynchrone Mirror- und Vault-Beziehungsereignisse

Ereignisse für asynchrone Mirror- und Vault-Beziehungen liefern Ihnen Informationen zum Status Ihrer asynchronen SnapMirror und Vault-Beziehungen, sodass Sie diese auf potenzielle Probleme überwachen können. Asynchrone Spiegel- und Vault-Beziehungsereignisse werden sowohl für Volume- als auch für Storage-VM-Schutzbeziehungen unterstützt. Für die Notfallwiederherstellung von Storage-VMs werden jedoch nur Vault-Beziehungen nicht unterstützt. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Aufprallbereich: Schutz

Die SnapMirror und Vault-Beziehungsereignisse werden auch für Storage-VMs generiert, die durch die Notfallwiederherstellung von Storage-VMs geschützt sind, jedoch nicht für Beziehungen zwischen Bestandteilobjekten.

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Asynchroner Spiegel und Tresor fehlerhaft (ocumEvtMirrorVaultRelationshipUnhealthy)	Risiko	SnapMirror -Beziehung	Warnung
Asynchroner Spiegel und Tresor abgebrochen (ocumEvtMirrorVaultRelationshipStateBrokenoff)	Risiko	SnapMirror -Beziehung	Fehler
Asynchrone Spiegelung und Vault-Initialisierung fehlgeschlagen (ocumEvtMirrorVaultRelationshipInitializeFailed)	Risiko	SnapMirror -Beziehung	Fehler
Asynchrone Spiegel- und Vault-Aktualisierung fehlgeschlagen (ocumEvtMirrorVaultRelationshipUpdateFailed)	Risiko	SnapMirror -Beziehung	Fehler
Asynchroner Mirror- und Vault-Lag-Fehler (ocumEvtMirrorVaultRelationshipLagError)	Risiko	SnapMirror -Beziehung	Fehler
Asynchrone Spiegel- und Vault-Verzögerungswarnung (ocumEvtMirrorVaultRelationshipLagWarning)	Risiko	SnapMirror -Beziehung	Warnung
Asynchrone Spiegelung und Vault-Neusynchronisierung fehlgeschlagen (ocumEvtMirrorVaultRelationshipResyncFailed)	Risiko	SnapMirror -Beziehung	Fehler

Das Ereignis „SnapMirror -Updatefehler“ wird vom Active IQ Portal (Config Advisor) ausgelöst.

Snapshot-Ereignisse

Snapshot-Ereignisse liefern Informationen zum Status von Snapshots, sodass Sie die Snapshots auf potenzielle Probleme überwachen können. Die Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignisnamen, den Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Automatisches Löschen von Snapshots deaktiviert (nicht zutreffend)	Ereignis	Volumen	Information
Automatisches Löschen von Snapshots aktiviert (nicht zutreffend)	Ereignis	Volumen	Information
Snapshot-Konfiguration automatisch löschen, geändert (nicht zutreffend)	Ereignis	Volumen	Information

SnapVault -Beziehungsereignisse

SnapVault Beziehungsereignisse liefern Ihnen Informationen zum Status Ihrer SnapVault -Beziehungen, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Asynchroner Tresor fehlerhaft (ocumEvtSnapVaultRelationshipUnhealthy)	Risiko	SnapMirror -Beziehung	Warnung
Asynchroner Tresor abgebrochen (ocumEvtSnapVaultRelationshipStateBrokenoff)	Risiko	SnapMirror -Beziehung	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Asynchrone Vault-Initialisierung fehlgeschlagen (ocumEvtSnapVaultRelationshipInitializeFailed)	Risiko	SnapMirror -Beziehung	Fehler
Asynchrone Vault-Aktualisierung fehlgeschlagen (ocumEvtSnapVaultRelationshipUpdateFailed)	Risiko	SnapMirror -Beziehung	Fehler
Asynchroner Vault-Lag-Fehler (ocumEvtSnapVaultRelationshipLagError)	Risiko	SnapMirror -Beziehung	Fehler
Asynchrone Vault-Verzögerungswarnung (ocumEvtSnapVaultRelationshipLagWarning)	Risiko	SnapMirror -Beziehung	Warnung
Asynchrone Vault-Neusynchronisierung fehlgeschlagen (ocumEvtSnapvaultRelationshipResyncFailed)	Risiko	SnapMirror -Beziehung	Fehler

Ereignisse der Speicherfailovereinstellungen

Ereignisse der Speicherfailover-Einstellungen (SFO) liefern Ihnen Informationen darüber, ob Ihr Speicherfailover deaktiviert oder nicht konfiguriert ist, sodass Sie es auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Speicher-Failover-Verbindung: Eine oder mehrere Verbindungen sind ausgefallen (ocumEvtSfoInterconnectOneOrMoreLinksDown)	Risiko	Node	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Speicherfailover deaktiviert (ocumEvtSfoSettingsDisabled)	Risiko	Node	Fehler
Speicherfailover nicht konfiguriert (ocumEvtSfoSettingsNotConfigured)	Risiko	Node	Fehler
Speicher-Failover-Status – Übernahme (ocumEvtSfoStateTakeover)	Risiko	Node	Warnung
Speicherfailoverstatus – teilweise Rückgabe (ocumEvtSfoStatePartialGiveback)	Risiko	Node	Fehler
Speicher-Failover-Knotenstatus „Down“ (ocumEvtSfoNodeStatusDown)	Risiko	Node	Fehler
Speicher-Failover-Übernahme nicht möglich (ocumEvtSfoTakeoverNotPossible)	Risiko	Node	Fehler

Speicherdienstereignisse

Speicherdienstereignisse liefern Ihnen Informationen zur Erstellung und zum Abonnement von Speicherdiensten, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Speicherdienst erstellt (Nicht zutreffend)	Ereignis	Lagerservice	Information

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Abonnierter Speicherdienst (Nicht zutreffend)	Ereignis	Lagerservice	Information
Speicherdienst abgemeldet (Nicht zutreffend)	Ereignis	Lagerservice	Information

Aufprallbereich: Schutz

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Unerwartete Löschung der verwalteten SnapMirror -BeziehungocumEvtStorageServiceUnsupportedRelationshipDeletion	Risiko	Lagerservice	Warnung
Unerwartete Löschung des Storage Service Member Volumes (ocumEvtStorageServiceUnexpectedVolumeDeletion)	Vorfall	Lagerservice	Kritisch

Lagerregalereignisse

Durch Speicherregalereignisse werden Sie über ungewöhnliche Zustände Ihres Speicherregals informiert, sodass Sie es auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Abnormaler Spannungsbereich (ocumEvtShelfVoltageAbnormal)	Risiko	Ablageboden	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Abnormaler Strombereich (ocumEvtShelfCurrentAbnormal)	Risiko	Ablageboden	Warnung
Abnormale Temperatur (ocumEvtShelfTemperatureAbnormal)	Risiko	Ablageboden	Warnung

Speicher-VM-Ereignisse

Storage-VM-Ereignisse (Storage Virtual Machine, auch als SVM bezeichnet) liefern Ihnen Informationen zum Status Ihrer Storage-VMs (SVMs), sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
CIFS-Dienst der Speicher-VM ausgefallen (ocumEvtVserverCifsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM CIFS-Dienst nicht konfiguriert (Nicht zutreffend)	Ereignis	SVM	Information
Versuche, eine Verbindung zu einer nicht vorhandenen CIFS-Freigabe herzustellen *(nbladeCifsNoPrivShare)	Vorfall	SVM	Kritisch
CIFS-NetBIOS-Namenskonflikt *(nbladeCifsNbNameConflict)	Risiko	SVM	Fehler
CIFS-Schattenkopie-Vorgang fehlgeschlagen *(cifsShadowCopyFailure)	Risiko	SVM	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Viele CIFS-Verbindungen *(nbladeCifsManyAuths)	Risiko	SVM	Fehler
Maximale CIFS-Verbindung überschritten *(nbladeCifsMaxOpenSameFile)	Risiko	SVM	Fehler
Maximale Anzahl von CIFS-Verbindungen pro Benutzer überschritten *(nbladeCifsMaxSessPerUsrConn)	Risiko	SVM	Fehler
SVM FC/FCoE-Dienst ausgefallen (ocumEvtVserverFcServiceStatusDown)	Vorfall	SVM	Kritisch
SVM-iSCSI-Dienst ausgefallen (ocumEvtVserverIscsiServiceStatusDown)	Vorfall	SVM	Kritisch
NFS-Dienst der Speicher-VM ausgefallen (ocumEvtVserverNfsServiceStatusDown)	Vorfall	SVM	Kritisch
SVM FC/FCoE-Dienst nicht konfiguriert (Nicht zutreffend)	Ereignis	SVM	Information
SVM-iSCSI-Dienst nicht konfiguriert (Nicht zutreffend)	Ereignis	SVM	Information
SVM NFS-Dienst nicht konfiguriert (Nicht zutreffend)	Ereignis	SVM	Information
Speicher-VM gestoppt (ocumEvtVserverDown)	Risiko	SVM	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
AV-Server zu beschäftigt, um neue Scan-Anforderung anzunehmen *(nbladeVscanConnBackPressure)	Risiko	SVM	Fehler
Keine AV-Serververbindung für Virenscan *(nbladeVscanNoScannerConn)	Vorfall	SVM	Kritisch
Kein AV-Server registriert *(nbladeVscanNoRegdScanner)	Risiko	SVM	Fehler
Keine reagierende AV-Serververbindung *(nbladeVscanConnInactive)	Ereignis	SVM	Information
Versuch eines nicht autorisierten Benutzers, den AV-Server zu beschädigen *(nbladeVscanBadUserPrivAccess)	Risiko	SVM	Fehler
Virus vom AV-Server gefunden *(nbladeVscanVirusDetected)	Risiko	SVM	Fehler

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
SVM erkannt (Nicht zutreffend)	Ereignis	SVM	Information
SVM gelöscht (Nicht zutreffend)	Ereignis	Cluster	Information
SVM umbenannt (Nicht zutreffend)	Ereignis	SVM	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer SVM-IOPS-Schwellenwert überschritten (ocumSvmIopsIncident)	Vorfall	SVM	Kritisch
SVM-IOPS-Warnschwelle überschritten (ocumSvmIopsWarning)	Risiko	SVM	Warnung
Kritischer Schwellenwert für SVM MB/s 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-Latenzwarnschwelle überschritten (ocumSvmLatencyWarning)	Risiko	SVM	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Überwachungsprotokoll deaktiviert (ocumVserverAuditLogDisabled)	Risiko	SVM	Warnung
Anmeldebanner deaktiviert (ocumVserverLoginBannerDisabled)	Risiko	SVM	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
SSH verwendet unsichere Chiffren (ocumVserverSSHInsecure)	Risiko	SVM	Warnung
Anmeldebanner geändert (ocumVserverLoginBannerChanged)	Risiko	SVM	Warnung
Die Anti-Ransomware-Überwachung der Storage-VM ist deaktiviert (antiRansomwareSvmStateDisabled).	Risiko	SVM	Warnung
Die Anti-Ransomware-Überwachung der Storage-VM ist aktiviert (Lernmodus) (antiRansomwareSvmStateDryrun)	Ereignis	SVM	Information
Für die Anti-Ransomware-Überwachung geeignete Speicher-VM (Lernmodus) (ocumEvtSvmArwCandidate)	Ereignis	SVM	Information

Benutzer- und Gruppenkontingentereignisse

Benutzer- und Gruppenkontingentereignisse liefern Ihnen Informationen zur Kapazität des Benutzer- und Benutzergruppenkontingents sowie zu den Datei- und Datenträgerlimits, sodass Sie potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Soft-Limit für Benutzer- oder Gruppenkontingentspeicherplatz überschritten (ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Risiko	Benutzer- oder Gruppenkontingent	Warnung
Hartes Speicherplatzlimit für Benutzer- oder Gruppenkontingente erreicht (ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingent	Kritisch
Soft-Limit für die Anzahl der Dateien im Benutzer- oder Gruppenkontingent überschritten (ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Risiko	Benutzer- oder Gruppenkontingent	Warnung
Festes Limit für die Anzahl der Dateien im Benutzer- oder Gruppenkontingent erreicht (ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Vorfall	Benutzer- oder Gruppenkontingent	Kritisch

Volumenereignisse

Volume-Ereignisse liefern Informationen zum Status von Volumes, sodass Sie diese auf potenzielle Probleme überwachen können. Die Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignisnamen, den Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Ein Sternchen (*) kennzeichnet EMS-Ereignisse, die in Unified Manager-Ereignisse konvertiert wurden.

Wirkungsbereich: Verfügbarkeit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Volumen eingeschränkt (ocumEvtVolumeRestricted)	Risiko	Volumen	Warnung
Volume offline (ocumEvtVolumeOffline)	Vorfall	Volumen	Kritisch
Volume teilweise verfügbar (ocumEvtVolumePartiallyAvailable)	Risiko	Volumen	Fehler
Volume nicht gemountet (Nicht zutreffend)	Ereignis	Volumen	Information
Volume gemountet (Nicht zutreffend)	Ereignis	Volumen	Information
Volume erneut bereitgestellt (Nicht zutreffend)	Ereignis	Volumen	Information
Volume-Junction-Pfad inaktiv (ocumEvtVolumeJunctionPathInactive)	Risiko	Volumen	Warnung
Automatische Volume-Größenanpassung aktiviert (Nicht zutreffend)	Ereignis	Volumen	Information
Automatische Volume-Größenanpassung deaktiviert (nicht zutreffend)	Ereignis	Volumen	Information
Automatische Volume-Größenanpassung – Maximale Kapazität geändert (Nicht zutreffend)	Ereignis	Volumen	Information
Automatische Volumengrößenerhöhung – Größe geändert (nicht zutreffend)	Ereignis	Volumen	Information

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Gefährdeter Speicherplatz auf Thin-Provisioned-Volume (ocumThinProvisionVolumeSpaceAtRisk)	Risiko	Volumen	Warnung
Fehler beim Volume-Effizienz-Vorgang (ocumEvtVolumeEfficiencyOperationError)	Risiko	Volumen	Fehler
Volume-Speicherplatz voll (ocumEvtVolumeFull)	Risiko	Volumen	Fehler
Volume-Speicherplatz fast voll (ocumEvtVolumeNearlyFull)	Risiko	Volumen	Warnung
Logischer Speicherplatz des Datenträgers voll *(volumeLogicalSpaceFull)	Risiko	Volumen	Fehler
Logischer Speicherplatz des Volumes fast voll *(volumeLogicalSpaceNearlyFull)	Risiko	Volumen	Warnung
Logischer Speicherplatz des Volumes Normal *(volumeLogicalSpaceAllOK)	Ereignis	Volumen	Information
Reservespeicherplatz für Volume-Snapshot voll (ocumEvtSnapshotFull)	Risiko	Volumen	Warnung
Zu viele Snapshot-Kopien (ocumEvtSnapshotTooMany)	Risiko	Volumen	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Volume-Qtree-Kontingent überbelegt (ocumEvtVolumeQtreeQuotaOvercommitted)	Risiko	Volumen	Fehler
Volume-Qtree-Kontingent fast überlastet (ocumEvtVolumeQtreeQuotaAlmostOvercommitted)	Risiko	Volumen	Warnung
Abnormale Volumenwachstumsrate (ocumEvtVolumeGrowthRateAbnormal)	Risiko	Volumen	Warnung
Volumen in Tagen bis zur Vollendung (ocumEvtVolumeDaysUntilFullSoon)	Risiko	Volumen	Fehler
Volume-Speicherplatzgarantie deaktiviert (nicht zutreffend)	Ereignis	Volumen	Information
Volume-Speicherplatzgarantie aktiviert (nicht zutreffend)	Ereignis	Volumen	Information
Garantie für Speicherplatz geändert (nicht zutreffend)	Ereignis	Volumen	Information
Volume-Snapshot-Reservetage bis zur Vollendung (ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Risiko	Volumen	Fehler
FlexGroup -Bestandteile haben Platzprobleme *(flexGroupConstituentsHaveSpaceIssues)	Risiko	Volumen	Fehler

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
FlexGroup -Bestandteil -Raumstatus Alle OK *(flexGroupConstituentsSpaceStatusAllOK)	Ereignis	Volumen	Information
FlexGroup -Bestandteile haben Inodes-Probleme *(flexGroupConstituentsHaveInodesIssues)	Risiko	Volumen	Fehler
FlexGroup -Bestandteile -Inodes-Status: Alle OK *(flexGroupConstituentsInodesStatusAllOK)	Ereignis	Volumen	Information
WAFL -Volume-AutoSize -Fehler *(waflVolAutoSizeFail)	Risiko	Volumen	Fehler
WAFL -Volume-AutoSize erledigt *(waflVolAutoSizeDone)	Ereignis	Volumen	Information
FlexGroup -Volumen ist zu über 80 % ausgelastet*	Vorfall	Volumen	Fehler
FlexGroup Volumen ist zu über 90 % ausgelastet*	Vorfall	Volumen	Kritisch
Anomalie der Volume-Speichereffizienz (ocumVolumeAbnormalStorageEfficiencyWarning)	Risiko	Volumen	Warnung
Volume-Snapshot-Reserve nicht ausreichend genutzt (volumeSnaphotReserveUnderutilizedWarning)	Ereignis	Volumen	Warnung
Volume-Snapshot-Reserve nicht ausreichend genutzt (volumeSnaphotReserveUnderutilizedCleared)	Ereignis	Volumen	Warnung

Wirkungsbereich: Konfiguration

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Volume umbenannt (Nicht zutreffend)	Ereignis	Volumen	Information
Erkanntes Volumen (Nicht zutreffend)	Ereignis	Volumen	Information
Volume gelöscht (Nicht zutreffend)	Ereignis	Volumen	Information

Wirkungsbereich: Leistung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Warnschwelle für maximale IOPS des QoS-Volumes überschritten (ocumQosVolumeMaxIopsWarning)	Risiko	Volumen	Warnung
Warnschwelle für maximales QoS-Volumen (MB/s) überschritten (ocumQosVolumeMaxMbpsWarning)	Risiko	Volumen	Warnung
Warnschwelle für maximale IOPS/TB des QoS-Volumes überschritten (ocumQosVolumeMaxIopsPerTbWarning)	Risiko	Volumen	Warnung
Latenzschwelle für Workload-Volumen überschritten, wie in der Richtlinie zum Leistungs-Servicelevel definiert (ocumConformanceLatencyWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Volume-IOPS-Schwellenwert überschritten (ocumVolumeIopsIncident)	Vorfall	Volumen	Kritisch
Schwellenwert für Volume-IOPS-Warnung überschritten (ocumVolumeIopsWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume 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
Schwellenwert für Volume-Latenzwarnung überschritten (ocumVolumeLatencyWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-Cache-Miss-Ratio überschritten (ocumVolumeCacheMissRatioIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume-Cache-Miss-Ratio überschritten (ocumVolumeCacheMissRatioWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für Volume-Latenz und IOPS überschritten (ocumVolumeLatencyIopsIncident)	Vorfall	Volumen	Kritisch
Schwellenwert für Volume-Latenz und IOPS-Warnung überschritten (ocumVolumeLatencyIopsWarning)	Risiko	Volumen	Warnung
Volume-Latenz und kritischer MB/s-Schwellenwert überschritten (ocumVolumeLatencyMbpsIncident)	Vorfall	Volumen	Kritisch
Volume-Latenz und MB/s-Warnschwelle überschritten (ocumVolumeLatencyMbpsWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-Latenz und genutzte Gesamtleistungskapazität überschritten (ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume-Latenz und genutzte Gesamtleistungskapazität überschritten (ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-Latenz und Aggregatauslastung überschritten (ocumVolumeLatencyAggregateUtilizationIncident)	Vorfall	Volumen	Kritisch

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Warnschwelle für Volume-Latenz und Aggregatauslastung überschritten (ocumVolumeLatencyAggregateUtilizationWarning)	Risiko	Volumen	Warnung
Kritischer Schwellenwert für Volume-Latenz und genutzte Knotenleistungskapazität überschritten (ocumVolumeLatencyNodePerfCapacityUsedIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume-Latenz und Knotenleistung bei genutzter Kapazität überschritten (ocumVolumeLatencyNodePerfCapacityUsedWarning)	Risiko	Volumen	Warnung
Verwendete Volume-Latenz und Knotenleistungskapazität – kritischer Übernahmeschwellenwert überschritten (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Vorfall	Volumen	Kritisch
Verwendete Volume-Latenz und Knotenleistungskapazität – Schwellenwert für Übernahmewarnung überschritten (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Kritischer Schwellenwert für Volume-Latenz und Knotenauslastung überschritten (ocumVolumeLatencyNodeUtilizationIncident)	Vorfall	Volumen	Kritisch
Warnschwelle für Volume-Latenz und Knotenauslastung überschritten (ocumVolumeLatencyNodeUtilizationWarning)	Risiko	Volumen	Warnung

Wirkungsbereich: Sicherheit

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Die Volume-Anti-Ransomware-Überwachung ist aktiviert (aktiver Modus) (antiRansomwareVolumeStateEnabled)	Ereignis	Volumen	Information
Die Volume-Anti-Ransomware-Überwachung ist deaktiviert (antiRansomwareVolumeStateDisabled).	Risiko	Volumen	Warnung
Volume-Anti-Ransomware-Überwachung ist aktiviert (Lernmodus) (antiRansomwareVolumeStateDryrun)	Ereignis	Volumen	Information
Die Volume-Anti-Ransomware-Überwachung ist angehalten (Lernmodus) (antiRansomwareVolumeStateDryrunPaused)	Risiko	Volumen	Warnung

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Die Volume-Anti-Ransomware-Überwachung ist angehalten (aktiver Modus) (antiRansomwareVolumeStateEnablePaused)	Risiko	Volumen	Warnung
Die Volume-Anti-Ransomware-Überwachung wird deaktiviert (antiRansomwareVolumeStateDisableInProgress)	Risiko	Volumen	Warnung
Ransomware-Aktivität erkannt (callHomeRansomwareActivitySeen)	Vorfall	Volumen	Kritisch
Für die Anti-Ransomware-Überwachung geeignetes Volume (Lernmodus) (ocumEvtVolumeArwCandidate)	Ereignis	Volumen	Information
Für die Anti-Ransomware-Überwachung geeignetes Volume (Aktivmodus) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Risiko	Volumen	Warnung
Das Volume weist laute Anti-Ransomware-Warnmeldungen auf (antiRansomwareFeatureNoisyVolume)	Risiko	Volumen	Warnung

Wirkungsbereich: Datenschutz

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Volume verfügt über unzureichenden lokalen Snapshot-Schutz (volumeLacksLocalProtectionWarning)	Risiko	Volumen	Warnung
Das Volume verfügt über keinen ausreichenden lokalen Snapshot-Schutz (volumeLacksLocalProtectionCleared)	Risiko	Volumen	Warnung

Statusereignisse für die Volumeverschiebung

Statusereignisse zur Volumeverschiebung informieren Sie über den Status Ihrer Volumeverschiebung, sodass Sie diese auf potenzielle Probleme überwachen können. Ereignisse werden nach Auswirkungsbereich gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe, den Quellentyp und den Schweregrad.

Wirkungsbereich: Kapazität

Ereignisname (Trap-Name)	Auswirkungsstufe	Quellentyp	Schwere
Status der Datenträgerverschiebung: In Bearbeitung (Nicht zutreffend)	Ereignis	Volumen	Information
Status der Volumeverschiebung – Fehlgeschlagen (ocumEvtVolumeMoveFailed)	Risiko	Volumen	Fehler
Status der Datenträgerverschiebung: Abgeschlossen (Nicht zutreffend)	Ereignis	Volumen	Information
Volume-Verschiebung – Umstellung verschoben (ocumEvtVolumeMoveCutoverDeferred)	Risiko	Volumen	Warnung

Beschreibung der Ereignisfenster und Dialogfelder

Ereignisse benachrichtigen Sie über alle Probleme in Ihrer Umgebung. Sie können die Inventarseite und die Seite mit den Ereignisdetails der Ereignisverwaltung verwenden, um alle Ereignisse zu überwachen. Sie können die Benachrichtigung im Dialogfeld „Benachrichtigungs-Setup-Optionen“ konfigurieren. Auf der Seite „Ereigniseinrichtung“ können Sie Ereignisse deaktivieren oder aktivieren.

Benachrichtigungsseite

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 versendet werden.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

E-Mail

In diesem Bereich können Sie die folgenden E-Mail-Einstellungen für Warnbenachrichtigungen konfigurieren:

- **Absenderadresse**

  Gibt die E-Mail-Adresse an, von der die Warnbenachrichtigung gesendet wird. Dieser Wert wird auch als Absenderadresse für einen Bericht verwendet, wenn dieser freigegeben wird. Wenn die Absenderadresse bereits mit der Adresse „ActiveIQUnifiedManager@localhost.com“ ausgefüllt ist, sollten Sie sie in eine echte, funktionierende E-Mail-Adresse ändern, um sicherzustellen, dass 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, der zum Senden der Warnbenachrichtigung an die angegebenen Empfänger verwendet wird.

- **Benutzername**

  Gibt den SMTP-Benutzernamen an. Der SMTP-Benutzername ist nur erforderlich, wenn SMTPAUTH im SMTP-Server aktiviert ist.

- **Passwort**

  Gibt das SMTP-Passwort an. Der SMTP-Benutzername ist nur erforderlich, wenn SMTPAUTH im SMTP-Server aktiviert ist.

- **Hafen**

  Gibt den Port an, der vom SMTP-Hostserver zum Senden von Warnbenachrichtigungen verwendet wird.

  Der Standardwert ist 25.

- **START/TLS verwenden**

  Durch Aktivieren dieses Kontrollkästchens wird eine sichere Kommunikation zwischen dem SMTP-Server und dem Verwaltungsserver mithilfe der TLS/SSL-Protokolle (auch als start_tls und StartTLS bezeichnet) gewährleistet.

- **SSL verwenden**

  Durch Aktivieren dieses Kontrollkästchens wird eine sichere Kommunikation zwischen dem SMTP-Server und dem Verwaltungsserver mithilfe des SSL-Protokolls gewährleistet.

SNMP

In diesem Bereich können Sie die folgenden SNMP-Trap-Einstellungen konfigurieren:

- **Version**

  Gibt die SNMP-Version an, die Sie je nach der Art der erforderlichen Sicherheit verwenden möchten. Zu den Optionen gehören 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 Verwaltungsserver gesendeten SNMP-Traps empfängt. Um mehrere Trap-Ziele anzugeben, trennen Sie jeden Host durch ein Komma.

  Alle anderen SNMP-Einstellungen, wie beispielsweise „Version“ und „Ausgehender Port“, müssen für alle Hosts in der Liste gleich sein.

- **Ausgehender Trap-Port**

  Gibt den Port an, über den der SNMP-Server die Traps empfängt, die vom Management-Server gesendet werden.

  Der Standardwert ist 162.

- **Gemeinschaft**

  Der Community-String für den Zugriff auf den Host.

- **Motor-ID**

  Gibt die eindeutige Kennung des SNMP-Agenten an und wird automatisch vom Verwaltungsserver generiert. Engine ID ist mit 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**

  Gibt das zur Authentifizierung eines Benutzers verwendete Protokoll an. Zu den Protokolloptionen gehören MD5 und SHA. MD5 ist der Standardwert. Das Authentifizierungsprotokoll ist mit SNMP Version 3 mit

Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Authentifizierungskennwort**

  Gibt das Kennwort an, das bei der Authentifizierung eines Benutzers verwendet wird. Das Authentifizierungskennwort ist mit SNMP Version 3 mit Authentifizierung und SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

- **Datenschutzprotokoll**

  Gibt das Datenschutzprotokoll an, das zum Verschlüsseln von SNMP-Nachrichten verwendet wird. 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.

- **Datenschutz-Passwort**

  Gibt das Kennwort bei Verwendung des Datenschutzprotokolls an. Ein Datenschutzkennwort ist mit SNMP Version 3 mit Authentifizierung und Verschlüsselung verfügbar.

Weitere Informationen zu SNMP-Objekten und Traps finden Sie im Downloadbereich"Active IQ Unified Manager MIB" von der NetApp Support-Site.

Inventarseite für die Ereignisverwaltung

Auf der Inventarseite der Ereignisverwaltung können Sie eine Liste der aktuellen Ereignisse und ihrer Eigenschaften anzeigen. Sie können Aufgaben wie das Bestätigen, Auflösen und Zuweisen von Ereignissen ausführen. Sie können auch eine Benachrichtigung für bestimmte Ereignisse hinzufügen.

Die Informationen auf dieser Seite werden alle 5 Minuten automatisch aktualisiert, um sicherzustellen, dass die aktuellsten neuen Ereignisse angezeigt werden.

Filterkomponenten

Ermöglicht Ihnen, die in der Ereignisliste angezeigten Informationen anzupassen. Sie können die Liste der angezeigten Ereignisse mithilfe der folgenden Komponenten verfeinern:

- Menü „Ansicht“ zur Auswahl aus einer vordefinierten Liste mit Filterauswahlen.

  Dazu gehören Elemente wie alle aktiven (neuen und bestätigten) Ereignisse, aktive Leistungsereignisse, mir (dem angemeldeten Benutzer) zugewiesene Ereignisse und alle während aller Wartungsfenster generierten Ereignisse.

- Suchbereich zum Verfeinern der Ereignisliste durch Eingabe ganzer oder teilweiser Begriffe.
- Filterschaltfläche, die den Filterbereich öffnet, sodass Sie aus allen verfügbaren Feldern und Feldattributen auswählen können, um die Liste der Ereignisse zu verfeinern.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Zuweisen an**

  Ermöglicht Ihnen, den Benutzer auszuwählen, dem das Ereignis zugewiesen ist. Wenn Sie einem Benutzer

ein Ereignis zuweisen, werden der Benutzername und die Uhrzeit, zu der Sie das Ereignis zugewiesen haben, der Ereignisliste für die ausgewählten Ereignisse hinzugefügt.

  - Mich

    Weist das Ereignis dem aktuell angemeldeten Benutzer zu.

  - Ein anderer Benutzer

    Zeigt das Dialogfeld „Besitzer zuweisen“ an, in dem Sie das Ereignis anderen Benutzern zuweisen oder neu zuweisen können. Sie können die Zuweisung von Ereignissen auch aufheben, indem Sie das Eigentümerfeld leer lassen.

- **Anerkennen**

  Bestätigt die ausgewählten Ereignisse.

  Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und die Uhrzeit, zu der Sie das Ereignis bestätigt haben, der Ereignisliste für die ausgewählten Ereignisse hinzugefügt. Wenn Sie ein Ereignis bestätigen, sind Sie für die Verwaltung dieses Ereignisses verantwortlich.

  Sie können Informationsereignisse nicht bestätigen.

- **Als gelöst markieren**

  Ermöglicht Ihnen, den Ereignisstatus in „Gelöst“ zu ändern.

  Wenn Sie ein Ereignis lösen, werden Ihr Benutzername und der Zeitpunkt der Lösung des Ereignisses der Ereignisliste für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie Korrekturmaßnahmen für das Ereignis ergriffen haben, müssen Sie das Ereignis als gelöst markieren.

- **Benachrichtigung hinzufügen**

  Zeigt das Dialogfeld „Warnung hinzufügen“ an, in dem Sie Warnungen für die ausgewählten Ereignisse hinzufügen können.

- **Berichte**

  Ermöglicht Ihnen, Details der aktuellen Ereignisansicht in eine CSV-Datei (Comma-Separated Values) oder ein PDF-Dokument zu exportieren.

- **Spaltenauswahl ein-/ausblenden**

  Ermöglicht Ihnen, die auf der Seite anzuzeigenden Spalten auszuwählen und die Reihenfolge auszuwählen, in der sie angezeigt werden.

Ereignisliste

Zeigt Details aller Ereignisse sortiert nach Auslösezeit an.

Standardmäßig wird die Ansicht „Alle aktiven Ereignisse“ angezeigt, um die neuen und bestätigten Ereignisse der letzten sieben Tage anzuzeigen, die die Auswirkungsstufe „Vorfall“ oder „Risiko“ aufweisen.

- **Ausgelöste Zeit**

Der Zeitpunkt, zu dem das Ereignis generiert wurde.

- **Schwere**

  Der Schweregrad des Ereignisses: Kritisch ( ), Fehler ( ), Warnung ( ) und Informationen ( ).

- **Zustand**

  Der Ereignisstatus: Neu, Bestätigt, Gelöst oder Veraltet.

- **Auswirkungsebene**

  Die Auswirkungsstufe des Ereignisses: Vorfall, Risiko, Ereignis oder Upgrade.

- **Aufprallbereich**

  Der Auswirkungsbereich des Ereignisses: Verfügbarkeit, Kapazität, Leistung, Schutz, Konfiguration oder Sicherheit.

- **Name**

  Der Name des Ereignisses. Sie können den Namen auswählen, um die Seite mit den Ereignisdetails für dieses Ereignis anzuzeigen.

- **Quelle**

  Der Name des Objekts, bei dem das Ereignis aufgetreten ist. Sie können den Namen auswählen, um die Seite mit den Integritäts- oder Leistungsdetails für dieses Objekt anzuzeigen.

  Wenn ein Verstoß gegen die gemeinsame QoS-Richtlinie auftritt, wird in diesem Feld nur das Workload-Objekt angezeigt, das die meisten IOPS oder MB/s verbraucht. Zusätzliche Workloads, die diese Richtlinie verwenden, werden auf der Seite „Ereignisdetails“ angezeigt.

- **Quellentyp**

  Der Objekttyp (z. B. Storage VM, Volume oder Qtree), mit dem das Ereignis verknüpft ist.

- **Zugewiesen an**

  Der Name des Benutzers, dem das Ereignis zugewiesen ist.

- **Ereignisursprung**

  Ob das Ereignis vom „Active IQ Portal“ oder direkt vom „Active IQ Unified Manager“ stammt.

- **Anmerkungsname**

  Der Name der Anmerkung, die dem Speicherobjekt zugewiesen ist.

- **Anmerkungen**

  Die Anzahl der Notizen, die für ein Ereignis hinzugefügt werden.

- **Ausstehende Tage**

  Die Anzahl der Tage seit der ersten Generierung des Ereignisses.

- **Zugewiesene Zeit**

  Die Zeit, die vergangen ist, seit das Ereignis einem Benutzer zugewiesen wurde. Wenn die verstrichene Zeit eine Woche überschreitet, wird der Zeitstempel angezeigt, wann 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 Zeit, die seit der Bestätigung des Ereignisses vergangen ist. Wenn die verstrichene Zeit mehr als eine Woche beträgt, wird der Zeitstempel angezeigt, wann das Ereignis bestätigt wurde.

- **Gelöst von**

  Der Name des Benutzers, der das Ereignis gelöst hat. Das Feld ist leer, wenn das Ereignis nicht behoben ist.

- **Gelöst Zeit**

  Die Zeit, die seit der Lösung des Ereignisses vergangen ist. Wenn die verstrichene Zeit mehr als eine Woche beträgt, wird der Zeitstempel angezeigt, wann das Ereignis behoben wurde.

- **Veraltete Zeit**

  Der Zeitpunkt, zu dem der Status des Ereignisses „Veraltet“ wurde.

Seite mit Veranstaltungsdetails

Auf der Seite „Ereignisdetails“ können Sie die Details eines ausgewählten Ereignisses anzeigen, z. B. den Schweregrad des Ereignisses, die Auswirkungsstufe, den Auswirkungsbereich und die Ereignisquelle. Sie können auch zusätzliche Informationen zu möglichen Abhilfemaßnahmen zur Behebung des Problems anzeigen.

- **Veranstaltungsname**

  Der Name des Ereignisses und die Uhrzeit, zu der das Ereignis zuletzt gesehen wurde.

  Bei Nichtleistungsereignissen sind die zuletzt angezeigten Informationen nicht bekannt, solange sich das Ereignis im Status „Neu“ oder „Bestätigt“ befindet, und werden daher ausgeblendet.

- **Veranstaltungsbeschreibung**

  Eine kurze Beschreibung des Ereignisses.

  In einigen Fällen wird in der Ereignisbeschreibung ein Grund für die Auslösung des Ereignisses angegeben.

- **Umstrittene Komponente**

  Bei dynamischen Leistungsereignissen werden in diesem Abschnitt Symbole angezeigt, die die logischen

und physischen Komponenten des Clusters darstellen. Wenn eine Komponente umstritten ist, wird ihr Symbol eingekreist und rot hervorgehoben.

Eine Beschreibung der hier angezeigten Komponenten finden Sie unter *Clusterkomponenten und warum sie miteinander in Konflikt geraten können*.

Die Abschnitte „Ereignisinformationen“, „Systemdiagnose“ und „Vorgeschlagene Maßnahmen“ werden in anderen Themen beschrieben.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Notizensymbol**

  Ermöglicht Ihnen, eine Notiz zum Ereignis hinzuzufügen oder zu aktualisieren und alle von anderen Benutzern hinterlassenen Notizen zu überprüfen.

Aktionsmenü

- **Mir zuweisen**

  Weist Ihnen das Ereignis zu.

- **Anderen zuweisen**

  Öffnet das Dialogfeld „Besitzer zuweisen“, in dem Sie das Ereignis anderen Benutzern zuweisen oder neu zuweisen können.

  Wenn Sie einem Benutzer ein Ereignis zuweisen, werden der Name des Benutzers und die Uhrzeit der Ereigniszuweisung in der Ereignisliste für die ausgewählten Ereignisse hinzugefügt.

  Sie können die Zuweisung von Ereignissen auch aufheben, indem Sie das Eigentümerfeld leer lassen.

- **Anerkennen**

  Bestätigt die ausgewählten Ereignisse, sodass Sie nicht weiterhin wiederholt Warnbenachrichtigungen erhalten.

  Wenn Sie ein Ereignis bestätigen, werden Ihr Benutzername und die Uhrzeit, zu der Sie das Ereignis bestätigt haben, der Ereignisliste (Bestätigt von) für die ausgewählten Ereignisse hinzugefügt. Wenn Sie ein Ereignis bestätigen, übernehmen Sie die Verantwortung für die Verwaltung dieses Ereignisses.

- **Als gelöst markieren**

  Ermöglicht Ihnen, den Ereignisstatus in „Gelöst“ zu ändern.

  Wenn Sie ein Ereignis lösen, werden Ihr Benutzername und der Zeitpunkt der Lösung des Ereignisses in der Ereignisliste (Gelöst von) für die ausgewählten Ereignisse hinzugefügt. Nachdem Sie Korrekturmaßnahmen für das Ereignis ergriffen haben, müssen Sie das Ereignis als gelöst markieren.

- **Benachrichtigung hinzufügen**

  Zeigt das Dialogfeld „Warnung hinzufügen“ an, in dem Sie eine Warnung für das ausgewählte Ereignis hinzufügen können.

Was im Abschnitt „Ereignisinformationen“ angezeigt wird

Im Abschnitt „Ereignisinformationen“ auf der Seite „Ereignisdetails“ können Sie die Details zu einem ausgewählten Ereignis anzeigen, z. B. den Schweregrad des Ereignisses, die Auswirkungsstufe, den Auswirkungsbereich und die Ereignisquelle.

Felder, die für den Ereignistyp nicht relevant sind, werden ausgeblendet. Sie können die folgenden Ereignisdetails anzeigen:

- **Ereignisauslösezeit**

  Der Zeitpunkt, zu dem das Ereignis generiert wurde.

- **Zustand**

  Der Ereignisstatus: Neu, Bestätigt, Gelöst oder Veraltet.

- **Veraltete Ursache**

  Die Aktionen, die dazu geführt haben, dass das Ereignis veraltet ist, z. B. wurde das Problem behoben.

- **Veranstaltungsdauer**

  Bei aktiven (neuen und bestätigten) Ereignissen ist dies die Zeit zwischen der Erkennung und dem Zeitpunkt der letzten Analyse des Ereignisses. Bei veralteten Ereignissen ist dies die Zeit zwischen der Erkennung und der Lösung des Ereignisses.

  Dieses Feld wird für alle Leistungsereignisse und für andere Ereignistypen nur angezeigt, nachdem sie gelöst oder veraltet wurden.

- **Zuletzt gesehen**

  Das Datum und die Uhrzeit, zu der das Ereignis zuletzt als aktiv angesehen wurde.

  Bei Leistungsereignissen kann dieser Wert aktueller sein als die Ereignisauslösezeit, da dieses Feld nach jeder neuen Erfassung von Leistungsdaten 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.

- **Schwere**

  Der Schweregrad des Ereignisses: Kritisch ( ), Fehler ( ), Warnung ( ) und Informationen ( ).

- **Auswirkungsebene**

  Die Auswirkungsstufe des Ereignisses: Vorfall, Risiko, Ereignis oder Upgrade.

- **Aufprallbereich**

  Der Auswirkungsbereich des Ereignisses: Verfügbarkeit, Kapazität, Leistung, Schutz, Konfiguration oder Sicherheit.

- **Quelle**

  Der Name des Objekts, bei dem das Ereignis aufgetreten ist.

Beim Anzeigen der Details für ein freigegebenes QoS-Richtlinienereignis werden in diesem Feld bis zu drei der Workload-Objekte aufgelistet, die die meisten IOPS oder MBps verbrauchen.

Sie können auf den Link zum Quellennamen klicken, um die Seite mit den Integritäts- oder Leistungsdetails für dieses Objekt anzuzeigen.

- **Quellenanmerkungen**

  Zeigt den Namen und Wert der Anmerkung für das Objekt an, mit dem das Ereignis verknüpft ist.

  Dieses Feld wird nur für Integritätsereignisse auf Clustern, SVMs und Volumes angezeigt.

- **Quellgruppen**

  Zeigt die Namen aller Gruppen an, zu denen das betroffene Objekt gehört.

  Dieses Feld wird nur für Integritätsereignisse auf Clustern, SVMs und Volumes angezeigt.

- **Quellentyp**

  Der Objekttyp (z. B. SVM, Volume oder Qtree), mit dem das Ereignis verknüpft ist.

- **Auf Cluster**

  Der Name des Clusters, auf dem das Ereignis aufgetreten ist.

  Sie können auf den Link zum Clusternamen klicken, um die Seite mit den Integritäts- oder Leistungsdetails für diesen Cluster anzuzeigen.

- **Anzahl der betroffenen Objekte**

  Die Anzahl der vom Ereignis betroffenen Objekte.

  Sie können auf den Objektlink klicken, um die Inventarseite mit den Objekten anzuzeigen, die derzeit von diesem Ereignis betroffen sind.

  Dieses Feld wird nur für Leistungsereignisse angezeigt.

- **Betroffene Bände**

  Die Anzahl der Datenträger, die von diesem Ereignis betroffen sind.

  Dieses Feld wird nur für Leistungsereignisse auf Knoten oder Aggregaten angezeigt.

- **Ausgelöste Richtlinie**

  Der Name der Schwellenwertrichtlinie, die das Ereignis ausgelöst hat.

  Sie können den Cursor über den Richtliniennamen bewegen, um die Details der Schwellenwertrichtlinie anzuzeigen. Bei adaptiven QoS-Richtlinien werden auch die definierte Richtlinie, die Blockgröße und der Zuweisungstyp (zugewiesener Speicherplatz oder verwendeter Speicherplatz) angezeigt.

  Dieses Feld wird nur für Leistungsereignisse angezeigt.

- **Regel-ID**

Bei Active IQ -Plattformereignissen ist dies die Nummer der Regel, die zum Generieren des Ereignisses ausgelöst wurde.

- **Bestätigt von**

  Der Name der Person, die das Ereignis bestätigt hat, und der Zeitpunkt der Bestätigung des Ereignisses.

- **Gelöst von**

  Der Name der Person, die das Ereignis gelöst hat, und der Zeitpunkt der Lösung des Ereignisses.

- **Zugewiesen an**

  Der Name der Person, die mit der Arbeit an der Veranstaltung beauftragt ist.

- **Alarmeinstellungen**

  Die folgenden Informationen zu Warnungen werden angezeigt:

  - Wenn dem ausgewählten Ereignis keine Warnungen zugeordnet sind, wird der Link **Warnung hinzufügen** angezeigt.

    Sie können das Dialogfeld „Warnung hinzufügen“ öffnen, indem Sie auf den Link klicken.

  - 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.

  - Wenn dem ausgewählten Ereignis mehr als eine Warnung zugeordnet ist, wird die Anzahl der Warnungen angezeigt.

    Sie können die Seite „Alarm-Setup“ öffnen, indem Sie auf den Link klicken, um weitere Details zu diesen Alarmen anzuzeigen.

  Deaktivierte Warnungen werden nicht angezeigt.

- **Letzte Benachrichtigung gesendet**

  Datum und Uhrzeit der letzten Warnmeldung.

- **Senden per**

  Der Mechanismus, der zum Senden der Alarmbenachrichtigung verwendet wurde: E-Mail oder SNMP-Trap.

- **Vorheriger Skriptlauf**

  Der Name des Skripts, das beim Generieren der Warnung ausgeführt wurde.

Was im Abschnitt „Vorgeschlagene Aktionen“ angezeigt wird

Der Abschnitt „Vorgeschlagene Maßnahmen“ auf der Seite mit den Ereignisdetails enthält mögliche Gründe für das Ereignis und schlägt einige Maßnahmen vor, damit Sie versuchen können, das Ereignis selbst zu beheben. Die vorgeschlagenen Maßnahmen

werden je nach Art des Ereignisses oder der Art des überschrittenen Schwellenwerts individuell angepasst.

Dieser Bereich wird nur für bestimmte Ereignistypen angezeigt.

In einigen Fällen werden auf der Seite **Hilfe**-Links bereitgestellt, die auf zusätzliche Informationen zu vielen vorgeschlagenen Aktionen verweisen, einschließlich Anweisungen zum Ausführen 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 beinhalten.

Sie sollten die hier vorgeschlagenen Maßnahmen lediglich als Anleitung zur Lösung dieses Ereignisses betrachten. Die Maßnahmen, die Sie zur Lösung dieses Ereignisses ergreifen, sollten auf dem Kontext Ihrer Umgebung basieren.

Wenn Sie das Objekt und das Ereignis detaillierter analysieren möchten, klicken Sie auf die Schaltfläche **Arbeitslast analysieren**, um die Seite „Arbeitslastanalyse“ anzuzeigen.

Es gibt bestimmte Ereignisse, die Unified Manager gründlich diagnostizieren und eine einzige Lösung bereitstellen kann. Sofern verfügbar, werden diese Lösungen mit der Schaltfläche **Fix It** angezeigt. Klicken Sie auf diese Schaltfläche, damit Unified Manager das Problem behebt, das das Ereignis verursacht.

Bei Active IQ -Plattformereignissen kann dieser Abschnitt einen Link zu einem NetApp Knowledgebase-Artikel enthalten, sofern verfügbar, der das Problem und mögliche Lösungen beschreibt. An Standorten ohne externen Netzwerkzugriff wird lokal eine PDF-Datei des Knowledgebase-Artikels geöffnet. Die PDF-Datei ist Teil der Regeldatei, die Sie manuell auf die Unified Manager-Instanz herunterladen.

Was der Abschnitt „Systemdiagnose“ anzeigt

Der Abschnitt „Systemdiagnose“ auf der Seite „Ereignisdetails“ enthält Informationen, die Ihnen bei der Diagnose von Problemen helfen können, die möglicherweise für das Ereignis verantwortlich waren.

Dieser Bereich wird nur bei manchen Veranstaltungen angezeigt.

Einige Leistungsereignisse stellen Diagramme bereit, die für das jeweilige ausgelöste Ereignis relevant sind. Normalerweise umfasst dies ein IOPS- oder MBps-Diagramm und ein Latenzdiagramm für die letzten zehn Tage. Bei dieser Anordnung können Sie sehen, welche Speicherkomponenten die Latenz am stärksten beeinflussen oder von der Latenz betroffen sind, wenn das Ereignis aktiv ist.

Für dynamische Leistungsereignisse werden die folgenden Diagramme angezeigt:

- Arbeitslastlatenz – Zeigt den Verlauf der Latenz für die Arbeitslasten der Top-Opfer, Bullys oder Sharks bei der umstrittenen Komponente an.
- Workload-Aktivität – Zeigt Details zur Workload-Nutzung der konkurrierenden Clusterkomponente an.
- Ressourcenaktivität – Zeigen Sie historische Leistungsstatistiken für die umstrittene Clusterkomponente an.

Andere Diagramme werden angezeigt, wenn einige Clusterkomponenten miteinander konkurrieren.

Andere Ereignisse liefern eine kurze Beschreibung der Art der Analyse, die das System am Speicherobjekt durchführt. In einigen Fällen gibt es eine oder mehrere Zeilen, eine für jede analysierte Komponente, für systemdefinierte Leistungsrichtlinien, die mehrere Leistungsindikatoren analysieren. In diesem Szenario wird neben der Diagnose ein grünes oder rotes Symbol angezeigt, um anzugeben, ob bei dieser bestimmten

Diagnose ein Problem gefunden wurde oder nicht.

Seite „Ereigniseinrichtung“

Auf der Seite „Ereigniseinrichtung“ wird die Liste der deaktivierten Ereignisse angezeigt und es werden Informationen wie der zugehörige Objekttyp und der Schweregrad des Ereignisses bereitgestellt. Sie können auch Aufgaben wie das globale Deaktivieren oder Aktivieren von Ereignissen ausführen.

Sie können auf diese Seite nur zugreifen, wenn Sie über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie für ausgewählte Ereignisse die folgenden Aufgaben ausführen:

- **Deaktivieren**

  Öffnet das Dialogfeld „Ereignisse deaktivieren“, in dem Sie Ereignisse deaktivieren können.

- **Aktivieren**

  Aktiviert ausgewählte Ereignisse, die Sie zuvor deaktiviert hatten.

- **Upload-Regeln**

  Öffnet das Dialogfeld „Regeln hochladen“, das es Sites ohne externen Netzwerkzugriff ermöglicht, die Active IQ Regeldatei manuell in Unified Manager hochzuladen. Die Regeln werden für Cluster-AutoSupport -Nachrichten ausgeführt, um Ereignisse für Systemkonfiguration, Verkabelung, Best Practice und Verfügbarkeit zu generieren, wie von der Active IQ Plattform definiert.

- **EMS-Events abonnieren**

  Startet das Dialogfeld „EMS-Ereignisse abonnieren“, in dem Sie den Empfang bestimmter Event Management System (EMS)-Ereignisse von den Clustern abonnieren können, die Sie überwachen. Das EMS sammelt Informationen zu Ereignissen, die im Cluster auftreten. Wenn eine Benachrichtigung für ein abonniertes EMS-Ereignis eingeht, wird ein Unified Manager-Ereignis mit dem entsprechenden Schweregrad generiert.

Listenansicht

In der Listenansicht werden (in Tabellenform) Informationen zu deaktivierten Ereignissen angezeigt. Mithilfe der Spaltenfilter können Sie die angezeigten Daten anpassen.

- **Ereignis**

  Zeigt den Namen des deaktivierten Ereignisses an.

- **Schwere**

  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 wird.

Dialogfeld „Ereignisse deaktivieren“

Im Dialogfeld „Ereignisse deaktivieren“ wird die Liste der Ereignistypen angezeigt, für die Sie Ereignisse deaktivieren können. Sie können Ereignisse für einen Ereignistyp basierend auf einem bestimmten Schweregrad oder für eine Reihe von Ereignissen deaktivieren.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Bereich „Ereigniseigenschaften“

Im Bereich „Ereigniseigenschaften“ werden die folgenden Ereigniseigenschaften angegeben:

- **Ereignisschwere**

  Ermöglicht Ihnen die Auswahl von Ereignissen basierend auf dem Schweregradtyp, der „Kritisch“, „Fehler“, „Warnung“ oder „Information“ sein kann.

- **Ereignisname enthält**

  Ermöglicht Ihnen, Ereignisse zu filtern, deren Name die angegebenen Zeichen enthält.

- **Passende Ereignisse**

  Zeigt die Liste der Ereignisse an, die dem Schweregrad des Ereignisses und der von Ihnen angegebenen Textzeichenfolge entsprechen.

- **Ereignisse deaktivieren**

  Zeigt die Liste der Ereignisse an, die Sie zum Deaktivieren ausgewählt haben.

  Neben dem Ereignisnamen wird auch der Schweregrad des Ereignisses angezeigt.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie für die ausgewählten Ereignisse die folgenden Aufgaben ausführen:

- **Speichern und schließen**

  Deaktiviert den Ereignistyp und schließt das Dialogfeld.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld.

Verwalten von Warnungen

Sie können Warnmeldungen so konfigurieren, dass automatisch Benachrichtigungen gesendet werden, wenn bestimmte Ereignisse oder Ereignisse mit einem bestimmten Schweregrad eintreten. Sie können einer Warnung auch ein Skript zuordnen, das

ausgeführt wird, wenn eine Warnung ausgelöst wird.

Was sind Warnungen

Obwohl Ereignisse kontinuierlich auftreten, generiert der Unified Manager nur dann eine Warnung, wenn ein Ereignis bestimmte Filterkriterien erfüllt. Sie können die Ereignisse auswählen, bei denen Warnungen generiert werden sollen – beispielsweise, wenn ein Speicherplatzschwellenwert überschritten wird oder ein Objekt offline geht. Sie können einer Warnung auch ein Skript zuordnen, das ausgeführt wird, wenn eine Warnung ausgelöst wird.

Zu den Filterkriterien gehören Objektklasse, Name oder Ereignisschweregrad.

Welche Informationen sind in einer Warn-E-Mail enthalten?

Warn-E-Mails von Unified Manager enthalten den Ereignistyp, den Schweregrad des Ereignisses, den Namen der Richtlinie oder des Schwellenwerts, der bzw. die das Ereignis verursacht hat, sowie eine Beschreibung des Ereignisses. Die E-Mail-Nachricht enthält außerdem einen Hyperlink für jedes Ereignis, über den Sie die Detailseite für das Ereignis in der Benutzeroberfläche anzeigen können.

Warn-E-Mails werden an alle Benutzer gesendet, die den Erhalt von Warnmeldungen abonniert haben.

Wenn sich ein Leistungsindikator oder Kapazitätswert während eines Erfassungszeitraums stark ändert, kann dies dazu führen, dass für dieselbe Schwellenwertrichtlinie gleichzeitig ein kritisches Ereignis und ein Warnereignis ausgelöst werden. In diesem Fall erhalten Sie möglicherweise eine E-Mail für das Warnereignis und eine für das kritische Ereignis. Dies liegt daran, dass Sie mit Unified Manager separate Abonnements für den Empfang von Warnmeldungen bei Warnungen und kritischen Schwellenwertüberschreitungen abschließen können.

Nachfolgend sehen Sie ein Beispiel für eine Warn-E-Mail:

Benachrichtigungen hinzufügen

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

Bevor Sie beginnen

- Sie müssen Benachrichtigungseinstellungen wie die E-Mail-Adresse des Benutzers, den SMTP-Server und den SNMP-Trap-Host konfiguriert haben, damit der Active IQ Unified Manager Server diese Einstellungen verwenden kann, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.
- Sie müssen die Ressourcen und Ereignisse kennen, für die Sie die Warnung auslösen möchten, sowie die Benutzernamen oder E-Mail-Adressen der Benutzer, die Sie benachrichtigen möchten.
- Wenn Sie möchten, dass basierend auf dem Ereignis ein Skript ausgeführt wird, müssen Sie das Skript über die Seite „Skripte“ zu Unified Manager hinzugefügt haben.

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können nach dem Empfang eines Ereignisses direkt auf der Seite „Ereignisdetails“ eine Warnung erstellen. Außerdem können Sie eine Warnung auch auf der Seite „Warnungseinrichtung“ erstellen, wie hier beschrieben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
2. Klicken Sie auf der Seite **Alarm-Setup** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Warnung hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für die Warnung ein.
4. Klicken Sie auf **Ressourcen** und wählen Sie die Ressourcen aus, die in die Warnung einbezogen oder davon ausgeschlossen werden sollen.

   Sie können einen Filter festlegen, indem Sie im Feld **Name enthält** eine Textzeichenfolge angeben, um eine Gruppe von Ressourcen auszuwählen. Basierend auf der von Ihnen angegebenen Textzeichenfolge zeigt die Liste der verfügbaren Ressourcen nur die Ressourcen an, die der Filterregel entsprechen. Bei der von Ihnen angegebenen Textzeichenfolge wird zwischen Groß- und Kleinschreibung unterschieden.

   Wenn eine Ressource sowohl den von Ihnen angegebenen Einschluss- als auch Ausschlussregeln entspricht, hat die Ausschlussregel Vorrang vor der Einschlussregel und für Ereignisse im Zusammenhang mit der ausgeschlossenen Ressource wird keine Warnung generiert.

5. Klicken Sie auf **Ereignisse** und wählen Sie basierend auf dem Ereignisnamen oder dem Schweregradtyp die Ereignisse aus, für die Sie eine Warnung auslösen möchten.

   Um mehr als ein Ereignis auszuwählen, drücken Sie die Strg-Taste, während Sie Ihre Auswahl treffen.

6. Klicken Sie auf **Aktionen** und wählen Sie die Benutzer aus, die Sie benachrichtigen möchten, wählen Sie die Benachrichtigungshäufigkeit, wählen Sie, ob ein SNMP-Trap an den Trap-Empfänger gesendet werden soll, und weisen Sie ein Skript zu, das ausgeführt werden soll, wenn eine Warnung generiert wird.

   Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnung zur Bearbeitung erneut öffnen, wird das Feld „Name“ leer angezeigt, da die geänderte E-Mail-Adresse nicht mehr dem zuvor ausgewählten Benutzer zugeordnet ist. 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.

   Sie können Benutzer auch über SNMP-Traps benachrichtigen.

7. Klicken Sie auf **Speichern**.

Beispiel für das Hinzufügen einer Warnung

Dieses Beispiel zeigt, wie Sie eine Warnung erstellen, die die folgenden Anforderungen erfüllt:

- Warnungsname: HealthTest
- Ressourcen: schließt alle Datenträger ein, deren Name „abc“ enthält, und schließt alle Datenträger 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

Führen Sie im Dialogfeld „Warnung hinzufügen“ die folgenden Schritte aus:

1. Klicken Sie auf **Name** und geben Sie ein*`HealthTest` * im Feld **Alarmname**.
2. Klicken Sie auf **Ressourcen** und wählen Sie auf der Registerkarte „Einschließen“ aus der Dropdownliste **Volumes** aus.
   a. Eingeben*`abc` * im Feld **Name enthält**, um die Volumes anzuzeigen, deren Name „abc“ enthält.
   b. Wählen Sie **+[All Volumes whose name contains 'abc']** + aus dem Bereich „Verfügbare Ressourcen“ und verschieben Sie es in den Bereich „Ausgewählte Ressourcen“.
   c. Klicken Sie auf **Ausschließen** und geben Sie ein*`xyz` * in das Feld **Name enthält** ein und klicken Sie dann auf **Hinzufügen**.
3. Klicken Sie auf **Ereignisse** und wählen Sie im Feld „Ereignisschweregrad“ die Option **Kritisch** aus.
4. Wählen Sie im Bereich „Übereinstimmende Ereignisse“ die Option „Alle kritischen Ereignisse“ aus und verschieben Sie sie in den Bereich „Ausgewählte Ereignisse“.
5. Klicken Sie auf **Aktionen** und geben Sie ein*`sample@domain.com` * im Feld „Diese Benutzer benachrichtigen“.
6. Wählen Sie **Alle 15 Minuten erinnern**, um den Benutzer alle 15 Minuten zu benachrichtigen.

   Sie können einen Alarm so konfigurieren, dass den Empfängern für einen bestimmten Zeitraum wiederholt Benachrichtigungen gesendet werden. Sie sollten den Zeitpunkt ermitteln, ab dem die Ereignisbenachrichtigung für den Alarm aktiv ist.
7. Wählen Sie im Menü „Auszuführendes Skript auswählen“ die Option „Skript **Test**“ aus.
8. Klicken Sie auf **Speichern**.

Richtlinien zum Hinzufügen von Warnungen

Sie können Warnungen basierend auf einer Ressource, beispielsweise einem Cluster, Knoten, Aggregat oder Volume, und Ereignissen eines bestimmten Schweregradtyps hinzufügen. Als bewährte Methode können Sie für jedes Ihrer kritischen Objekte eine Warnung hinzufügen, nachdem Sie den Cluster hinzugefügt haben, zu dem das Objekt gehört.

Sie können die folgenden Richtlinien und Überlegungen verwenden, um Warnungen zu erstellen und Ihre Systeme effektiv zu verwalten:

- Beschreibung der Warnung

  Sie sollten eine Beschreibung für die Warnung angeben, damit Sie Ihre Warnungen effektiv verfolgen können.

- Ressourcen

  Sie sollten entscheiden, welche physische oder logische Ressource eine Warnung erfordert. Sie können Ressourcen nach Bedarf ein- und ausschließen. Wenn Sie beispielsweise Ihre Aggregate durch die Konfiguration einer Warnung genau überwachen möchten, müssen Sie die erforderlichen Aggregate aus der Ressourcenliste auswählen.

Wenn Sie beispielsweise eine Ressourcenkategorie auswählen, **+[All User or Group Quotas] +**, dann erhalten Sie Benachrichtigungen für alle Objekte in dieser Kategorie.

> Durch die Auswahl eines Clusters als Ressource werden nicht automatisch die Speicherobjekte innerhalb dieses Clusters ausgewählt. 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.

- Ereignisschweregrad

  Sie sollten entscheiden, ob ein Ereignis mit einem bestimmten Schweregrad (Kritisch, Fehler, Warnung) die Warnung auslösen soll und wenn ja, welcher Schweregrad.

- Ausgewählte Veranstaltungen

  Wenn Sie eine Warnung basierend auf dem Typ des generierten Ereignisses hinzufügen, sollten Sie entscheiden, für welche Ereignisse eine Warnung erforderlich ist.

  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 angeben. Sie können Ihre Skripte einer Warnung zuordnen, sodass sie ausgeführt werden, wenn eine Warnung generiert wird.

- Benachrichtigungshäufigkeit

  Sie können einen Alarm so konfigurieren, dass den Empfängern für eine bestimmte Zeit wiederholt eine Benachrichtigung gesendet wird. Sie sollten den Zeitpunkt ermitteln, ab dem die Ereignisbenachrichtigung für den Alarm aktiv ist. Wenn Sie möchten, dass die Ereignisbenachrichtigung wiederholt wird, 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 Warnungen für Leistungsereignisse

Sie können Warnmeldungen für einzelne Leistungsereignisse konfigurieren, genau wie für alle anderen Ereignisse, die Unified Manager empfängt. Wenn Sie außerdem alle Leistungsereignisse gleich behandeln und E-Mails an dieselbe Person senden möchten, können Sie eine einzelne Warnung erstellen, die Sie benachrichtigt, wenn kritische oder warnende Leistungsereignisse ausgelöst werden.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Das folgende Beispiel zeigt, wie ein Ereignis für alle kritischen Latenz-, IOPS- und MBps-Ereignisse erstellt

wird. Sie können dieselbe Methode verwenden, um Ereignisse aus allen Leistungsindikatoren und für alle Warnereignisse auszuwählen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
2. Klicken Sie auf der Seite **Alarm-Setup** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Warnung hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für die Warnung ein.
4. Wählen Sie auf der Seite **Ressourcen** keine Ressourcen aus.

   Da keine Ressourcen ausgewählt sind, wird die Warnung auf alle Cluster, Aggregate, Volumes usw. angewendet, für die diese Ereignisse empfangen werden.

5. Klicken Sie auf **Ereignisse** und führen Sie die folgenden Aktionen aus:
   a. Wählen Sie in der Liste „Ereignisschweregrad“ **Kritisch** aus.
   b. Geben Sie im Feld „Ereignisname enthält“ Folgendes ein:*`latency` * und klicken Sie dann auf den Pfeil, um alle passenden Ereignisse auszuwählen.
   c. Geben Sie im Feld „Ereignisname enthält“ Folgendes ein:*`iops` * und klicken Sie dann auf den Pfeil, um alle passenden Ereignisse auszuwählen.
   d. Geben Sie im Feld „Ereignisname enthält“ Folgendes ein:*`mbps` * und klicken Sie dann auf den Pfeil, um alle passenden Ereignisse auszuwählen.
6. Klicken Sie auf **Aktionen** und wählen Sie dann im Feld **Diese Benutzer benachrichtigen** den Namen des Benutzers aus, der die Warn-E-Mail erhalten soll.
7. Konfigurieren Sie auf dieser Seite alle anderen Optionen zum Ausgeben von SNMP-Traps und Ausführen eines Skripts.
8. Klicken Sie auf **Speichern**.

Testwarnungen

Sie können eine Warnung testen, um zu überprüfen, ob Sie sie richtig konfiguriert haben. Wenn ein Ereignis ausgelöst wird, wird eine Warnung generiert und eine Warn-E-Mail an die konfigurierten Empfänger gesendet. Mithilfe der Testwarnung können Sie überprüfen, ob die Benachrichtigung gesendet und Ihr Skript ausgeführt wird.

Bevor Sie beginnen

- Sie müssen Benachrichtigungseinstellungen wie die E-Mail-Adresse der Empfänger, den SMTP-Server und den SNMP-Trap konfiguriert haben.

  Der Unified Manager-Server kann diese Einstellungen verwenden, um Benachrichtigungen an Benutzer zu senden, wenn ein Ereignis generiert wird.

- Sie müssen ein Skript zugewiesen und so konfiguriert haben, dass es ausgeführt wird, wenn die Warnung generiert wird.
- Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.

2. Wählen Sie auf der Seite **Alarm-Setup** den Alarm aus, den Sie testen möchten, und klicken Sie dann auf **Test**.

   Eine Test-Benachrichtigungs-E-Mail wird an die E-Mail-Adressen gesendet, die Sie beim Erstellen der Benachrichtigung angegeben haben.

Aktivieren und Deaktivieren von Warnungen für behobene und veraltete Ereignisse

Für alle Ereignisse, die Sie zum Senden von Warnungen konfiguriert haben, wird eine Warnmeldung gesendet, wenn diese Ereignisse alle verfügbaren Status durchlaufen: Neu, Bestätigt, Gelöst und Veraltet. Wenn Sie keine Warnmeldungen für Ereignisse erhalten möchten, die in den Status „Gelöst“ oder „Veraltet“ wechseln, können Sie eine globale Einstellung konfigurieren, um diese Warnmeldungen zu unterdrücken.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Standardmäßig werden für Ereignisse, die in den Status „Gelöst“ oder „Veraltet“ wechseln, keine Warnungen gesendet.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
2. Führen Sie auf der Seite **Alarm-Setup** mithilfe des Schiebereglers neben dem Element **Alarme für behobene und veraltete Ereignisse** eine der folgenden Aktionen aus:

Zu…	Machen Sie Folgendes…
Beenden Sie das Senden von Warnmeldungen, wenn Ereignisse behoben oder veraltet sind	Bewegen Sie den Schieberegler nach links
Beginnen Sie mit dem Senden von Warnmeldungen, wenn Ereignisse behoben oder verworfen werden	Bewegen Sie den Schieberegler nach rechts

Ausschließen von Disaster Recovery-Zielvolumes von der Generierung von Warnungen

Beim Konfigurieren von Volumewarnungen können Sie im Dialogfeld „Warnung“ eine Zeichenfolge angeben, die ein Volume oder eine Gruppe von Volumes identifiziert. Wenn Sie jedoch die Notfallwiederherstellung für SVMs konfiguriert haben, haben Quell- und Zielvolumes denselben Namen, sodass Sie für beide Volumes Warnungen erhalten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können Warnungen für Zielvolumes zur Notfallwiederherstellung deaktivieren, indem Sie Volumes ausschließen, die den Namen der Ziel-SVM haben. 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 Sie Warnungen für das Volume „vol1“ auf der primären SVM „vs1“ erstellen, aber die Generierung der Warnung auf einem Volume mit demselben Namen auf der SVM „vs1-dr“ ausschließen.

Führen Sie im Dialogfeld „Warnung hinzufügen“ die folgenden Schritte aus:

Schritte

1. Klicken Sie auf **Name** und geben Sie einen Namen und eine Beschreibung für die Warnung ein.
2. Klicken Sie auf **Ressourcen** und wählen Sie dann die Registerkarte **Einschließen**.
   a. Wählen Sie **Volume** aus der Dropdown-Liste und geben Sie dann*`vol1` * im Feld **Name enthält**, um die Volumes anzuzeigen, deren Name „vol1“ enthält.
   b. Wählen Sie **+[All Volumes whose name contains 'vol1'] +** aus dem Bereich **Verfügbare Ressourcen** und verschieben Sie es in den Bereich **Ausgewählte Ressourcen**.
3. Wählen Sie die Registerkarte **Ausschließen**, wählen Sie **Volume**, geben Sie ein*`vs1-dr` * in das Feld **Name enthält** ein und klicken Sie dann auf **Hinzufügen**.

   Dadurch wird verhindert, dass die Warnung für das Volume „vol1“ auf SVM „vs1-dr“ generiert wird.
4. Klicken Sie auf **Ereignisse** und wählen Sie das oder die Ereignisse aus, die Sie auf das oder die Volumes anwenden möchten.
5. Klicken Sie auf **Aktionen** und wählen Sie dann im Feld **Diese Benutzer benachrichtigen** den Namen des Benutzers aus, der die Warn-E-Mail erhalten soll.
6. Konfigurieren Sie auf dieser Seite alle anderen Optionen zum Ausgeben von SNMP-Traps und Ausführen eines Skripts und klicken Sie dann auf **Speichern**.

Warnungen anzeigen

Sie können die Liste der Warnungen, die für verschiedene Ereignisse erstellt werden, auf der Seite „Warnungseinrichtung“ anzeigen. Sie können auch Alarmeigenschaften wie die Alarmbeschreibung, Benachrichtigungsmethode und -häufigkeit, Ereignisse, die den Alarm auslösen, E-Mail-Empfänger der Alarme und betroffene Ressourcen wie Cluster, Aggregate und Volumes anzeigen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritt

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.

   Die Liste der Warnungen wird auf der Seite „Warnungseinrichtung“ angezeigt.

Benachrichtigungen bearbeiten

Sie können Alarmeigenschaften wie die Ressource, mit der der Alarm verknüpft ist, Ereignisse, Empfänger, Benachrichtigungsoptionen, Benachrichtigungshäufigkeit und zugehörige Skripte bearbeiten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
2. Wählen Sie auf der Seite **Alarm-Setup** den Alarm aus, den Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
3. Bearbeiten Sie im Dialogfeld **Alarm bearbeiten** nach Bedarf die Abschnitte „Name“, „Ressourcen“, „Ereignisse“ und „Aktionen“.

   Sie können das mit der Warnung verknüpfte Skript ändern oder entfernen.

4. Klicken Sie auf **Speichern**.

Benachrichtigungen löschen

Sie können eine Warnung löschen, wenn sie nicht mehr benötigt wird. Sie können beispielsweise eine Warnung löschen, die für eine bestimmte Ressource erstellt wurde, wenn diese Ressource nicht mehr von Unified Manager überwacht wird.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
2. Wählen Sie auf der Seite **Alarm-Setup** die Alarme aus, die Sie löschen möchten, und klicken Sie auf **Löschen**.
3. Klicken Sie auf **Ja**, um die Löschanforderung zu bestätigen.

Beschreibung der Warnfenster und Dialogfelder

Sie sollten Warnungen konfigurieren, um Benachrichtigungen über Ereignisse zu erhalten, indem Sie das Dialogfeld „Warnung hinzufügen“ verwenden. Sie können die Liste der Warnungen auch auf der Seite „Warnungseinrichtung“ anzeigen.

Seite „Alarm-Setup“

Auf der Seite „Alarm-Setup“ wird eine Liste mit Alarmen angezeigt und es werden Informationen zu Alarmnamen, Status, Benachrichtigungsmethode und Benachrichtigungshäufigkeit bereitgestellt. Sie können auf dieser Seite auch Warnungen hinzufügen, bearbeiten, entfernen, aktivieren oder deaktivieren.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

- **Hinzufügen**

  Zeigt das Dialogfeld „Warnung hinzufügen“ an, in dem Sie neue Warnungen hinzufügen können.

- **Bearbeiten**

  Zeigt das Dialogfeld „Warnung bearbeiten“ an, in dem Sie ausgewählte Warnungen bearbeiten können.

- **Löschen**

  Löscht die ausgewählten Warnungen.

- **Aktivieren**

  Aktiviert das Senden von Benachrichtigungen für die ausgewählten Warnungen.

- **Deaktivieren**

  Deaktiviert die ausgewählten Warnungen, wenn Sie das Senden von Benachrichtigungen vorübergehend beenden möchten.

- **Prüfen**

  Testet die ausgewählten Warnungen, um ihre Konfiguration nach dem Hinzufügen oder Bearbeiten zu überprüfen.

- **Warnungen für gelöste und veraltete Ereignisse**

  Ermöglicht Ihnen, das Senden von Warnungen zu aktivieren oder zu deaktivieren, wenn Ereignisse in den Status „Gelöst“ oder „Veraltet“ verschoben werden. Dies kann dazu beitragen, dass Benutzer keine unnötigen Benachrichtigungen erhalten.

Listenansicht

Die Listenansicht zeigt in tabellarischer Form Informationen zu den erstellten Warnungen an. Mithilfe der Spaltenfilter können Sie die angezeigten Daten anpassen. Sie können auch eine Warnung auswählen, um im Detailbereich weitere Informationen dazu anzuzeigen.

- **Status**

  Gibt an, ob eine Warnung aktiviert ist ( ) oder deaktiviert ( ).

- **Alarm**

  Zeigt den Namen der Warnung an.

- **Beschreibung**

  Zeigt eine Beschreibung für die Warnung an.

- **Benachrichtigungsmethode**

  Zeigt die für die Warnung ausgewählte Benachrichtigungsmethode an. Sie können Benutzer per E-Mail oder SNMP-Traps benachrichtigen.

- **Benachrichtigungshäufigkeit**

  Gibt die Häufigkeit (in Minuten) an, mit der der Verwaltungsserver weiterhin Benachrichtigungen sendet, bis das Ereignis bestätigt, gelöst oder in den Status „Veraltet“ versetzt wird.

Detailbereich

Der Detailbereich bietet weitere Informationen zur ausgewählten Warnung.

- **Name der Warnung**

  Zeigt den Namen der Warnung an.

- **Alarmbeschreibung**

  Zeigt eine Beschreibung für die Warnung an.

- **Veranstaltungen**

  Zeigt die Ereignisse an, für die Sie den Alarm auslösen möchten.

- **Ressourcen**

  Zeigt die Ressourcen an, für die Sie den Alarm auslösen möchten.

- **Beinhaltet**

  Zeigt die Gruppe von Ressourcen an, für die Sie den Alarm auslösen möchten.

- **Ausgeschlossen**

  Zeigt die Gruppe von Ressourcen an, für die Sie den Alarm nicht auslösen möchten.

- **Benachrichtigungsmethode**

  Zeigt die Benachrichtigungsmethode für die Warnung an.

- **Benachrichtigungshäufigkeit**

  Zeigt die Häufigkeit an, mit der der Verwaltungsserver weiterhin Warnbenachrichtigungen sendet, bis das Ereignis bestätigt, behoben oder in den Status „Veraltet“ versetzt 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 Warnbenachrichtigung erhalten.

Dialogfeld „Warnung hinzufügen“

Sie können Warnmeldungen erstellen, die Sie benachrichtigen, wenn ein bestimmtes Ereignis generiert wird, sodass Sie das Problem schnell beheben und dadurch die Auswirkungen auf Ihre Umgebung minimieren können. Sie können Warnungen für eine einzelne Ressource oder eine Gruppe von Ressourcen sowie für Ereignisse eines bestimmten Schweregrads erstellen. Sie können auch die Benachrichtigungsmethode und die Häufigkeit der Warnungen angeben.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Name

In diesem Bereich können Sie einen Namen und eine Beschreibung für die Warnung angeben:

- **Name der Warnung**

  Ermöglicht Ihnen, einen Alarmnamen anzugeben.

- **Alarmbeschreibung**

  Ermöglicht Ihnen, eine Beschreibung für die Warnung anzugeben.

Ressourcen

In diesem Bereich können Sie eine einzelne Ressource auswählen oder die Ressourcen basierend auf einer dynamischen Regel gruppieren, für die Sie den Alarm auslösen möchten. Eine *dynamische Regel* ist der Satz von Ressourcen, der basierend auf der von Ihnen angegebenen Textzeichenfolge 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 Warnung von einer der Detailseiten des Speicherobjekts aus erstellen, wird das Speicherobjekt automatisch in die Warnung aufgenommen.

- **Enthalten**

  Ermöglicht Ihnen, die Ressourcen einzuschließen, für die Sie Warnungen auslösen möchten. Sie können eine Textzeichenfolge angeben, um Ressourcen zu gruppieren, die der Zeichenfolge entsprechen, und diese Gruppe für die Einbeziehung in die Warnung auswählen. Sie können beispielsweise alle Datenträger gruppieren, deren Name die Zeichenfolge „abc“ enthält.

- **Ausschließen**

  Ermöglicht Ihnen, Ressourcen auszuschließen, für die Sie keine Warnungen auslösen möchten. Sie können beispielsweise alle Volumes ausschließen, deren Name die Zeichenfolge „xyz“ enthält.

  Die Registerkarte „Ausschließen“ wird nur angezeigt, wenn Sie alle Ressourcen eines bestimmten Ressourcentyps auswählen: beispielsweise +[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 die Warnung wird für das Ereignis nicht generiert.

Veranstaltungen

In diesem Bereich können Sie die Ereignisse auswählen, für die Sie Benachrichtigungen erstellen möchten. Sie können Warnungen für Ereignisse basierend auf einem bestimmten Schweregrad oder für eine Reihe von Ereignissen erstellen.

Um mehr als ein Ereignis auszuwählen, sollten Sie die Strg-Taste gedrückt halten, während Sie Ihre Auswahl treffen.

- **Ereignisschwere**

Ermöglicht Ihnen die Auswahl von Ereignissen basierend auf dem Schweregradtyp, der „Kritisch“, „Fehler“ oder „Warnung“ sein kann.

- **Ereignisname enthält**

  Ermöglicht Ihnen die Auswahl von Ereignissen, deren Name bestimmte Zeichen enthält.

Aktionen

In diesem Bereich können Sie die Benutzer angeben, die Sie benachrichtigen möchten, wenn ein Alarm ausgelöst wird. Sie können auch die Benachrichtigungsmethode und die Benachrichtigungshäufigkeit angeben.

- **Diese Benutzer benachrichtigen**

  Ermöglicht Ihnen, die E-Mail-Adresse oder den Benutzernamen des Benutzers anzugeben, der Benachrichtigungen erhalten soll.

  Wenn Sie die für den Benutzer angegebene E-Mail-Adresse ändern und die Warnung zur Bearbeitung erneut öffnen, wird das Feld „Name“ leer angezeigt, da die geänderte E-Mail-Adresse nicht mehr dem zuvor ausgewählten Benutzer zugeordnet ist. 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 Ihnen, die Häufigkeit anzugeben, mit der der Verwaltungsserver Benachrichtigungen sendet, bis das Ereignis bestätigt, behoben oder in den veralteten Status versetzt wird.

  Sie können zwischen folgenden Benachrichtigungsmethoden wählen:

  - Nur einmal benachrichtigen
  - Benachrichtigung in einer festgelegten Häufigkeit
  - Benachrichtigen Sie in einer bestimmten Häufigkeit innerhalb eines bestimmten Zeitbereichs

- **SNMP-Trap ausgeben**

  Durch Aktivieren dieses Kontrollkästchens können Sie angeben, ob SNMP-Traps an den global konfigurierten SNMP-Host gesendet werden sollen.

- **Skript ausführen**

  Ermöglicht Ihnen, der Warnung Ihr benutzerdefiniertes Skript hinzuzufügen. Dieses Skript wird ausgeführt, wenn eine Warnung generiert wird.

> Wenn diese Funktion in der Benutzeroberfläche nicht verfügbar ist, liegt das daran, dass Ihr Administrator sie deaktiviert hat. Bei Bedarf können Sie diese Funktion unter **Speicherverwaltung** > **Funktionseinstellungen** aktivieren.

Befehlsschaltflächen

- **Speichern**

  Erstellt eine Warnung und schließt das Dialogfeld.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld.

Dialogfeld „Warnung bearbeiten“

Sie können Alarmeigenschaften wie die Ressource, mit der der Alarm verknüpft ist, Ereignisse, Skripts und Benachrichtigungsoptionen bearbeiten.

Name

In diesem Bereich können Sie den Namen und die Beschreibung der Warnung bearbeiten.

- **Name der Warnung**

  Ermöglicht Ihnen, den Alarmnamen zu bearbeiten.

- **Alarmbeschreibung**

  Ermöglicht Ihnen, eine Beschreibung für die Warnung anzugeben.

- **Alarmzustand**

  Ermöglicht Ihnen, den Alarm zu aktivieren oder zu deaktivieren.

Ressourcen

In diesem Bereich können Sie eine einzelne Ressource auswählen oder die Ressourcen basierend auf einer dynamischen Regel gruppieren, für die Sie den Alarm 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 einzuschließen, für die Sie Warnungen auslösen möchten. Sie können eine Textzeichenfolge angeben, um Ressourcen zu gruppieren, die der Zeichenfolge entsprechen, und diese Gruppe für die Einbeziehung in die Warnung auswählen. Sie können beispielsweise alle Volumes gruppieren, deren Name die Zeichenfolge „`vol0`“ enthält.

- **Ausschließen**

  Ermöglicht Ihnen, Ressourcen auszuschließen, für die Sie keine Warnungen auslösen möchten. Sie können beispielsweise alle Volumes ausschließen, deren Name die Zeichenfolge „xyz“ enthält.

> Die Registerkarte „Ausschließen“ wird nur angezeigt, wenn Sie alle Ressourcen eines bestimmten Ressourcentyps auswählen, z. B. +[All Volumes] + oder +[All Volumes whose name contains 'xyz'] +.

Veranstaltungen

In diesem Bereich können Sie die Ereignisse auswählen, für die Sie die Warnungen auslösen möchten. Sie können eine Warnung für Ereignisse basierend auf einem bestimmten Schweregrad oder für eine Reihe von Ereignissen auslösen.

- **Ereignisschwere**

  Ermöglicht Ihnen die Auswahl von Ereignissen basierend auf dem Schweregradtyp, der „Kritisch“, „Fehler“ oder „Warnung“ sein kann.

- **Ereignisname enthält**

  Ermöglicht Ihnen die Auswahl von Ereignissen, deren Name die angegebenen Zeichen enthält.

Aktionen

In diesem Bereich können Sie die Benachrichtigungsmethode und die Benachrichtigungshäufigkeit festlegen.

- **Diese Benutzer benachrichtigen**

  Ermöglicht Ihnen, die E-Mail-Adresse oder den Benutzernamen zu bearbeiten oder eine neue E-Mail-Adresse oder einen neuen Benutzernamen zum Empfangen von Benachrichtigungen anzugeben.

- **Benachrichtigungshäufigkeit**

  Ermöglicht Ihnen, die Häufigkeit zu bearbeiten, mit der der Verwaltungsserver Benachrichtigungen sendet, bis das Ereignis bestätigt, gelöst oder in den veralteten Status versetzt wird.

  Sie können zwischen folgenden Benachrichtigungsmethoden wählen:

  - Nur einmal benachrichtigen
  - Benachrichtigung in einer festgelegten Häufigkeit
  - Benachrichtigen Sie in einer bestimmten Häufigkeit innerhalb eines bestimmten Zeitbereichs

- **SNMP-Trap ausgeben**

  Ermöglicht Ihnen anzugeben, ob SNMP-Traps an den global konfigurierten SNMP-Host gesendet werden sollen.

- **Skript ausführen**

  Ermöglicht Ihnen, der Warnung ein Skript zuzuordnen. Dieses Skript wird ausgeführt, wenn eine Warnung generiert wird.

Befehlsschaltflächen

- **Speichern**

  Speichert die Änderungen und schließt das Dialogfeld.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld.

Skripte verwalten

Sie können Skripte verwenden, um mehrere Speicherobjekte in Unified Manager automatisch zu ändern oder zu aktualisieren. Das Skript ist mit einer Warnung verknüpft.

Wenn ein Ereignis eine Warnung auslöst, wird das Skript ausgeführt. Sie können benutzerdefinierte Skripte hochladen und deren Ausführung testen, wenn eine Warnung generiert wird.

Die Möglichkeit, Skripte in Unified Manager hochzuladen und auszuführen, ist standardmäßig aktiviert. Wenn Ihre Organisation 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"

So funktionieren Skripte mit Warnungen

Sie können Ihrem Skript eine Warnung zuordnen, sodass das Skript ausgeführt wird, wenn für ein Ereignis in Unified Manager eine Warnung ausgelöst wird. Sie können die Skripts verwenden, um Probleme mit Speicherobjekten zu beheben oder zu ermitteln, welche Speicherobjekte die Ereignisse generieren.

Wenn für ein Ereignis in Unified Manager eine Warnung generiert wird, wird eine Warn-E-Mail an die angegebenen Empfänger gesendet. Wenn Sie eine Warnung mit einem Skript verknüpft haben, wird das Skript ausgeführt. Die Einzelheiten zu den an das Skript übergebenen Argumenten können Sie der Warn-E-Mail entnehmen.

> Wenn Sie ein benutzerdefiniertes Skript erstellt und es mit einer Warnung für einen bestimmten Ereignistyp verknüpft haben, werden Aktionen basierend auf Ihrem benutzerdefinierten Skript für diesen Ereignistyp ausgeführt und die Aktionen **Fix it** sind standardmäßig auf der Seite „Verwaltungsaktionen“ oder im Unified Manager-Dashboard nicht verfügbar.

Das Skript verwendet die folgenden Argumente zur Ausführung:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Sie können die Argumente in Ihren Skripten verwenden und zugehörige Ereignisinformationen sammeln oder Speicherobjekte ändern.

Beispiel zum Abrufen von Argumenten aus Skripten

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

Wenn eine Warnung generiert wird, wird dieses Skript ausgeführt und die folgende Ausgabe angezeigt:

```
-`eventID : 290`
-`eventSourceID : 4138`
```

Skripts hinzufügen

Sie können in Unified Manager Skripte hinzufügen und die Skripte mit Warnungen verknüpfen. Diese Skripte werden automatisch ausgeführt, wenn eine Warnung generiert wird, und ermöglichen es Ihnen, Informationen zu Speicherobjekten zu erhalten, für die das Ereignis generiert wird.

Bevor Sie beginnen

- Sie müssen die Skripte erstellt und gespeichert haben, die Sie dem Unified Manager-Server hinzufügen möchten.
- 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 wird Perl 5 standardmäßig installiert und Skripte unterstützen nur das, was Perl 5 unterstützt. Wenn Perl nach Unified Manager installiert wurde, müssen Sie den Unified Manager-Server neu starten.
  - 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 Warnskripts zu verfolgen, müssen Sie sicherstellen, dass die Protokolldateien nicht irgendwo im Installationsordner von Unified Manager erstellt werden.

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können benutzerdefinierte Skripte hochladen und Ereignisdetails zur Warnung sammeln.

> Wenn diese Funktion in der Benutzeroberfläche nicht verfügbar ist, liegt das daran, dass Ihr Administrator sie deaktiviert hat. Bei Bedarf können Sie diese Funktion unter **Speicherverwaltung** > **Funktionseinstellungen** aktivieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Skripte**.
2. Klicken Sie auf der Seite **Skripte** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Skript hinzufügen** auf **Durchsuchen**, um Ihre Skriptdatei auszuwählen.
4. Geben Sie eine Beschreibung für das ausgewählte Skript ein.
5. Klicken Sie auf **Hinzufügen**.

Verwandte Informationen

"Aktivieren und Deaktivieren der Möglichkeit zum Hochladen von Skripten"

Skripte löschen

Sie können ein Skript aus Unified Manager löschen, wenn das Skript nicht mehr benötigt wird oder nicht mehr gültig ist.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Das Skript darf nicht mit einer Warnung verknüpft sein.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Skripte**.
2. Wählen Sie auf der Seite **Skripte** das Skript aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang mit einem Klick auf **Ja**.

Testskriptausführung

Sie können überprüfen, ob Ihr Skript korrekt ausgeführt wird, wenn eine Warnung für ein Speicherobjekt generiert wird.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen ein Skript im unterstützten Dateiformat in Unified Manager hochgeladen haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Skripte**.
2. Fügen Sie auf der Seite **Skripte** Ihr Testskript hinzu.
3. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
4. Führen Sie auf der Seite **Alarm-Setup** eine der folgenden Aktionen aus:

Zu…	Machen Sie Folgendes…
Hinzufügen einer Benachrichtigung	a. Klicken Sie auf **Hinzufügen**. b. Ordnen Sie im Abschnitt „Aktionen“ die Warnung Ihrem Testskript zu.

Zu…	Machen Sie Folgendes…
Bearbeiten einer Benachrichtigung	a. Wählen Sie eine Warnung aus und klicken Sie dann auf **Bearbeiten**. b. Ordnen Sie im Abschnitt „Aktionen“ die Warnung Ihrem Testskript zu.

5. Klicken Sie auf **Speichern**.
6. Wählen Sie auf der Seite **Alarm-Setup** den Alarm aus, den Sie hinzugefügt oder geändert haben, und klicken Sie dann auf **Test**.

   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.

Unterstützte Unified Manager CLI-Befehle

Als Speicheradministrator können Sie die CLI-Befehle verwenden, um Abfragen zu den Speicherobjekten durchzuführen, beispielsweise zu Clustern, Aggregaten, Volumes, Qtrees und LUNs. Sie können die CLI-Befehle verwenden, um die interne Datenbank des Unified Managers und die ONTAP Datenbank abzufragen. Sie können CLI-Befehle auch in Skripten verwenden, die zu Beginn oder am Ende eines Vorgangs oder beim Auslösen einer Warnung ausgeführt werden.

Allen Befehlen muss der Befehl vorangestellt werden `um cli login` und einen gültigen Benutzernamen und ein gültiges Passwort zur Authentifizierung.

Stellen Sie zum Ausführen des Befehls *um run* sicher, dass Ihr Konto über den Anwendungszugriff *console* verfügt.

CLI-Befehl	Beschreibung	Ausgabe
`um cli login -u <username> [-p <password>]`	Meldet sich bei der CLI an. Aus Sicherheitsgründen sollten Sie nach der Option „-u“ nur den Benutzernamen eingeben. Bei dieser Verwendung werden Sie zur Eingabe des Kennworts aufgefordert und das Kennwort wird nicht im Verlauf oder 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 sich von der CLI ab.	Zeigt die entsprechende Meldung an.

CLI-Befehl	Beschreibung	Ausgabe
`um help`	Zeigt alle Unterbefehle der ersten Ebene an.	Zeigt alle Unterbefehle der ersten Ebene an.
`um run cmd [ -t <timeout> ] <cluster> <command>`	Die einfachste Möglichkeit, einen Befehl auf einem oder mehreren Hosts auszuführen. Wird hauptsächlich für Alarmskripte verwendet, um einen Vorgang auf ONTAP abzurufen oder auszuführen. Das optionale Timeout-Argument legt ein maximales Zeitlimit (in Sekunden) fest, das für die Ausführung des Befehls auf dem Client erforderlich ist. Der Standardwert ist 0 (ewig warten).	Wie von ONTAP erhalten.
`um run query <sql command>`	Führt eine SQL-Abfrage aus. Es sind nur Abfragen zulässig, die aus der Datenbank lesen. Aktualisierungs-, Einfüge- oder Löschvorgänge werden nicht unterstützt.	Die Ergebnisse werden in tabellarischer Form angezeigt. Wenn ein leerer Satz zurückgegeben wird oder ein Syntaxfehler oder eine fehlerhafte Anfrage vorliegt, wird die entsprechende Fehlermeldung angezeigt.
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Fügt der Liste der verwalteten Speichersysteme eine Datenquelle hinzu. Eine Datenquelle beschreibt, wie Verbindungen zu Speichersystemen hergestellt werden. Beim Hinzufügen einer Datenquelle müssen die Optionen -u (Benutzername) und -P (Passwort) angegeben werden. Die Option -t (Protokoll) gibt das für die Kommunikation mit dem Cluster verwendete Protokoll an (http oder https). Wenn das Protokoll nicht angegeben ist, werden beide Protokolle versucht. Die Option -p (Port) gibt den Port an, der für die Kommunikation mit dem Cluster verwendet wird. Wenn der Port nicht angegeben ist, wird der Standardwert des entsprechenden Protokolls versucht. Dieser Befehl kann nur vom Speicheradministrator ausgeführt werden.	Der Benutzer wird aufgefordert, das Zertifikat zu akzeptieren, und die entsprechende Meldung wird gedruckt.

CLI-Befehl	Beschreibung	Ausgabe
`um datasource list [ <datasource-id>]`	Zeigt die Datenquellen für verwaltete Speichersysteme an.	Zeigt die folgenden Werte im Tabellenformat 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 Speicheradministrator 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> .. ]`	Listet alle Optionen auf, die Sie mit dem Befehl „Set“ konfigurieren können.	Zeigt die folgenden Werte im Tabellenformat an: `Name, Value, Default Value, and Requires Restart.`
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	Legt eine oder mehrere Optionen fest. Der Befehl kann nur vom Speicheradministrator ausgeführt werden.	Zeigt die entsprechende Meldung an.
`um version`	Zeigt die Softwareversion von Unified Manager 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 keinen Header anzuzeigen. ObjectType kann LUN, Qtree, Cluster, Volume, Quota oder SVM sein. Beispiel: **`um lun list -cluster 1`** In diesem Beispiel ist „-cluster“ der Objekttyp und „1“ die Objekt-ID. Der Befehl listet alle LUNs innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an: `ID and LUN path.`

CLI-Befehl	Beschreibung	Ausgabe
`um svm list [-q] [ -ObjectType <object-id>]`	Listet die Speicher-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 Objekttyp und „1“ die Objekt-ID. Der Befehl listet alle Speicher-VMs innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an: `Name and Cluster ID.`
`um qtree list [-q] [ -ObjectType <object-id>]`	Listet die Qtrees nach dem Filtern nach dem angegebenen Objekt auf. -q ist für alle Befehle anwendbar, um keinen Header anzuzeigen. ObjectType kann LUN, Qtree, Cluster, Volume, Quota oder SVM sein. Beispiel: **`um qtree list -cluster 1`** In diesem Beispiel ist „-cluster“ der Objekttyp und „1“ die Objekt-ID. Der Befehl listet alle Qtrees innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte im Tabellenformat an: `Qtree ID and Qtree Name.`
`um disk list [-q] [-ObjectType <object-id>]`	Listet die Datenträger nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann Disk, Aggr, Node oder Cluster sein. Beispiel: **`um disk list -cluster 1`** In diesem Beispiel ist „-cluster“ der Objekttyp und „1“ die Objekt-ID. Der Befehl listet alle Festplatten innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in tabellarischer Form an `ObjectType and object-id.`

CLI-Befehl	Beschreibung	Ausgabe
`um cluster list [-q] [-ObjectType <object-id>]`	Listet die Cluster nach dem Filtern nach dem angegebenen Objekt 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 Objekttyp und „1“ die Objekt-ID. Der Befehl listet den Cluster auf, zu dem das Aggregat mit der ID 1 gehört.	Zeigt die folgenden Werte im Tabellenformat an: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.`
`um cluster node list [-q] [-ObjectType <object-id>]`	Listet die Clusterknoten nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann Disk, Aggr, Node oder Cluster sein. Beispiel: **`um cluster node list -cluster 1`** In diesem Beispiel ist „-cluster“ der Objekttyp und „1“ die Objekt-ID. Der Befehl listet alle Knoten innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in tabellarischer Form an `Name and Cluster ID.`
`um volume list [-q] [-ObjectType <object-id>]`	Listet die Datenträger nach dem Filtern nach dem angegebenen Objekt auf. ObjectType kann LUN, Qtree, Cluster, Volume, Quota, SVM oder Aggregat sein. Beispiel: **`um volume list -cluster 1`** In diesem Beispiel ist „-cluster“ der Objekttyp und „1“ die Objekt-ID. Der Befehl listet alle Volumes innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in tabellarischer Form an `Volume ID and Volume Name.`

CLI-Befehl	Beschreibung	Ausgabe
`um quota user list [-q] [-ObjectType <object-id>]`	Listet die Kontingentbenutzer 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 Objekttyp und „1“ die Objekt-ID. Der Befehl listet alle Kontingentbenutzer innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in tabellarischer Form an `ID, Name, SID and Email`.
`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 Objekttyp und „1“ die Objekt-ID. Der Befehl listet alle Aggregate innerhalb des Clusters mit der ID 1 auf.	Zeigt die folgenden Werte in tabellarischer Form an `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>`	Löst ein oder mehrere Ereignisse auf.	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 basierend auf Quelle, Status und IDs.	Zeigt die folgenden Werte in tabellarischer Form an `Source, Source type, Name, Severity, State, User and Timestamp`.

CLI-Befehl	Beschreibung	Ausgabe
`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

Auf der Seite „Skripte“ können Sie Unified Manager Skripte hinzufügen.

Seite „Skripte“

Auf der Seite „Skripte“ können Sie Ihre benutzerdefinierten Skripte zu Unified Manager hinzufügen. Sie können diese Skripte mit Warnungen verknüpfen, um die automatische Neukonfiguration von Speicherobjekten zu ermöglichen.

Auf der Seite „Skripte“ können Sie Skripte zum Unified Manager hinzufügen oder daraus löschen.

Befehlsschaltflächen

- **Hinzufügen**

  Zeigt das Dialogfeld „Skript hinzufügen“ an, in dem Sie Skripte hinzufügen können.

- **Löschen**

  Löscht das ausgewählte Skript.

Listenansicht

Die Listenansicht zeigt die Skripte, die Sie zu Unified Manager hinzugefügt haben, in tabellarischer Form an.

- **Name**

  Zeigt den Namen des Skripts an.

- **Beschreibung**

  Zeigt die Beschreibung des Skripts an.

Dialogfeld „Skript hinzufügen“

Über das Dialogfeld „Skript hinzufügen“ können Sie Unified Manager Skripte hinzufügen. Sie können mit Ihren Skripten Warnungen konfigurieren, um Ereignisse, die für Speicherobjekte generiert werden, automatisch aufzulösen.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

- **Skriptdatei auswählen**

  Ermöglicht Ihnen, ein Skript für die Warnung auszuwählen.

- **Beschreibung**

  Ermöglicht Ihnen, eine Beschreibung für das Skript anzugeben.

Überwachen und Verwalten der Clusterleistung

Einführung in die Leistungsüberwachung von Active IQ Unified Manager

Active IQ Unified Manager (früher OnCommand Unified Manager) bietet Leistungsüberwachungsfunktionen und Ereignisursachenanalyse für Systeme, auf denen NetApp ONTAP -Software ausgeführt wird.

Unified Manager hilft Ihnen, Workloads zu identifizieren, die Clusterkomponenten überbeanspruchen und die Leistung anderer Workloads im Cluster verringern. Durch die Definition von Richtlinien für Leistungsschwellenwerte können Sie auch Maximalwerte für bestimmte Leistungsindikatoren festlegen, sodass Ereignisse generiert werden, wenn der Schwellenwert überschritten wird. Unified Manager benachrichtigt Sie über diese Leistungsereignisse, sodass Sie Korrekturmaßnahmen ergreifen und die Leistung wieder auf das normale Betriebsniveau bringen können. Sie können Ereignisse in der Unified Manager-Benutzeroberfläche anzeigen und analysieren.

Unified Manager überwacht die Leistung von zwei Arten von Workloads:

- Benutzerdefinierte Workloads

  Diese Workloads bestehen aus FlexVol -Volumes und FlexGroup -Volumes, die Sie in Ihrem Cluster erstellt haben.

- Systemdefinierte Workloads

  Diese Arbeitslasten bestehen aus internen Systemaktivitäten.

Leistungsüberwachungsfunktionen von Unified Manager

Unified Manager sammelt und analysiert Leistungsstatistiken von Systemen, auf denen ONTAP -Software ausgeführt wird. Es verwendet dynamische Leistungsschwellenwerte und benutzerdefinierte Leistungsschwellenwerte, um eine Vielzahl von Leistungsindikatoren über viele Clusterkomponenten hinweg zu überwachen.

Eine hohe Antwortzeit (Latenz) weist darauf hin, dass das Speicherobjekt, beispielsweise ein Volume, langsamer als normal arbeitet. Dieses Problem weist auch darauf hin, dass die Leistung für Clientanwendungen, die das Volume verwenden, nachgelassen hat. Unified Manager identifiziert die Speicherkomponente, bei der das Leistungsproblem auftritt, und bietet eine Liste mit empfohlenen Maßnahmen zur Behebung des Leistungsproblems.

Unified Manager umfasst die folgenden Funktionen:

- Überwacht und analysiert Workload-Leistungsstatistiken eines Systems, auf dem ONTAP -Software ausgeführt wird.
- Verfolgt Leistungsindikatoren 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 (Reaktionszeit), Auslastung, Leistungskapazität und Cache-Verhältnis.

- Ermöglicht Ihnen die Erstellung benutzerdefinierter Richtlinien für Leistungsschwellenwerte, die Ereignisse auslösen und E-Mail-Benachrichtigungen senden, wenn die Schwellenwerte überschritten werden.
- Verwendet systemdefinierte Schwellenwerte und dynamische Leistungsschwellenwerte, die Ihre Workload-Aktivität erfassen, um Leistungsprobleme zu erkennen und Sie darauf aufmerksam zu machen.
- Identifiziert die Quality of Service-Richtlinien (QoS) und Performance Service Level-Richtlinien (PSLs), die auf Ihre Volumes und LUNs angewendet werden.
- Identifiziert eindeutig die Clusterkomponente, um die es geht.
- Identifiziert Workloads, die Clusterkomponenten übermäßig beanspruchen, und die Workloads, deren Leistung durch die erhöhte Aktivität beeinträchtigt wird.

Unified Manager-Schnittstellen zur Verwaltung der Speichersystemleistung

Diese Abschnitte enthalten Informationen zu den beiden Benutzeroberflächen, die Active IQ Unified Manager zur Behebung von Problemen mit der Datenspeicherkapazität, -verfügbarkeit und dem Schutz bereitstellt. Die beiden Benutzeroberflächen sind die Unified Manager-Webbenutzeroberfläche und die Wartungskonsole.

Wenn Sie die Schutzfunktionen in Unified Manager verwenden möchten, müssen Sie auch OnCommand Workflow Automation (WFA) installieren und konfigurieren.

Unified Manager-Web-Benutzeroberfläche

Über die Web-Benutzeroberfläche von Unified Manager kann ein Administrator Clusterprobleme im Zusammenhang mit der Datenspeicherkapazität, -verfügbarkeit und -sicherheit überwachen und beheben.

In diesen Abschnitten werden einige allgemeine Arbeitsabläufe beschrieben, die ein Administrator befolgen kann, um Probleme mit der Speicherkapazität, der Datenverfügbarkeit oder dem Schutz zu beheben, die in der Web-Benutzeroberfläche von Unified Manager angezeigt werden.

Wartungskonsole

Mit der Wartungskonsole von Unified Manager kann ein Administrator Betriebssystemprobleme, Probleme bei Versionsaktualisierungen, Probleme beim Benutzerzugriff und Netzwerkprobleme im Zusammenhang mit dem Unified Manager-Server selbst überwachen, diagnostizieren und beheben. Wenn die Web-Benutzeroberfläche von Unified Manager nicht verfügbar ist, ist die Wartungskonsole die einzige Möglichkeit, auf Unified Manager zuzugreifen.

Sie können diese Informationen verwenden, um auf die Wartungskonsole zuzugreifen und damit Probleme im Zusammenhang mit der Funktion des Unified Manager-Servers zu lösen.

Clusterkonfiguration und Leistungsdatenerfassungsaktivität

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-Benutzeroberfläche angezeigt werden. Dieses Intervall gilt auch bei Änderungen an einem Cluster.

Wenn Sie beispielsweise einem SVM in einem Cluster zwei neue Volumes hinzufügen, werden Ihnen diese neuen Objekte nach dem nächsten Abfrageintervall, das bis zu 15 Minuten dauern kann, in der Benutzeroberfläche angezeigt.

Unified Manager sammelt alle fünf Minuten aktuelle *Leistungsstatistiken* von allen überwachten Clustern. Es analysiert diese Daten, um Leistungsereignisse und potenzielle Probleme zu identifizieren. Es werden 30 Tage lang fünfminütige historische Leistungsdaten und 180 Tage lang einstündige historische Leistungsdaten gespeichert. Auf diese Weise können Sie sehr detaillierte Leistungsdetails für den aktuellen Monat und allgemeine Leistungstrends für bis zu ein Jahr anzeigen.

Die Erfassungsabfragen werden um einige Minuten versetzt, sodass die Daten nicht von allen Clustern gleichzeitig gesendet werden, was die Leistung beeinträchtigen könnte.

In der folgenden Tabelle werden die Erfassungsaktivitäten beschrieben, die Unified Manager durchführt:

Aktivität	Zeitintervall	Beschreibung
Umfrage zur Leistungsstatistik	Alle 5 Minuten	Sammelt Leistungsdaten in Echtzeit von jedem Cluster.
Statistische Analyse	Alle 5 Minuten	Nach jeder Statistikabfrage vergleicht Unified Manager die gesammelten Daten mit benutzerdefinierten, systemdefinierten und dynamischen Schwellenwerten. Wenn Leistungsschwellenwerte überschritten werden, generiert Unified Manager Ereignisse und sendet E-Mails an angegebene Benutzer, sofern dies entsprechend konfiguriert ist.
Konfigurationsumfrage	Alle 15 Minuten	Sammelt detaillierte Inventarinformationen von jedem Cluster, um alle Speicherobjekte (Knoten, SVMs, Volumes usw.) zu identifizieren.
Zusammenfassung	Stündlich	Fasst die letzten 12 fünfminütigen Leistungsdatenerfassungen zu Stundendurchschnitten zusammen. Die stündlichen Durchschnittswerte werden auf einigen UI-Seiten verwendet und 180 Tage lang gespeichert.

Aktivität	Zeitintervall	Beschreibung
Prognoseanalyse und Datenbereinigung	Jeden Tag nach Mitternacht	Analysiert Clusterdaten, um dynamische Schwellenwerte für die Volume-Latenz und IOPS für die nächsten 24 Stunden festzulegen. Löscht alle fünfminütigen Leistungsdaten, die älter als 30 Tage sind, aus der Datenbank.
Datenbereinigung	Jeden Tag nach 2 Uhr morgens	Löscht alle Ereignisse, die älter als 180 Tage sind, und alle dynamischen Schwellenwerte, die älter als 180 Tage sind, aus der Datenbank.
Datenbereinigung	Jeden Tag nach 3:30 Uhr	Löscht alle einstündigen Leistungsdaten aus der Datenbank, die älter als 180 Tage sind.

Was ein Datenkontinuitätserfassungszyklus ist

Ein Datenkontinuitätserfassungszyklus ruft Leistungsdaten außerhalb des Echtzeit-Clusterleistungserfassungszyklus ab, der standardmäßig alle fünf Minuten ausgeführt wird. Durch die Datenkontinuitätserfassung kann Unified Manager Lücken in statistischen Daten schließen, die auftreten, wenn keine Echtzeitdaten erfasst werden konnten.

Unified Manager führt Abfragen zur Datenkontinuitätserfassung historischer Leistungsdaten durch, wenn die folgenden Ereignisse eintreten:

- Zunächst wird ein Cluster zu Unified Manager hinzugefügt.

  Unified Manager sammelt historische Leistungsdaten der letzten 15 Tage. Auf diese Weise können Sie einige Stunden nach dem Hinzufügen eines Clusters die historischen Leistungsinformationen der letzten zwei Wochen anzeigen.

  Darüber hinaus werden systemdefinierte Schwellenwertereignisse für den vorherigen Zeitraum gemeldet, sofern solche vorhanden sind.

- Der aktuelle Zyklus zur Erfassung von Leistungsdaten wird nicht rechtzeitig abgeschlossen.

  Wenn die Echtzeit-Leistungsabfrage über den fünfminütigen Erfassungszeitraum hinausgeht, wird ein Datenkontinuitätserfassungszyklus eingeleitet, um die fehlenden Informationen zu erfassen. Ohne die Datenkontinuitätserfassung wird der nächste Erfassungszeitraum übersprungen.

- Unified Manager war für einen bestimmten Zeitraum nicht erreichbar und ist dann wieder online, beispielsweise in den folgenden Situationen:
  - Es wurde neu gestartet.
  - Es wurde während eines Software-Upgrades oder beim Erstellen einer Sicherungsdatei heruntergefahren.

    - Ein Netzwerkausfall wird behoben.
- Auf einen Cluster kann für einen bestimmten Zeitraum nicht zugegriffen werden, er wird dann aber wieder online geschaltet, beispielsweise in den folgenden Situationen:
    - Ein Netzwerkausfall wird behoben.
    - Eine langsame Weitverkehrsnetzverbindung verzögerte die normale Erfassung von Leistungsdaten.

Ein Datenkontinuitätserfassungszyklus kann maximal 24 Stunden historische Daten erfassen. Wenn Unified Manager länger als 24 Stunden ausfällt, erscheint auf den UI-Seiten eine Lücke in den Leistungsdaten.

Ein Datenkontinuitätserfassungszyklus und ein Echtzeitdatenerfassungszyklus können nicht gleichzeitig ausgeführt werden. Der Datenkontinuitätserfassungszyklus muss abgeschlossen sein, bevor mit der Erfassung der Echtzeitleistungsdaten begonnen wird. Wenn für die Datenkontinuitätserfassung mehr als eine Stunde historische Daten erfasst werden müssen, wird oben im Benachrichtigungsbereich eine Bannernachricht für diesen Cluster angezeigt.

Was der Zeitstempel in erfassten Daten und Ereignissen bedeutet

Der Zeitstempel, der in den erfassten Integritäts- und Leistungsdaten oder als Erkennungszeit für ein Ereignis angezeigt wird, basiert auf der ONTAP Clusterzeit, 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 Sie Zeitstempel sehen, die für einen bestimmten Cluster falsch erscheinen, sollten Sie überprüfen, ob die Clusterzeit richtig eingestellt wurde.

Navigieren Sie durch Leistungsworkflows in der Unified Manager-GUI

Die Unified Manager-Schnittstelle bietet viele Seiten zum Sammeln und Anzeigen von Leistungsinformationen. Sie verwenden das linke Navigationsfeld, um zu Seiten in der GUI zu navigieren, und Sie verwenden Registerkarten und Links auf den Seiten, um Informationen anzuzeigen und zu konfigurieren.

Sie verwenden alle folgenden Seiten, um Informationen zur Clusterleistung zu überwachen und Fehler zu beheben:

- Dashboard-Seite
- Seiten zum Speicher- und Netzwerkobjektinventar
- Detailseiten zu Speicherobjekten (einschließlich des Performance-Explorers)
- Konfigurations- und Setup-Seiten
- Veranstaltungsseiten

Melden Sie sich bei der Benutzeroberfläche an

Sie können sich mit einem unterstützten Webbrowser bei der Unified Manager-

Benutzeroberfläche anmelden.

Bevor Sie beginnen

- Der Webbrowser muss Mindestanforderungen erfüllen.

  Die Interoperabilitätsmatrix finden Sie unter "mysupport.netapp.com/matrix" für die vollständige Liste der unterstützten Browserversionen.

- Sie müssen über die IP-Adresse oder URL des Unified Manager-Servers verfügen.

Nach einer Stunde Inaktivität werden Sie automatisch von der Sitzung abgemeldet. Dieser Zeitraum kann unter **Allgemein** > **Funktionseinstellungen** konfiguriert werden.

Schritte

1. Geben Sie die URL in Ihren Webbrowser ein, wobei URL die IP-Adresse oder der vollqualifizierte Domänenname (FQDN) des Unified Manager-Servers ist:
   - 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 zur Serverauthentifizierung installieren. . Geben Sie auf dem Anmeldebildschirm Ihren Benutzernamen und Ihr Passwort ein.

Wenn die Anmeldung bei der Benutzeroberfläche von Unified Manager durch SAML-Authentifizierung geschützt ist, geben Sie Ihre Anmeldeinformationen auf der Anmeldeseite des Identitätsanbieters (IdP) und nicht auf der Anmeldeseite von Unified Manager ein.

Die Dashboard-Seite wird angezeigt.

Wenn der Unified Manager-Server nicht initialisiert ist, wird in einem neuen Browserfenster der Assistent für die erste Erfahrung angezeigt. Sie müssen einen ersten E-Mail-Empfänger eingeben, an den E-Mail-Benachrichtigungen gesendet werden, den SMTP-Server, der die E-Mail-Kommunikation abwickelt, und angeben, ob AutoSupport aktiviert ist, um Informationen über Ihre Unified Manager-Installation an den technischen Support zu senden. Nachdem Sie diese Informationen eingegeben haben, wird die Unified Manager-Benutzeroberfläche angezeigt.

Grafische Oberfläche und Navigationspfade

Unified Manager bietet große Flexibilität und ermöglicht Ihnen, mehrere Aufgaben auf unterschiedliche Weise zu erledigen. Bei der Arbeit mit Unified Manager werden Sie viele Navigationspfade entdecken. Obwohl nicht alle möglichen Navigationskombinationen angezeigt werden können, sollten Sie mit einigen der häufigeren Szenarien vertraut sein.

Überwachen Sie die Clusterobjektnavigation

Sie können die Leistung aller Objekte in jedem von Unified Manager verwalteten Cluster überwachen. Durch die Überwachung Ihrer Speicherobjekte erhalten Sie einen Überblick über die Cluster- und Objektleistung und können Leistungsereignisse überwachen. Sie

können Leistung und Ereignisse auf hoher Ebene anzeigen oder alle Details der Objektleistung und Leistungsereignisse genauer untersuchen.

Dies ist ein Beispiel für viele mögliche Clusterobjektnavigationen:

1. Überprüfen Sie auf der Dashboard-Seite die Details im Bereich „Leistungskapazität“, um den Cluster zu identifizieren, der die meiste Leistungskapazität nutzt, und klicken Sie auf das Balkendiagramm, um zur Liste der Knoten für diesen Cluster zu navigieren.
2. Identifizieren Sie den Knoten mit dem höchsten Wert für die genutzte Leistungskapazität und klicken Sie auf diesen Knoten.
3. Klicken Sie auf der Seite „Knoten-/Leistungs-Explorer“ im Menü „Anzeigen und Vergleichen“ auf „**Aggregate auf diesem Knoten**“.
4. Identifizieren Sie das Aggregat, das die meiste Leistungskapazität nutzt, und klicken Sie auf dieses Aggregat.
5. Klicken Sie auf der Seite „Aggregate/Performance Explorer“ im Menü „Anzeigen und Vergleichen“ auf **Volumes auf diesem Aggregat**.
6. Identifizieren Sie die Volumes, die die meisten IOPS verwenden.

Sie sollten diese Volumes untersuchen, um festzustellen, ob Sie eine QoS-Richtlinie oder eine Performance-Service-Level-Richtlinie anwenden oder die Richtlinieneinstellungen ändern sollten, damit diese Volumes keinen so großen Prozentsatz der IOPS auf dem Cluster verwenden.

Navigation zur Überwachung der Clusterleistung

Sie können die Leistung aller von Unified Manager verwalteten Cluster überwachen. Durch die Überwachung Ihrer Cluster erhalten Sie einen Überblick über die Cluster- und Objektleistung und können Leistungsereignisse überwachen. Sie können Leistung und Ereignisse auf hoher Ebene anzeigen oder alle Details der Cluster- und Objektleistung sowie der Leistungsereignisse genauer untersuchen.

Dies ist ein Beispiel für viele mögliche Navigationspfade zur Clusterleistung:

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.
2. Um Informationen zur Leistung in diesen Aggregaten anzuzeigen, wählen Sie die Ansicht „Leistung: Alle Aggregate“ aus.
3. Identifizieren Sie das Aggregat, das Sie untersuchen möchten, und klicken Sie auf den Aggregatnamen, um zur Seite „Aggregate/Performance Explorer“ zu navigieren.
4. Wählen Sie optional im Menü „Anzeigen und Vergleichen“ andere Objekte aus, die mit diesem Aggregat verglichen werden sollen, und fügen Sie dann eines der Objekte zum Vergleichsbereich hinzu.

   Statistiken für beide Objekte werden zum Vergleich in den Zählerdiagrammen angezeigt.

5. Klicken Sie im Vergleichsbereich rechts auf der Explorer-Seite in einem der Zählerdiagramme auf **Zoom-Ansicht**, um Details zum Leistungsverlauf für dieses Aggregat anzuzeigen.

Navigation zur Ereignisuntersuchung

Die Ereignisdetailseiten des Unified Managers bieten Ihnen einen detaillierten Einblick in jedes Leistungsereignis. Dies ist hilfreich bei der Untersuchung von Leistungsereignissen, bei der Fehlerbehebung und bei der Feinabstimmung der Systemleistung.

Je nach Art des Performance-Events wird Ihnen möglicherweise eine von zwei Arten von Event-Detailseiten angezeigt:

- Ereignisdetailseite für benutzerdefinierte und systemdefinierte Schwellenwertrichtlinienereignisse
- Ereignisdetailseite für dynamische Schwellenwertrichtlinienereignisse

Dies ist ein Beispiel für eine Ereignisuntersuchungsnavigation.

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.
2. Klicken Sie im Menü „Ansicht“ auf „Aktive Leistungsereignisse“.
3. Klicken Sie auf den Namen des Ereignisses, das Sie untersuchen möchten. Die Seite mit den Ereignisdetails wird angezeigt.
4. Sehen Sie sich die Beschreibung des Ereignisses an und überprüfen Sie die vorgeschlagenen Maßnahmen (sofern verfügbar), um weitere Details zum Ereignis anzuzeigen, die Ihnen bei der Lösung des Problems helfen können. Sie können auf die Schaltfläche **Arbeitslast analysieren** klicken, um detaillierte Leistungsdiagramme anzuzeigen, die Ihnen bei der weiteren Analyse des Problems helfen.

Suche nach Speicherobjekten

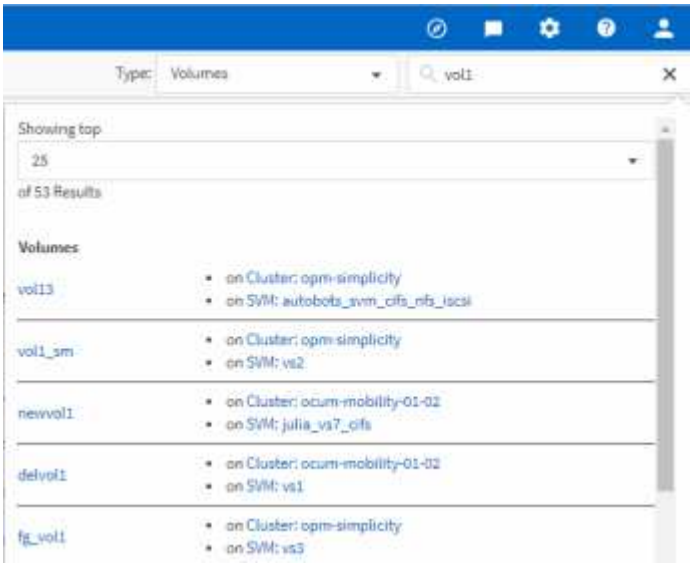
Um schnell auf ein bestimmtes Objekt zuzugreifen, können Sie das Feld **Alle Speicherobjekte durchsuchen** oben in der Menüleiste verwenden. Mit dieser Methode der globalen Suche über alle Objekte hinweg können Sie bestimmte Objekte schnell nach Typ finden. Die Suchergebnisse werden nach Speicherobjekttyp sortiert und Sie können sie mithilfe des Dropdown-Menüs filtern. Eine gültige Suche muss mindestens drei Zeichen enthalten.

Die globale Suche zeigt die Gesamtzahl der Ergebnisse an, es sind jedoch nur die ersten 25 Suchergebnisse zugänglich. Aus diesem Grund kann die globale Suchfunktion als ein Schnellzugriffstool zum Auffinden bestimmter Elemente betrachtet werden, wenn Sie wissen, welche Elemente Sie schnell finden möchten. Um vollständige Suchergebnisse zu erhalten, können Sie die Suche auf den Objektinventarseiten und die zugehörige Filterfunktion verwenden.

Sie können auf das Dropdown-Feld klicken und **Alle** auswählen, um gleichzeitig in allen Objekten und Ereignissen zu suchen. Alternativ können Sie auf das Dropdown-Feld klicken, um den Objekttyp anzugeben. Geben Sie mindestens drei Zeichen des Objekt- oder Ereignisnamens in das Feld **Alle Speicherobjekte durchsuchen** ein und drücken Sie dann die **Eingabetaste**, um die Suchergebnisse anzuzeigen, z. B.:

- Cluster: Clusternamen
- Knoten: Knotennamen
- Aggregate: Aggregatnamen
- SVMs: SVM-Namen

- Datenträger: Datenträgernamen
- LUNs: LUN-Pfade



LIFs und Ports können in der globalen Suchleiste nicht durchsucht werden.

In diesem Beispiel ist im Dropdown-Feld der Objekttyp „Volume“ ausgewählt. Wenn Sie „`vol`“ in das Feld **Alle Speicherobjekte durchsuchen** eingeben, wird eine Liste aller Volumes angezeigt, deren Namen diese Zeichen enthalten. Bei der Objektsuche können Sie auf ein beliebiges Suchergebnis klicken, um zur Performance Explorer-Seite dieses Objekts zu navigieren. Bei der Ereignissuche gelangen Sie durch Klicken auf ein Element im Suchergebnis zur Seite mit den Ereignisdetails.

Inhalt der Inventarseite filtern

Sie können die Daten der Inventarseite im Unified Manager filtern, um Daten anhand bestimmter Kriterien schnell zu finden. Mithilfe von Filtern können Sie den Inhalt der Unified Manager-Seiten eingrenzen und nur die Ergebnisse anzeigen, die Sie interessieren. Dies bietet eine sehr effiziente Methode, nur die Daten anzuzeigen, an denen Sie interessiert sind.

Verwenden Sie **Filtern**, um die Rasteransicht Ihren Wünschen entsprechend anzupassen. Die verfügbaren Filteroptionen basieren auf dem Objekttyp, der im Raster angezeigt wird. Wenn derzeit Filter angewendet werden, wird die Anzahl der angewendeten Filter rechts neben der Schaltfläche „Filter“ angezeigt.

Es werden drei Arten von Filterparametern unterstützt.

Parameter	Validierung
Zeichenfolge (Text)	Die Operatoren sind **enthält**, **beginnt mit**, **endet mit** und **enthält nicht**.
Anzahl	Die Operatoren sind **größer als**, **kleiner als**, **im letzten** und **zwischen**.

Parameter	Validierung
Aufzählung (Text)	Die Operatoren sind **ist** und **ist nicht**.

Die Felder „Spalte“, „Operator“ und „Wert“ sind für jeden Filter erforderlich. Die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. Sie können maximal vier Filter anwenden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten in Ihrer gefilterten Suche, nicht nur für die aktuell angezeigte Seite.

Sie können Filter über das Filterfeld hinzufügen.

1. Klicken Sie oben auf der Seite auf die Schaltfläche **Filter**. Das Filterfeld wird angezeigt.
2. Klicken Sie auf die linke Dropdown-Liste und wählen Sie ein Objekt aus, beispielsweise *Cluster* oder einen Leistungsindikator.
3. Klicken Sie auf die mittlere Dropdown-Liste und wählen Sie den Operator aus, den Sie verwenden möchten.
4. Wählen Sie in der letzten Liste einen Wert aus oder geben Sie ihn ein, um den Filter für dieses Objekt zu vervollständigen.
5. Um einen weiteren Filter hinzuzufügen, klicken Sie auf **+Filter hinzufügen**. Ein zusätzliches Filterfeld wird angezeigt. Vervollständigen Sie diesen Filter mit dem in den vorhergehenden Schritten beschriebenen Verfahren. Beachten Sie, dass nach dem Hinzufügen Ihres vierten Filters die Schaltfläche **+Filter hinzufügen** nicht mehr angezeigt wird.
6. Klicken Sie auf **Filter anwenden**. Die Filteroptionen werden auf das Raster angewendet und die Anzahl der Filter wird rechts neben der Schaltfläche „Filter“ angezeigt.
7. Verwenden Sie das Filterfeld, um einzelne Filter zu entfernen, indem Sie auf das Papierkorbsymbol rechts neben dem zu entfernenden Filter klicken.
8. Um alle Filter zu entfernen, klicken Sie unten im Filterbereich auf **Zurücksetzen**.

Filterbeispiel

Die Abbildung zeigt das Filterbedienfeld mit drei Filtern. Die Schaltfläche **+Filter hinzufügen** wird angezeigt, wenn Sie weniger als die maximal vier Filter haben.

Nachdem Sie auf **Filter anwenden** geklickt haben, wird das Filterfenster geschlossen, Ihre Filter werden angewendet und die Anzahl der angewendeten Filter wird angezeigt ( ).

Überwachen Sie die Clusterleistung vom Dashboard aus

Das Unified Manager-Dashboard bietet einige Bereiche, die den allgemeinen Leistungsstatus aller Cluster anzeigen, die von dieser Instanz von Unified Manager überwacht werden. Damit können Sie die Gesamtleistung der verwalteten Cluster beurteilen und alle identifizierten spezifischen Ereignisse schnell notieren, lokalisieren oder zur Lösung zuweisen.

Leistungsbereiche auf dem Dashboard verstehen

Das Unified Manager Dashboard bietet einige Bereiche, die den Leistungsstatus auf hoher Ebene für alle Cluster anzeigen, die in Ihrer Umgebung überwacht werden. Sie können den Status für alle Cluster oder für einen einzelnen Cluster anzeigen.

Zusätzlich zur Anzeige von Leistungsinformationen zeigen die meisten Panels auch die Anzahl der aktiven Ereignisse in dieser Kategorie und die Anzahl der in den letzten 24 Stunden hinzugefügten neuen Ereignisse an. Mithilfe dieser Informationen können Sie entscheiden, welche Cluster Sie möglicherweise weiter analysieren müssen, um gemeldete Ereignisse zu beheben. Wenn Sie auf die Ereignisse klicken, werden die wichtigsten Ereignisse angezeigt und ein Link zur Inventarseite der Ereignisverwaltung bereitgestellt, die gefiltert ist, um die Ereignisse in dieser Kategorie anzuzeigen.

Die folgenden Felder zeigen den Leistungsstatus an.

- **Leistungskapazitätspanel**

  Beim Anzeigen aller Cluster zeigt dieses Fenster den Leistungskapazitätswert für jeden Cluster (Durchschnittswert der letzten Stunde) und die Anzahl der Tage an, bis die Leistungskapazität die Obergrenze erreicht (basierend auf der täglichen Wachstumsrate). Durch Klicken auf das Balkendiagramm gelangen Sie zur Knotenbestandsseite für diesen Cluster. Beachten Sie, dass auf der Seite „Knoteninventar“ die durchschnittliche Leistungskapazität der letzten 72 Stunden angezeigt wird. Dieser Wert stimmt also möglicherweise nicht mit dem Dashboard-Wert überein.

  Beim Anzeigen eines einzelnen Clusters zeigt dieses Fenster die Leistungskapazität des Clusters, die gesamten IOPS und die Gesamtdurchsatzwerte an.

- **Workload-IOPS-Panel**

  Wenn die aktive Workloadverwaltung aktiviert ist und ein einzelner Cluster angezeigt wird, zeigt dieses Fenster die Gesamtzahl der Workloads an, die derzeit in einem bestimmten IOPS-Bereich ausgeführt werden.

- **Arbeitslastleistungspanel**

  Wenn die aktive Workload-Verwaltung aktiviert ist, wird in diesem Bereich die Gesamtzahl der konformen und nicht konformen Workloads angezeigt, die jedem definierten Performance-Service-Level zugewiesen sind. Durch Klicken auf ein Balkendiagramm gelangen Sie zu den dieser Richtlinie zugewiesenen Arbeitslasten auf der Seite „Arbeitslasten“.

- **Nutzungsübersicht**

  Wenn Sie alle Cluster anzeigen, können Sie die Cluster nach dem höchsten IOPS oder Durchsatz (MB/s) sortiert anzeigen.

  Wenn Sie einen einzelnen Cluster anzeigen, können Sie die Arbeitslasten auf diesem Cluster nach dem höchsten IOPS oder Durchsatz (MB/s) sortiert anzeigen.

Leistungsbannernachrichten und -beschreibungen

Unified Manager zeigt möglicherweise Bannernachrichten auf der Benachrichtigungsseite (von der Benachrichtigungsglocke aus) an, um Sie auf Statusprobleme für einen bestimmten Cluster aufmerksam zu machen.

Bannernachricht	Beschreibung	Auflösung
`No performance data is being collected from cluster cluster_name. Restart Unified Manager to correct this issue.`	Der Unified Manager-Sammeldienst wurde beendet und es werden keine Leistungsdaten von Clustern gesammelt.	Starten Sie Unified Manager neu, um dieses Problem zu beheben. Wenn das Problem dadurch nicht behoben wird, wenden Sie sich an den technischen Support.
`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 wird ein Datenkontinuitätserfassungszyklus ausgeführt, um Leistungsdaten außerhalb des Echtzeit-Clusterleistungserfassungszyklus abzurufen.	Es ist keine Aktion erforderlich. Aktuelle Leistungsdaten werden erfasst, nachdem der Datenkontinuitätserfassungszyklus abgeschlossen ist. Ein Datenkontinuitätserfassungszyklus wird ausgeführt, wenn ein neuer Cluster hinzugefügt wird oder wenn Unified Manager aus irgendeinem Grund keine aktuellen Leistungsdaten erfassen konnte.

Ändern des Erfassungsintervalls für Leistungsstatistiken

Das Standarderfassungsintervall für Leistungsstatistiken beträgt 5 Minuten. Sie können dieses Intervall auf 10 oder 15 Minuten ändern, wenn Sie feststellen, dass Sammlungen aus großen Clustern nicht innerhalb der Standardzeit abgeschlossen werden. Diese Einstellung wirkt sich auf die Erfassung von Statistiken aus allen Clustern aus, die diese Instanz von Unified Manager überwacht.

Bevor Sie beginnen

Sie müssen über eine Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.

Das Problem, dass die Erfassung von Leistungsstatistiken nicht rechtzeitig abgeschlossen wird, wird durch die Bannermeldungen angezeigt `Unable to consistently collect from cluster <cluster_name>` oder `Data collection is taking too long on cluster <cluster_name>`.

Sie sollten das Erfassungsintervall nur ändern, wenn dies aufgrund eines Problems bei der Statistikerfassung erforderlich ist. Ändern Sie diese Einstellung aus keinem anderen Grund.

> Das Ändern dieses Werts von der Standardeinstellung von 5 Minuten kann sich auf die Anzahl und Häufigkeit der von Unified Manager gemeldeten Leistungsereignisse auswirken. Beispielsweise lösen systemdefinierte Leistungsschwellenwerte Ereignisse aus, wenn die Richtlinie 30 Minuten lang überschritten wird. Bei der Verwendung von 5-Minuten-Sammlungen muss die Richtlinie bei sechs aufeinanderfolgenden Sammlungen überschritten werden. Bei 15-Minuten-Abholungen darf die Richtlinie nur für zwei Abholperioden überschritten werden.

Eine Meldung unten auf der Seite „Cluster-Setup“ gibt das aktuelle Intervall zur Erfassung statistischer Daten an.

Schritte

1. Melden Sie sich per SSH als Wartungsbenutzer beim Unified Manager-Host an.

   Die Eingabeaufforderungen der Unified Manager-Wartungskonsole werden angezeigt.

2. Geben Sie die Nummer der Menüoption mit der Bezeichnung **Konfiguration des Leistungsabfrageintervalls** ein und drücken Sie dann die Eingabetaste.
3. Geben Sie bei entsprechender Aufforderung das Wartungsbenutzerkennwort erneut ein.
4. Geben Sie die Zahl für das neue Abfrageintervall ein, das Sie festlegen möchten, und drücken Sie dann die Eingabetaste.

Wenn Sie das Erfassungsintervall des Unified Managers auf 10 oder 15 Minuten geändert haben und über eine aktuelle Verbindung zu einem externen Datenanbieter (z. B. Graphite) verfügen, müssen Sie das Übertragungsintervall des Datenanbieters so ändern, dass es gleich oder größer als das Erfassungsintervall des Unified Managers ist.

Beheben von Workload-Problemen mit dem Workload-Analyzer

Der Workload-Analysator bietet eine Möglichkeit, wichtige Integritäts- und Leistungskriterien für einen einzelnen Workload auf einer einzigen Seite anzuzeigen, um die Fehlerbehebung zu unterstützen. Durch die Anzeige aller aktuellen und vergangenen Ereignisse für eine Arbeitslast können Sie sich ein besseres Bild davon machen, warum bei der Arbeitslast derzeit möglicherweise ein Leistungs- oder Kapazitätsproblem vorliegt.

Mithilfe dieses Tools können Sie auch feststellen, ob der Speicher die Ursache für Leistungsprobleme einer Anwendung ist oder ob das Problem durch ein Netzwerkproblem oder ein anderes damit zusammenhängendes Problem verursacht wird.

Sie können diese Funktion von verschiedenen Stellen der Benutzeroberfläche aus starten:

- Über die Auswahl „Workload-Analyse“ im linken Navigationsmenü
- Klicken Sie auf der Seite mit den Ereignisdetails auf die Schaltfläche **Arbeitslast analysieren**
- Klicken Sie auf einer beliebigen Workload-Inventarseite (Volume, LUN, Workload, NFS-Freigabe oder SMB/CIFS-Freigabe) auf das Symbol „Mehr“ ⋮ , dann **Arbeitslast analysieren**
- Klicken Sie auf der Seite „Virtuelle Maschinen“ in einem beliebigen Datastore-Objekt auf die Schaltfläche „Arbeitslast analysieren“.

Wenn Sie das Tool über das linke Navigationsmenü starten, können Sie den Namen einer beliebigen Arbeitslast eingeben, die Sie analysieren möchten, und den Zeitraum auswählen, für den Sie die Fehlerbehebung durchführen möchten. Wenn Sie das Tool von einer der Workload- oder virtuellen Maschineninventarseiten aus starten, wird der Name des Workloads automatisch eingetragen und die Daten des Workloads werden im Standardzeitraum von 2 Stunden angezeigt. Wenn Sie das Tool von der Seite „Ereignisdetails“ aus starten, wird der Name der Arbeitslast automatisch eingetragen und die Daten der letzten 10 Tage angezeigt.

Welche Daten zeigt der Workload Analyzer an

Auf der Seite „Workload-Analysator“ werden Informationen zu allen aktuellen Ereignissen

angezeigt, die sich auf die Arbeitslast auswirken könnten, Empfehlungen zur möglichen Behebung des Problems, das das Ereignis verursacht hat, sowie Diagramme zur Analyse des Leistungs- und Kapazitätsverlaufs.

Oben auf der Seite geben Sie den Namen der Arbeitslast (Volume oder LUN) an, die Sie analysieren möchten, und den Zeitraum, für den Sie Statistiken anzeigen möchten. Sie können den Zeitrahmen jederzeit ändern, wenn Sie einen kürzeren oder längeren Zeitraum anzeigen möchten.

In den anderen Bereichen der Seite werden die Analyseergebnisse sowie die Leistungs- und Kapazitätsdiagramme angezeigt.

> Arbeitslastdiagramme für LUNs bieten nicht denselben Grad an Statistiken wie Diagramme für Volumes. Daher werden Sie bei der Analyse dieser beiden Arbeitslasttypen Unterschiede feststellen.

- **Bereich mit Ereigniszusammenfassung**

  Zeigt eine kurze Übersicht über die Anzahl und Art der Ereignisse an, die im Laufe des Zeitraums aufgetreten sind. Wenn Ereignisse aus unterschiedlichen Wirkungsbereichen (z. B. Leistung und Kapazität) vorliegen, werden diese Informationen angezeigt, sodass Sie Details für den Ereignistyp auswählen können, der Sie interessiert. Klicken Sie auf den Ereignistyp, um eine Liste der Ereignisnamen anzuzeigen.

  Wenn während des Zeitraums nur ein Ereignis auftritt, wird für einige Ereignisse eine Liste mit Empfehlungen zur Behebung des Problems aufgeführt.

- **Ereigniszeitleiste**

  Zeigt alle Ereignisse an, die während des angegebenen Zeitraums aufgetreten sind. Bewegen Sie den Cursor über jedes Ereignis, um den Ereignisnamen anzuzeigen.

  Wenn Sie auf dieser Seite gelandet sind, indem Sie auf der Seite mit den Ereignisdetails auf die Schaltfläche **Arbeitslast analysieren** geklickt haben, wird das Symbol für das ausgewählte Ereignis größer angezeigt, sodass Sie das Ereignis identifizieren können.

- **Bereich Leistungsdiagramme**

  Zeigt Diagramme für Latenz, Durchsatz (sowohl IOPS als auch MB/s) und Auslastung (sowohl für den Knoten als auch für das Aggregat) basierend auf dem von Ihnen ausgewählten Zeitrahmen an. Sie können auf den Link „Leistungsdetails anzeigen“ klicken, um die Seite „Performance Explorer“ für die Arbeitslast anzuzeigen, falls Sie weitere Analysen durchführen möchten.

  - **Latenz** zeigt die Latenz für die Arbeitslast über den ausgewählten Zeitraum an. Das Diagramm verfügt über drei Ansichten, die Ihnen Folgendes anzeigen:
    - **Gesamt** Latenz
    - **Aufschlüsselung** der Latenz (aufgeschlüsselt nach Lese-, Schreib- und anderen Prozessen)
    - **Clusterkomponenten** Latenz (aufgeschlüsselt nach Clusterkomponente)

Sehen"Clusterkomponenten und warum sie kontrovers diskutiert werden können" für eine Beschreibung der hier angezeigten Clusterkomponenten. **Durchsatz zeigt sowohl den IOPS- als auch den MB/s-Durchsatz für die Arbeitslast über den ausgewählten Zeitraum an. Das Diagramm verfügt über vier Ansichten, die Ihnen Folgendes anzeigen:** * **Gesamt**-Durchsatz *** Aufschlüsselung des Durchsatzes (aufgeschlüsselt nach Lese-, Schreib- und anderen Prozessen)** * **Cloud-Durchsatz** (die MB/s, die zum Schreiben und Lesen

von Daten in die Cloud verwendet werden; für jene Workloads, die die Kapazität in die Cloud einteilen) *** IOPS mit Prognose (eine Vorhersage der erwarteten oberen und unteren IOPS-Durchsatzwerte über den Zeitraum) Dieses Diagramm zeigt außerdem die maximalen und minimalen Durchsatzschwellenwerte für die Dienstgüte (QoS) an, sofern konfiguriert, sodass Sie sehen können, wo das System den Durchsatz möglicherweise absichtlich mit QoS-Richtlinien begrenzt. Auslastung** zeigt die Auslastung sowohl für das Aggregat als auch für den Knoten an, auf dem die Arbeitslast im ausgewählten Zeitraum ausgeführt wird. Von hier aus können Sie sehen, ob Ihr Aggregat oder Knoten überlastet ist, was möglicherweise zu einer hohen Latenz führt. Bei der Analyse von FlexGroup -Volumes werden in den Nutzungsdiagrammen mehrere Knoten und mehrere Aggregate aufgeführt.

- **Kapazitätsdiagrammbereich**

  Zeigt Diagramme zur Datenkapazität und Snapshot-Kapazität für den letzten Monat für die Arbeitslast an.

  Bei Volumes können Sie auf den Link „Kapazitätsdetails anzeigen“ klicken, um die Seite „Integritätsdetails“ für die Arbeitslast anzuzeigen, falls Sie weitere Analysen durchführen möchten. LUNs stellen diesen Link nicht bereit, da für LUNs keine Seite mit Integritätsdetails vorhanden ist.

  - **Kapazitätsansicht** zeigt den insgesamt verfügbaren Speicherplatz an, der für die Arbeitslast zugewiesen ist, und den logisch verwendeten Speicherplatz (nach allen NetApp Optimierungen).
  - **Snapshot-Ansicht** zeigt den gesamten für Snapshot-Kopien reservierten Speicherplatz und die aktuell verwendete Speicherplatzmenge an. Beachten Sie, dass LUNs keine Snapshot-Ansicht bereitstellen.
  - **Cloud Tier View** zeigt an, wie viel Kapazität in der lokalen Leistungsstufe und wie viel in der Cloud-Stufe verwendet wird. Diese Diagramme enthalten eine Schätzung der verbleibenden Zeit, bis die Kapazität für diese Arbeitslast erschöpft ist. Diese Informationen basieren auf der historischen Nutzung und erfordern Daten von mindestens 10 Tagen. Wenn weniger als 30 Tage Kapazität übrig sind, kennzeichnet Unified Manager den Speicher als „fast voll“.

Wann würde ich den Workload-Analyzer verwenden?

Normalerweise verwenden Sie den Workload-Analyzer, um ein von einem Benutzer gemeldetes Latenzproblem zu beheben, ein gemeldetes Ereignis oder eine Warnung gründlicher zu analysieren oder eine Workload zu untersuchen, die Ihrer Ansicht nach nicht normal funktioniert.

Falls Benutzer Sie kontaktiert haben und Ihnen mitteilen, dass die von ihnen verwendete Anwendung sehr langsam läuft, können Sie die Latenz-, Durchsatz- und Auslastungsdiagramme für die Arbeitslast überprüfen, mit der die Anwendung ausgeführt wird, um festzustellen, ob der Speicher die Ursache des Leistungsproblems ist. Sie können das Kapazitätsdiagramm auch verwenden, um zu sehen, ob die Kapazität niedrig ist, da ein ONTAP -System, dessen Kapazität zu über 85 % genutzt wird, Leistungsprobleme verursachen kann. Mithilfe dieser Diagramme können Sie feststellen, ob das Problem durch den Speicher, ein Netzwerkproblem oder ein anderes damit zusammenhängendes Problem verursacht wird.

Falls Unified Manager ein Leistungsereignis generiert hat und Sie die Ursache des Problems genauer untersuchen möchten, können Sie den Workload-Analysator von der Seite „Ereignisdetails“ aus starten, indem Sie auf die Schaltfläche „Workload analysieren“ klicken, um einige der Latenz-, Durchsatz- und Kapazitätstrends für die Workload zu untersuchen.

Falls Sie beim Anzeigen einer Workload-Inventarseite (Volume, LUN, Workload, NFS-Freigabe oder SMB/CIFS-Freigabe) feststellen, dass eine Workload nicht normal funktioniert, können Sie auf das Symbol „Mehr“ klicken. ⋮ und dann auf **Arbeitslast analysieren**, um die Seite „Arbeitslastanalyse“ zu öffnen und die Arbeitslast weiter zu untersuchen.

Verwenden des Workload-Analysators

Es gibt viele Möglichkeiten, den Workload-Analyzer über die Benutzeroberfläche zu starten. Hier beschreiben wir das Starten des Tools über den linken Navigationsbereich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Workload-Analyse**.

   Die Seite „Arbeitslastanalyse“ wird angezeigt.

2. Wenn Sie den Workload-Namen kennen, geben Sie ihn ein. Wenn Sie sich bezüglich des vollständigen Namens nicht sicher sind, geben Sie mindestens 3 Zeichen ein. Das System zeigt dann eine Liste der Workloads an, die mit der Zeichenfolge übereinstimmen.
3. Wählen Sie den Zeitraum aus, wenn Sie Statistiken für einen längeren Zeitraum als die standardmäßigen 2 Stunden anzeigen möchten, und klicken Sie auf **Übernehmen**.
4. Zeigen Sie den Bereich „Zusammenfassung“ an, um die Ereignisse anzuzeigen, die während des Zeitraums aufgetreten sind.
5. Sehen Sie sich die Leistungs- und Kapazitätsdiagramme an, um zu sehen, wann eine der Metriken abnormal ist, und um zu prüfen, ob Ereignisse mit dem abnormalen Eintrag übereinstimmen.

Überwachen Sie die Clusterleistung von der Zielseite des Leistungsclusters aus

Auf der Zielseite des Leistungsclusters wird der allgemeine Leistungsstatus eines ausgewählten Clusters angezeigt, der von einer Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die Gesamtleistung eines bestimmten Clusters beurteilen und erkannte clusterspezifische Ereignisse schnell notieren, lokalisieren oder zur Lösung zuweisen.

Die Zielseite des Performance-Clusters verstehen

Die Zielseite des Leistungsclusters bietet eine allgemeine Leistungsübersicht eines ausgewählten Clusters, wobei der Schwerpunkt auf dem Leistungsstatus der zehn wichtigsten Objekte innerhalb des Clusters liegt. Leistungsprobleme werden oben auf der Seite im Bereich „Alle Ereignisse in diesem Cluster“ angezeigt.

Die Zielseite des Performance-Clusters bietet einen allgemeinen Überblick über jeden Cluster, der von einer Instanz von Unified Manager verwaltet wird. Auf dieser Seite erhalten Sie Informationen zu Ereignissen und zur Leistung und können Cluster überwachen und Fehler beheben. Das folgende Bild zeigt ein Beispiel der Performance Cluster-Landingpage für den Cluster mit dem Namen opm-mobility:

Die Ereignisanzahl auf der Seite „Clusterzusammenfassung“ stimmt möglicherweise nicht mit der Ereignisanzahl auf der Seite „Leistungsereignisinventar“ überein. Dies liegt daran, dass auf der Seite „Clusterübersicht“ in den Latenz- und Auslastungsbalken jeweils ein Ereignis angezeigt werden kann, wenn Richtlinien für kombinierte Schwellenwerte verletzt wurden, während auf der Seite „Leistungsereignisinventar“ nur ein Ereignis angezeigt wird, wenn eine kombinierte Richtlinie verletzt wurde.

Wenn ein Cluster nicht mehr von Unified Manager verwaltet wird, wird oben auf der Seite rechts neben dem Clusternamen der Status **Entfernt** angezeigt.

Zielseite des Performance-Clusters

Auf der Zielseite des Leistungsclusters wird der allgemeine Leistungsstatus eines ausgewählten Clusters angezeigt. Auf der Seite können Sie auf alle Details jedes Leistungsindikators für die Speicherobjekte im ausgewählten Cluster zugreifen.

Die Zielseite des Performance-Clusters enthält vier Registerkarten, die die Clusterdetails in vier Informationsbereiche unterteilen:

- Zusammenfassungsseite
  - Bereich „Clusterereignisse“
  - MB/s- und IOPS-Leistungsdiagramme
  - Bereich „Verwaltete Objekte“
- Seite „Top-Performer“
- Explorer-Seite
- Informationsseite

Seite „Zusammenfassung des Leistungsclusters“

Die Seite „Leistungscluster-Zusammenfassung“ bietet eine Zusammenfassung der aktiven Ereignisse, der IOPS-Leistung und der MB/s-Leistung für einen Cluster. Diese Seite enthält auch die Gesamtzahl der Speicherobjekte im Cluster.

Bereich „Cluster-Leistungsereignisse“

Im Bereich „Cluster-Leistungsereignisse“ werden Leistungsstatistiken und alle aktiven Ereignisse für den Cluster angezeigt. Dies ist besonders hilfreich bei der Überwachung Ihrer Cluster und aller clusterbezogenen Leistungen und Ereignisse.

Alle Ereignisse in diesem Clusterbereich

Im Bereich „Alle Ereignisse in diesem Cluster“ werden alle aktiven Cluster-Leistungsereignisse der letzten 72 Stunden angezeigt. Ganz links wird die Gesamtzahl der aktiven Ereignisse angezeigt. Diese Zahl stellt die Summe aller neuen und bestätigten Ereignisse für alle Speicherobjekte in diesem Cluster dar. Sie können auf den Link „Gesamtzahl aktiver Ereignisse“ klicken, um zur Seite „Ereignisinventar“ zu navigieren, die gefiltert ist, um diese Ereignisse anzuzeigen.

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 (insgesamt für Cluster, Knoten, Aggregate, SVMs, Volumes, LUNs, Namespaces, Ports und LIFs)
- Ausgenutzte Leistungskapazität (Gesamt für Knoten und Aggregate)

- Auslastung (Gesamt für Knoten, Aggregate und Ports)
- Sonstiges (Cache-Fehlerquote für Volumes)

Die Liste enthält aktive Leistungsereignisse, die durch benutzerdefinierte Schwellenwertrichtlinien, systemdefinierte Schwellenwertrichtlinien und dynamische Schwellenwerte ausgelöst werden.

Diagrammdaten (vertikale Zählerbalken) werden in Rot angezeigt ( ) für kritische Ereignisse und Gelb ( ) für Warnereignisse. Positionieren Sie Ihren Cursor über jedem vertikalen Zählerbalken, um den tatsächlichen Typ und die Anzahl der Ereignisse anzuzeigen. Sie können auf **Aktualisieren** klicken, um die Zählerfelddaten zu aktualisieren.

Sie können kritische Ereignisse und Warnereignisse im Leistungsdiagramm „Gesamtzahl aktiver Ereignisse“ ein- oder ausblenden, indem Sie in der Legende auf die Symbole **Kritisch** und **Warnung** klicken. Wenn Sie bestimmte Ereignistypen ausblenden, werden die Legendensymbole grau angezeigt.

Thekenpaneele

Die Zählerfelder zeigen die Clusteraktivität und Leistungsereignisse der letzten 72 Stunden an und umfassen die folgenden Zähler:

- **IOPS-Zählerpanel**

  IOPS gibt die Betriebsgeschwindigkeit des Clusters in der Anzahl der Eingabe-/Ausgabevorgänge pro Sekunde an. Dieses Zählerfeld bietet einen allgemeinen Überblick über den IOPS-Zustand des Clusters für den vorangegangenen 72-Stunden-Zeitraum. Sie können Ihren Cursor über die Trendlinie des Diagramms positionieren, um den IOPS-Wert für einen bestimmten Zeitraum anzuzeigen.

- **MB/s-Zählerfeld**

  MB/s gibt an, wie viele Daten in Megabyte pro Sekunde zum und vom Cluster übertragen wurden. Dieses Zählerfeld bietet einen umfassenden Überblick über den MB/s-Zustand des Clusters für den vorangegangenen 72-Stunden-Zeitraum. Sie können Ihren Cursor über die Trendlinie des Diagramms positionieren, um den MB/s-Wert für einen bestimmten Zeitraum anzuzeigen.

Die Zahl oben rechts im Diagramm im grauen Balken ist der Durchschnittswert der letzten 72 Stunden. Die unten und oben im Trendliniendiagramm angezeigten Zahlen stellen die Mindest- und Höchstwerte für den letzten 72-Stunden-Zeitraum dar. Der graue Balken unter dem Diagramm enthält die Anzahl der aktiven (neuen und bestätigten) Ereignisse und veralteten Ereignisse aus dem letzten 72-Stunden-Zeitraum.

Die Zählertafeln enthalten zwei Arten von Ereignissen:

- **Aktiv**

  Zeigt an, dass das Leistungsereignis derzeit aktiv ist (neu oder bestätigt). Das Problem, das das Ereignis verursacht hat, hat sich nicht von selbst behoben oder wurde nicht gelöst. Der Leistungsindikator für das Speicherobjekt bleibt über dem Leistungsschwellenwert.

- **Veraltet**

  Zeigt an, dass das Ereignis nicht mehr aktiv ist. Das Problem, das das Ereignis verursacht hat, hat sich von selbst behoben oder wurde gelöst. Der Leistungsindikator für das Speicherobjekt liegt nicht mehr über dem Leistungsschwellenwert.

Bei **aktiven Ereignissen** können Sie, sofern es ein Ereignis gibt, den Cursor über das Ereignissymbol

bewegen und auf die Ereignisnummer klicken, um zur entsprechenden Seite mit den Ereignisdetails zu gelangen. Wenn mehr als ein Ereignis vorliegt, können Sie auf **Alle Ereignisse anzeigen** klicken, um die Seite „Ereignisinventar“ anzuzeigen, die so gefiltert ist, dass alle Ereignisse für den ausgewählten Objektzählertyp angezeigt werden.

Bereich „Verwaltete Objekte“

Der Bereich „Verwaltete Objekte“ auf der Registerkarte „Leistungsübersicht“ bietet eine Übersicht auf oberster Ebene über die Speicherobjekttypen und -anzahl für den Cluster. In diesem Bereich können Sie den Status der Objekte in jedem Cluster verfolgen.

Bei der Anzahl der verwalteten Objekte handelt es sich um Zeitpunktdaten aus dem letzten Erfassungszeitraum. Im 15-Minuten-Takt werden neue Objekte entdeckt.

Wenn Sie auf die verknüpfte Nummer für einen beliebigen Objekttyp klicken, wird die Seite mit dem Objektleistungsinventar für diesen Objekttyp angezeigt. Die Objektbestandsseite wird gefiltert, um nur die Objekte in diesem Cluster anzuzeigen.

Die verwalteten Objekte sind:

- **Knoten**

  Ein physisches System in einem Cluster.

- **Aggregate**

  Ein Satz mehrerer RAID-Gruppen (Redundant Array of Independent Disks), die zum Schutz und zur Bereitstellung als einzelne Einheit verwaltet werden können.

- **Anschlüsse**

  Ein physischer Verbindungspunkt auf Knoten, der zum Verbinden mit anderen Geräten in einem Netzwerk verwendet wird.

- **Speicher-VMs**

  Eine virtuelle Maschine, die Netzwerkzugriff über eindeutige Netzwerkadressen bereitstellt. Ein SVM kann Daten aus einem anderen Namespace bereitstellen und ist getrennt vom Rest des Clusters verwaltbar.

- **Bände**

  Eine logische Entität, die über eines oder mehrere der unterstützten Zugriffsprotokolle zugängliche Benutzerdaten enthält. Die Zählung umfasst sowohl FlexVol Volumes als auch FlexGroup -Volumes; sie umfasst keine FlexGroup Bestandteile.

- **LUNs**

  Die Kennung einer logischen Fibre Channel (FC)-Einheit oder einer logischen iSCSI-Einheit. Eine logische Einheit entspricht normalerweise einem Speichervolumen und wird innerhalb eines Computerbetriebssystems als Gerät dargestellt.

- **Netzwerkschnittstellen**

  Eine logische Netzwerkschnittstelle, die einen Netzwerkzugriffspunkt zu einem Knoten darstellt. Die Zählung umfasst alle Schnittstellentypen.

Seite „Top-Performer“

Auf der Seite „Top-Performer“ werden die Speicherobjekte angezeigt, die basierend auf dem von Ihnen ausgewählten Leistungsindikator die höchste oder die niedrigste Leistung aufweisen. Beispielsweise können Sie in der Kategorie „Storage-VMs“ die SVMs anzeigen, die die höchsten IOPS, die höchste Latenz oder die niedrigsten MB/s aufweisen. Auf dieser Seite wird auch angezeigt, ob einer der Top-Performer aktive Leistungsereignisse (neu oder anerkannt) hat.

Auf der Seite „Top-Performer“ werden maximal 10 Exemplare jedes Objekts angezeigt. Beachten Sie, dass das Volume-Objekt sowohl FlexVol Volumes als auch FlexGroup -Volumes enthält.

- **Zeitraum**

  Sie können einen Zeitraum für die Anzeige der Top-Performer auswählen. Der ausgewählte Zeitraum gilt für alle Speicherobjekte. Verfügbare Zeitbereiche:

  - Letzte Stunde
  - Letzte 24 Stunden
  - Letzte 72 Stunden (Standard)
  - Letzte 7 Tage

- **Metrisch**

  Klicken Sie auf das Menü **Metrik**, um einen anderen Zähler auszuwählen. Zähleroptionen sind für den Objekttyp eindeutig. Verfügbare Zähler für das Objekt **Volumes** sind beispielsweise **Latenz**, **IOPS** und **MB/s**. Durch Ändern des Zählers werden die Paneldaten mit den Leistungsträgern basierend auf dem ausgewählten Zähler neu geladen.

  Verfügbare Zähler:

  - Latenz
  - IOPS
  - MB/s
  - Verwendete Leistungskapazität (für Knoten und Aggregate)
  - Auslastung (für Knoten und Aggregate)

- **Sortieren**

  Klicken Sie auf das Menü **Sortieren**, um eine aufsteigende oder absteigende Sortierung für das ausgewählte Objekt und den ausgewählten Zähler auszuwählen. Die Optionen sind **Vom Höchsten zum Niedrigsten** und **Vom Niedrigsten zum Höchsten**. Mit diesen Optionen können Sie die Objekte mit der höchsten oder der niedrigsten Leistung anzeigen.

- **Thekenbar**

  Der Zählerbalken im Diagramm zeigt die Leistungsstatistiken für jedes Objekt, dargestellt als Balken für dieses Element. Die Balkendiagramme sind farbcodiert. Wenn der Zähler keinen Leistungsschwellenwert überschreitet, wird der Zählerbalken blau angezeigt. Wenn eine Grenzwertverletzung aktiv ist (ein neues oder bestätigtes Ereignis), wird der Balken in der Farbe des Ereignisses angezeigt: Warnereignisse werden in Gelb angezeigt ( ) und kritische Ereignisse werden in Rot angezeigt ( ). Grenzwertüberschreitungen werden außerdem durch Schweregradsymbole für Warnungen und kritische

Ereignisse angezeigt.

Für jedes Diagramm zeigt die X-Achse die Leistungsstärksten für den ausgewählten Objekttyp an. Auf der Y-Achse werden die für den ausgewählten Zähler geltenden Einheiten angezeigt. Durch Klicken auf den Objektnamen-Link unter jedem vertikalen Balkendiagrammelement gelangen Sie zur Performance-Landingpage für das ausgewählte Objekt.

- **Schweregrad-Ereignisindikator**

  Das Symbol für den Indikator **Schweregradereignis** wird links neben dem Objektnamen für aktive kritische Ereignisse angezeigt ( ) oder Warnung ( ) Ereignisse in den Diagrammen der Top-Performer. Klicken Sie auf das Indikatorsymbol **Schweregradereignis**, um Folgendes anzuzeigen:

  - **Ein Ereignis**

    Navigiert zur Seite mit den Veranstaltungsdetails für diese Veranstaltung.

  - **Zwei oder mehr Ereignisse**

    Navigiert zur Seite „Ereignisinventar“, die gefiltert ist, um alle Ereignisse für das ausgewählte Objekt anzuzeigen.

- **Exportieren-Schaltfläche**

  Erstellt eine `.csv` Datei, die die Daten enthält, die in der Zählerleiste angezeigt werden. Sie können die Datei entweder für den einzelnen Cluster erstellen, den Sie gerade anzeigen, oder für alle Cluster im Rechenzentrum.

Überwachen Sie die Leistung mithilfe der Leistungsinventarseiten

Auf den Leistungsseiten des Objektbestands werden Leistungsinformationen, Leistungsereignisse und der Objektzustand für alle Objekte innerhalb einer Objekttypkategorie angezeigt. Dadurch erhalten Sie auf einen Blick einen Überblick über den Leistungsstatus jedes Objekts innerhalb eines Clusters, beispielsweise für alle Knoten oder alle Volumes.

Die Leistungsseiten des Objektbestands bieten einen umfassenden Überblick über den Objektstatus und ermöglichen Ihnen die Bewertung der Gesamtleistung aller Objekte sowie den Vergleich von Objektleistungsdaten. Sie können den Inhalt der Objektinventarseiten durch Suchen, Sortieren und Filtern verfeinern. Dies ist bei der Überwachung und Verwaltung der Objektleistung von Vorteil, da Sie so schnell Objekte mit Leistungsproblemen finden und mit der Fehlerbehebung beginnen können.

Standardmäßig werden Objekte auf den Seiten des Leistungsinventars nach der Leistungskritikalität des Objekts sortiert. Objekte mit neuen kritischen Leistungsereignissen werden zuerst aufgeführt, Objekte mit Warnereignissen an zweiter Stelle. Dadurch wird sofort visuell angezeigt, welche Probleme behoben werden müssen. Alle Leistungsdaten basieren auf einem 72-Stunden-Durchschnitt.

Sie können ganz einfach von der Leistungsseite des Objektbestands zu einer Objektdetailseite navigieren, indem Sie in der Spalte „Objektname“ auf den Objektnamen klicken. Klicken Sie beispielsweise auf der Inventarseite „Leistung/Alle Knoten“ auf ein Knotenobjekt in der Spalte **Knoten**. Die Objektdetailseite bietet

ausführliche Informationen und Einzelheiten zum ausgewählten Objekt, einschließlich eines Nebeneinandervergleichs aktiver Ereignisse.

Anzeigen der Leistungsinventarseiten für alle Speicherobjekte

Auf den Seiten „Leistungsinventar“ können Sie eine Zusammenfassung der Leistungsinformationen zu jedem der verfügbaren Speicherobjekte wie Clustern, Aggregaten, Volumes usw. anzeigen. Sie können auf die Detailseiten der Leistungsobjekte verlinken, um ausführliche Informationen zu einem bestimmten Objekt anzuzeigen.

Standardmäßig werden Objekte auf den Ansichtsseiten nach der Ereigniskritikalität sortiert. Objekte mit kritischen Ereignissen werden zuerst aufgelistet, Objekte mit Warnereignissen an zweiter Stelle. Dadurch wird sofort visuell angezeigt, welche Probleme behoben werden müssen.

Sie können Daten von diesen Seiten in eine durch Kommas getrennte Wertedatei exportieren.(`.csv`)-Datei, Microsoft Excel-Datei(`.xlsx`), oder(`.pdf`) Dokument mithilfe der Schaltfläche **Berichte** und verwenden Sie dann die exportierten Daten zum Erstellen von Berichten. Darüber hinaus können Sie die Seite anpassen und dann mithilfe der Schaltfläche **Geplante Berichte** die Erstellung und regelmäßige E-Mail-Versendung eines Berichts planen.

Alle Felder auf diesen Seiten können in benutzerdefinierten Ansichten und Berichten verwendet werden. Einige der Felder sind mit verwandten Seiten verknüpft, die eine detailliertere Ansicht ermöglichen.

Leistung: Ansicht „Alle Cluster“

Die Ansicht „Leistung: Alle Cluster“ zeigt eine Übersicht der Leistungsereignisse, Daten und Konfigurationsinformationen für jeden Cluster an, der von einer Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die Leistung Ihrer Cluster überwachen und Leistungsprobleme und Schwellenwertereignisse beheben.

Sie können jedem Objekt auf den Objektinventarseiten mithilfe der Schaltflächen **Richtlinie für Leistungsschwellenwerte zuweisen** und **Richtlinie für Leistungsschwellenwerte löschen** Richtlinien für Leistungsschwellenwerte zuweisen oder Schwellenwertrichtlinien daraus löschen.

Im Folgenden sind einige wichtige Felder in der Ansicht „Leistung: Alle Cluster“ aufgeführt.

- Cluster-FQDN: Der vollqualifizierte Domänenname (FQDN) des Clusters.
- IOPS: Die Eingabe-/Ausgabevorgänge pro Sekunde im Cluster.
- MB/s: Der Durchsatz des Clusters, 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. Sie können die auf jedem Knoten installierte ONTAP Version in der Ansicht „Leistung: Alle Knoten“ anzeigen.

- Schwellenwertrichtlinie: Die benutzerdefinierte(n) Leistungsschwellenwertrichtlinie(n), die für dieses Speicherobjekt aktiv sind. Sie können den Cursor über Richtliniennamen mit Auslassungspunkten (…)

positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen „Richtlinie für Leistungsschwellenwerte zuweisen“ und „Richtlinie für Leistungsschwellenwerte löschen“ bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken.

Leistung: Ansicht „Alle Volumes“

Die Ansicht „Leistung: Alle Volumes“ zeigt eine Übersicht der Leistungsereignisse, Zählerdaten und Konfigurationsinformationen für jedes FlexVol volume und FlexGroup -Volume an, das von einer Instanz von Unified Manager überwacht wird. Auf diese Weise können Sie die Leistung Ihrer Volumes schnell überwachen und Leistungsprobleme und Schwellenwertereignisse beheben.

Wenn Sie die Latenz und den Durchsatz eines bestimmten Objekts analysieren möchten, klicken Sie auf die Schaltfläche „Weitere Optionen“ ⋮ Klicken Sie dann auf **Arbeitslast analysieren** und Sie können Leistungs- und Kapazitätsdiagramme auf der Seite „Arbeitslastanalyse“ anzeigen. Sie können die Details im System Manager anzeigen, sofern Sie über gültige Anmeldeinformationen für den System Manager verfügen.

ⓘ Bei Datenschutzvolumes (DP) werden nur Zählerwerte für benutzergenerierten Datenverkehr angezeigt. Stammvolumes werden auf dieser Seite nicht angezeigt.

Im Folgenden sind einige wichtige Felder in der Ansicht „Leistung: Alle Volumes“ aufgeführt.

- Stil: Entweder FlexVol oder FlexGroup.
- Latenz: Bei FlexVol -Volumes ist dies die durchschnittliche Antwortzeit des Volumes für alle E/A-Anfragen, ausgedrückt in Millisekunden pro Vorgang. Bei FlexGroup -Volumes ist dies die durchschnittliche Latenz aller Bestandteil-Volumes.
- IOPS/TB: Die Anzahl der pro Sekunde verarbeiteten Eingabe-/Ausgabevorgänge basierend auf dem gesamten Speicherplatz, der von der Arbeitslast verbraucht wird, in Terabyte. Dieser Zähler misst, wie viel Leistung mit einer bestimmten Speicherkapazität bereitgestellt werden kann.
- IOPS: Bei FlexVol -Volumes ist dies die Anzahl der Eingabe-/Ausgabevorgänge pro Sekunde für das Volume. Bei FlexGroup -Volumes ist dies die Summe der IOPS für alle Bestandteil-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 für alle Bestandteil-Volumes.
- Kapazitätsfelder: Freie und Gesamtkapazität in GiB.

Weitere Informationen finden Sie unter den folgenden Links:

- "Zuweisen von Leistungsschwellenwertrichtlinien zu Speicherobjekten"
- "Entfernen von Leistungsschwellenwertrichtlinien aus Speicherobjekten"
- "Von Unified Manager überwachte Workloadtypen"
- "Anzeigen der auf bestimmte Volumes oder LUNs angewendeten QoS-Richtliniengruppeneinstellungen"
- "Verstehen der Empfehlungen des Unified Managers zum Tiering von Daten in der Cloud"
- "Anzeigen von Leistungsdiagrammen zum Vergleichen von Volumes oder LUNs, die sich in derselben QoS-Richtliniengruppe befinden"

Leistung: Alle Aggregate anzeigen

Die Ansicht „Leistung: Alle Aggregate“ zeigt eine Übersicht der Leistungsereignisse, Daten und Konfigurationsinformationen für jedes Aggregat, das von einer Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die Leistung Ihrer Aggregate überwachen und Leistungsprobleme und

Schwellenwertereignisse beheben.

Im Folgenden sind einige wichtige Felder in der Ansicht „Leistung: Alle Aggregate“ aufgeführt.

- Typ: Der Typ des Aggregats:
  - Festplatte
  - Hybrid. Kombiniert HDDs und SSDs, aber Flash Pool wurde nicht aktiviert.
  - Hybrid (Flash-Pool). Kombiniert HDDs und SSDs und Flash Pool wurde aktiviert.
  - SSD
  - SSD (FabricPool). Kombiniert SSDs und eine Cloud-Ebene
  - Festplatte (FabricPool). Kombiniert HDDs und eine Cloud-Ebene
  - VMDisk (SDS). Virtuelle Festplatten innerhalb einer virtuellen Maschine
  - VMDisk (FabricPool). Kombiniert virtuelle Festplatten und eine Cloud-Ebene
  - LUN (FlexArray)
- Berichterstellung für inaktive Daten: Ob die Funktion zur Berichterstellung für inaktive Daten für dieses Aggregat aktiviert oder deaktiviert ist. Wenn diese Option aktiviert ist, wird auf den Volumes dieses Aggregats die Menge kalter Daten in der Ansicht „Leistung: Alle Volumes“ angezeigt. Der Wert in diesem Feld lautet „N/A“, wenn die ONTAP -Version die Meldung inaktiver Daten nicht unterstützt.
- Schwellenwertrichtlinie: Die benutzerdefinierte(n) Leistungsschwellenwertrichtlinie(n), die für dieses Speicherobjekt aktiv sind. Sie können den Cursor über Richtliniennamen mit Auslassungspunkten (…) positionieren, um den vollständigen Richtliniennamen oder die Liste der zugewiesenen Richtliniennamen anzuzeigen. Die Schaltflächen „Richtlinie für Leistungsschwellenwerte zuweisen“ und „Richtlinie für Leistungsschwellenwerte löschen“ bleiben deaktiviert, bis Sie ein oder mehrere Objekte auswählen, indem Sie auf die Kontrollkästchen ganz links klicken. Weitere Informationen finden Sie unter den folgenden Links:
- "Zuweisen von Leistungsschwellenwertrichtlinien zu Speicherobjekten"
- "Entfernen von Leistungsschwellenwertrichtlinien aus Speicherobjekten"

Leistung: Alle Knoten anzeigen

Die Ansicht „Leistung: Alle Knoten“ zeigt eine Übersicht der Leistungsereignisse, Daten und Konfigurationsinformationen für jeden Knoten, der von einer Instanz von Unified Manager überwacht wird. Auf diese Weise können Sie die Leistung Ihrer Knoten schnell überwachen und Leistungsprobleme und Schwellenwertereignisse beheben.

> „Flash Cache Reads“ gibt den Prozentsatz der Lesevorgänge auf dem Knoten zurück, die vom Cache ausgeführt werden, anstatt von der Festplatte zurückgegeben zu werden. Flash-Cache-Daten werden nur für Knoten angezeigt und nur, wenn im Knoten ein Flash-Cache-Modul installiert ist.

Im Menü **Berichte** wird die Option **Hardwareinventarbericht** bereitgestellt, wenn Unified Manager und die von ihm verwalteten Cluster an einem Standort ohne externe Netzwerkverbindung installiert sind. Diese Schaltfläche generiert eine CSV-Datei, die eine vollständige Liste der Cluster- und Knoteninformationen enthält, z. B. Hardwaremodellnummern und Seriennummern, Datenträgertypen und -anzahl, installierte Lizenzen und mehr. Diese Berichtsfunktion ist hilfreich für die Vertragsverlängerung an sicheren Standorten, die nicht mit der NetApp Active IQ Plattform verbunden sind. Sie können jedem Objekt auf den Objektinventarseiten mithilfe der Schaltflächen **Richtlinie für Leistungsschwellenwerte zuweisen** und **Richtlinie für Leistungsschwellenwerte löschen** Richtlinien für Leistungsschwellenwerte zuweisen oder

Schwellenwertrichtlinien daraus löschen.

Weitere Informationen finden Sie unter den folgenden Links:

- "Zuweisen von Leistungsschwellenwertrichtlinien zu Speicherobjekten"
- "Entfernen von Leistungsschwellenwertrichtlinien aus Speicherobjekten"
- "Erstellen eines Hardware-Inventarberichts zur Vertragsverlängerung"

Leistung: Alle Storage-VMs anzeigen

Die Ansicht „Leistung: Alle Speicher-VMs“ zeigt eine Übersicht der Leistungsereignisse, Daten und Konfigurationsinformationen für jede Speicher-VM (SVM), die von einer Instanz von Unified Manager überwacht wird. Auf diese Weise können Sie die Leistung Ihrer SVMs schnell überwachen und Leistungsprobleme und Schwellenwertereignisse beheben. Das Feld „Latenz“ auf dieser Seite gibt die durchschnittliche Antwortzeit für alle E/A-Anfragen an, ausgedrückt in Millisekunden pro Vorgang.

Die auf dieser Seite aufgeführten SVMs umfassen nur Daten- und Cluster-SVMs. Unified Manager verwendet oder zeigt keine Admin- oder Node-SVMs an.

Weitere Informationen finden Sie unter den folgenden Links:

- "Zuweisen von Leistungsschwellenwertrichtlinien zu Speicherobjekten"
- "Entfernen von Leistungsschwellenwertrichtlinien aus Speicherobjekten"

Leistung: Alle LUNs anzeigen

Die Ansicht „Leistung: Alle LUNs“ zeigt eine Übersicht der Leistungsereignisse, Daten und Konfigurationsinformationen für jede LUN, die von einer Instanz von Unified Manager überwacht wird. Auf diese Weise können Sie die Leistung Ihrer LUNs schnell überwachen und Leistungsprobleme und Schwellenwertereignisse beheben.

Wenn Sie die Latenz und den Durchsatz eines bestimmten Objekts analysieren möchten, klicken Sie auf das Symbol „Mehr“ , dann **Arbeitslast analysieren** und Sie können Leistungs- und Kapazitätsdiagramme auf der Seite **Arbeitslastanalyse** anzeigen.

Weitere Informationen finden Sie unter den folgenden Links:

- "Überwachen von LUNs in einer Konsistenzgruppenbeziehung"
- "Bereitstellung von LUNs"
- "Zuweisen von Leistungsschwellenwertrichtlinien zu Speicherobjekten"
- "Entfernen von Leistungsschwellenwertrichtlinien aus Speicherobjekten"
- "Anzeigen von Volumes oder LUNs, die sich in derselben QoS-Richtliniengruppe befinden".
- "Anzeigen der auf bestimmte Volumes oder LUNs angewendeten QoS-Richtliniengruppeneinstellungen"
- "Bereitstellung von LUNs mithilfe von APIs"

Leistung: Alle NVMe-Namespaces anzeigen

Die Ansicht „Leistung: Alle NVMe-Namespaces“ zeigt eine Übersicht der Leistungsereignisse, Daten und Konfigurationsinformationen für jeden NVMe-Namespace, der von einer Instanz von Unified Manager überwacht wird. Auf diese Weise können Sie die Leistung und Integrität Ihrer Namespaces schnell überwachen

und Probleme und Schwellenwertereignisse beheben.

Gemeldet werden unter anderem folgende Informationen: Der aktuelle Status des Namespace. * Offline – Lese- oder Schreibzugriff auf den Namespace ist nicht zulässig. * Online – Lese- und Schreibzugriff auf den Namespace ist erlaubt. * NVFail – Der Namespace wurde aufgrund eines NVRAM Fehlers automatisch offline genommen. * Speicherplatzfehler – Der Namespace hat keinen Speicherplatz mehr.

Weitere Informationen finden Sie unter den folgenden Links:

- "Zuweisen von Leistungsschwellenwertrichtlinien zu Speicherobjekten"
- "Entfernen von Leistungsschwellenwertrichtlinien aus Speicherobjekten"

Leistung: Ansicht „Alle Netzwerkschnittstellen“

Die Ansicht „Leistung: Alle Netzwerkschnittstellen“ zeigt eine Übersicht der Leistungsereignisse, Daten und Konfigurationsinformationen für jede Netzwerkschnittstelle (LIF), die von dieser Instanz von Unified Manager überwacht wird. Auf dieser Seite können Sie die Leistung Ihrer Schnittstellen schnell überwachen und Leistungsprobleme und Schwellenwertereignisse beheben. Im Folgenden sind einige wichtige Felder in der Ansicht „Leistung: Alle Netzwerkschnittstellen“ aufgeführt.

- IOPS: Die Eingabe-/Ausgabevorgänge pro Sekunde. IOPS ist nicht auf NFS-LIFs und CIFS-LIFs anwendbar und wird für diese Typen als N/A angezeigt.
- Latenz: Die durchschnittliche Antwortzeit für alle E/A-Anfragen, ausgedrückt in Millisekunden pro Vorgang. Die Latenz gilt nicht für NFS-LIFs und CIFS-LIFs und wird für diese Typen als N/A angezeigt.
- Heimatstandort: Der Heimatstandort der Schnittstelle, angezeigt als Knotenname und Portname, getrennt durch einen Doppelpunkt (:). Wenn der Standort mit Auslassungspunkten (…) angezeigt wird, können Sie den Cursor über den Standortnamen bewegen, um den vollständigen Standort anzuzeigen.
- Aktueller Standort: Der aktuelle Standort der Schnittstelle, angezeigt als Knotenname und Portname, getrennt durch einen Doppelpunkt (:). Wenn der Standort mit Auslassungspunkten (…) angezeigt wird, können Sie den Cursor über den Standortnamen bewegen, um den vollständigen Standort anzuzeigen.
- Rolle: Die Schnittstellenrolle: Daten, Cluster, Knotenverwaltung oder Intercluster.

Zu den auf dieser Seite aufgeführten Schnittstellen gehören Data LIFs, Cluster LIFs, Node Management LIFs und Intercluster LIFs. Unified Manager verwendet oder zeigt keine System-LIFs an.

Leistung: Alle Ports anzeigen

Die Ansicht „Leistung: Alle Ports“ zeigt eine Übersicht der Leistungsereignisse, Daten und Konfigurationsinformationen für jeden Port, der von einer Instanz von Unified Manager überwacht wird. Auf diese Weise können Sie die Leistung Ihrer Ports schnell überwachen und Leistungsprobleme und Schwellenwertereignisse beheben. Für eine Portrolle wird die Netzwerkportfunktion angezeigt, entweder Daten oder Cluster. FCP-Ports können keine Rolle haben und die Rolle wird als N/A angezeigt.

Leistungsindikatorwerte werden nur für physische Ports angezeigt. Für VLANs oder Schnittstellengruppen werden keine Zählerwerte angezeigt.

Weitere Informationen finden Sie unter den folgenden Links:

- "Zuweisen von Leistungsschwellenwertrichtlinien zu Speicherobjekten"
- "Entfernen von Leistungsschwellenwertrichtlinien aus Speicherobjekten"

Leistung: Ansicht „QoS-Richtliniengruppen“

In der Ansicht „QoS-Richtliniengruppen“ werden die QoS-Richtliniengruppen angezeigt, die auf den von Unified Manager überwachten Clustern verfügbar sind. Dazu gehören herkömmliche QoS-Richtlinien, adaptive QoS-Richtlinien und QoS-Richtlinien, die mithilfe von Performance Service Levels zugewiesen werden.

Im Folgenden sind einige wichtige Felder in der Ansicht „Leistung: QoS-Richtliniengruppen“ aufgeführt.

- QoS-Richtliniengruppe: Der Name der QoS-Richtliniengruppe. 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 andere Informationen, die nicht im Namen enthalten waren, als das Performance Service Level in NSLM definiert wurde. Beispielsweise bedeutet der Name „NSLM_vs6_Performance_2_0“, dass dies die systemdefinierte PSL-Richtlinie „Performance“ von NSLM ist, die auf SVM „vs6“ mit einer erwarteten Latenz von „2 ms/op“ erstellt wurde.
- SVM: Die Speicher-VM (SVM), zu der die QoS-Richtliniengruppe gehört. Sie können auf den Namen der Speicher-VM klicken, um zur Detailseite dieser Speicher-VM zu navigieren. Beachten Sie, dass dieses Feld leer ist, wenn die QoS-Richtlinie auf der Admin-Speicher-VM erstellt wurde, da dieser Speicher-VM-Typ den Cluster darstellt.
- Min. Durchsatz: Der Mindestdurchsatz in IOPS, den die Richtliniengruppe garantiert bereitstellen wird. Bei adaptiven Richtlinien ist dies der minimal erwartete IOPS pro TB, der dem Volume oder LUN zugewiesen ist, basierend auf der zugewiesenen Größe des Speicherobjekts.
- Max. 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 Durchgang unendlich ist. Bei adaptiven Richtlinien ist dies der maximal (Spitzen-)IOPS pro TB, der dem Volume oder LUN zugewiesen ist, basierend entweder auf der zugewiesenen Größe des Speicherobjekts oder der verwendeten Größe des Speicherobjekts.
- Absolutes IOPS-Minimum: Bei adaptiven Richtlinien ist dies der absolute IOPS-Minimumwert, der als Außerkraftsetzung verwendet wird, wenn das erwartete IOPS unter diesem Wert liegt.
- Blockgröße: Die für die adaptive QoS-Richtlinie angegebene Blockgröße.
- Min. Zuweisung: Ob „zugewiesener Speicherplatz“ oder „verwendeter Speicherplatz“ zur Bestimmung des maximalen Durchsatzes (Spitzen-IOPS) verwendet wird.
- Erwartete Latenz: Die erwartete durchschnittliche Latenz für Speichereingabe-/-ausgabevorgänge.
- Geteilt: Bei herkömmlichen QoS-Richtlinien, ob die in der Richtliniengruppe definierten Durchsatzwerte von mehreren Objekten gemeinsam genutzt werden.
- Zugehörige Objekte: Die Anzahl der Workloads, die der QoS-Richtliniengruppe zugewiesen sind. Sie können auf die Schaltfläche „Erweitern“ (⌄) neben dem Namen der QoS-Richtliniengruppe, um weitere Details zur Richtliniengruppe anzuzeigen.
- Zugewiesene Kapazität: Die Menge an Speicherplatz, die die Objekte in der QoS-Richtliniengruppe derzeit verwenden.
- Zugehörige Objekte: Die Anzahl der Workloads, die der QoS-Richtliniengruppe zugewiesen sind, aufgeteilt in Volumes und LUNs. Sie können auf die Nummer klicken, um zu einer Seite zu navigieren, die weitere Details zu den ausgewählten Volumes oder LUNs bereitstellt.

Weitere Informationen finden Sie in den Themen unter"Verwalten der Leistung mithilfe von QoS-Richtliniengruppeninformationen" .

Verfeinern des Inhalts der Performance-Inventarseite

Die Inventarseiten für Leistungsobjekte enthalten Tools, mit denen Sie den Inhalt der

Objektinventardaten verfeinern können, sodass Sie bestimmte Daten schnell und einfach finden können.

Die auf den Inventarseiten des Leistungsobjekts enthaltenen Informationen können umfangreich sein und sich oft über mehrere Seiten erstrecken. Diese Art umfassender Daten eignet sich hervorragend zum Überwachen, Verfolgen und Verbessern der Leistung. Zum Auffinden spezifischer Daten sind jedoch Tools erforderlich, mit denen Sie die gesuchten Daten schnell finden können. Daher enthalten die Inventarseiten der Leistungsobjekte Funktionen zum Suchen, Sortieren und Filtern. Darüber hinaus können Sie durch Suchen und Filtern Ihre Ergebnisse weiter eingrenzen.

Suche auf den Seiten zur Objektinventarleistung

Sie können auf den Seiten zur Objektinventarleistung nach Zeichenfolgen suchen. Verwenden Sie das Suchfeld oben rechts auf der Seite, um Daten schnell anhand des Objektnamens oder des Richtliniennamens zu finden. Auf diese Weise können Sie schnell bestimmte Objekte und die zugehörigen Daten finden oder Richtlinien schnell finden und zugehörige Richtlinienobjektdaten anzeigen.

Schritt

1. Führen Sie je nach Ihren Suchanforderungen eine der folgenden Optionen aus:

So finden Sie dies …	Geben Sie Folgendes ein…
Ein bestimmtes Objekt	Geben Sie den Objektnamen in das Feld **Suchen** ein und klicken Sie auf **Suchen**. Das gesuchte Objekt und die zugehörigen Daten werden angezeigt.
Eine benutzerdefinierte Leistungsschwellenrichtlinie	Geben Sie den gesamten oder einen Teil des Richtliniennamens in das Feld **Suchen** ein und klicken Sie auf **Suchen**. Es werden die Objekte angezeigt, die der gesuchten Richtlinie zugeordnet sind.

Sortieren auf den Seiten zur Objektinventarleistung

Sie können alle Daten auf den Seiten zur Objektinventarleistung nach jeder Spalte in aufsteigender oder absteigender Reihenfolge sortieren. Auf diese Weise können Sie schnell Objektinventardaten finden, was bei der Leistungsprüfung oder beim Beginn eines Fehlerbehebungsprozesses hilfreich ist.

Die zum Sortieren ausgewählte Spalte wird durch einen hervorgehobenen Spaltennamen und ein Pfeilsymbol angezeigt, das rechts neben dem Namen die Sortierrichtung angibt. Ein Aufwärtspfeil zeigt eine aufsteigende Reihenfolge an, ein Abwärtspfeil eine absteigende Reihenfolge. Die Standardsortierreihenfolge ist nach **Status** (Ereigniskritikalität) in absteigender Reihenfolge, wobei die kritischsten Leistungsereignisse zuerst aufgeführt werden.

Schritt

1. Sie können auf einen Spaltennamen klicken, um die Sortierreihenfolge der Spalte in aufsteigender oder absteigender Reihenfolge umzuschalten.

Der Inhalt der Seite „Objektbestandsleistung“ wird basierend auf der ausgewählten Spalte in aufsteigender oder absteigender Reihenfolge sortiert.

Filtern Sie Daten auf den Seiten zur Objektbestandsleistung

Sie können Daten auf den Seiten zur Objektbestandsleistung filtern, um Daten anhand bestimmter Kriterien schnell zu finden. Mithilfe von Filtern können Sie den Inhalt der Seiten zur Objektinventarleistung eingrenzen und nur die von Ihnen angegebenen Ergebnisse anzeigen. Dies bietet eine sehr effiziente Methode, nur die Leistungsdaten anzuzeigen, die Sie interessieren.

Sie können das Filterfeld verwenden, um die Rasteransicht nach Ihren Wünschen anzupassen. Die verfügbaren Filteroptionen basieren auf dem Objekttyp, der im Raster angezeigt wird. Wenn derzeit Filter angewendet werden, wird die Anzahl der angewendeten Filter rechts neben der Schaltfläche „Filter“ angezeigt.

Es werden drei Arten von Filterparametern unterstützt.

Parameter	Validierung
Zeichenfolge (Text)	Die Operatoren sind **enthält**, **beginnt mit**, **endet mit** und **enthält nicht**.
Anzahl	Die Operatoren sind **größer als**, **kleiner als**, **im letzten** und **zwischen**.
Aufzählung (Text)	Die Operatoren sind **ist** und **ist nicht**.

Die Felder „Spalte“, „Operator“ und „Wert“ sind für jeden Filter erforderlich. Die verfügbaren Filter spiegeln die filterbaren Spalten auf der aktuellen Seite wider. Sie können maximal vier Filter anwenden. Gefilterte Ergebnisse basieren auf kombinierten Filterparametern. Gefilterte Ergebnisse gelten für alle Seiten in Ihrer gefilterten Suche, nicht nur für die aktuell angezeigte Seite.

Sie können Filter über das Filterfeld hinzufügen.

1. Klicken Sie oben auf der Seite auf die Schaltfläche **Filter**. Das Filterfeld wird angezeigt.
2. Klicken Sie auf die linke Dropdown-Liste und wählen Sie ein Objekt aus, beispielsweise *Cluster* oder einen Leistungsindikator.
3. Klicken Sie auf die mittlere Dropdown-Liste und wählen Sie den Operator aus, den Sie verwenden möchten.
4. Wählen Sie in der letzten Liste einen Wert aus oder geben Sie ihn ein, um den Filter für dieses Objekt zu vervollständigen.
5. Um einen weiteren Filter hinzuzufügen, klicken Sie auf **+Filter hinzufügen**. Ein zusätzliches Filterfeld wird angezeigt. Vervollständigen Sie diesen Filter mit dem in den vorhergehenden Schritten beschriebenen Verfahren. Beachten Sie, dass nach dem Hinzufügen Ihres vierten Filters die Schaltfläche **+Filter hinzufügen** nicht mehr angezeigt wird.
6. Klicken Sie auf **Filter anwenden**. Die Filteroptionen werden auf das Raster angewendet und die Anzahl der Filter wird rechts neben der Schaltfläche „Filter“ angezeigt.
7. Verwenden Sie das Filterfeld, um einzelne Filter zu entfernen, indem Sie auf das Papierkorbsymbol rechts neben dem zu entfernenden Filter klicken.

8. Um alle Filter zu entfernen, klicken Sie unten im Filterbereich auf **Zurücksetzen**.

Filterbeispiel

Die Abbildung zeigt das Filterbedienfeld mit drei Filtern. Die Schaltfläche **+Filter hinzufügen** wird angezeigt, wenn Sie weniger als die maximal vier Filter haben.

Nachdem Sie auf **Filter anwenden** geklickt haben, wird das Filterfenster geschlossen, Ihre Filter werden angewendet und die Anzahl der angewendeten Filter wird angezeigt (3).

Informieren Sie sich über die Empfehlungen des Unified Managers zur Datenschichtung in der Cloud.

In der Ansicht „Leistung: Alle Volumes“ werden Informationen zur Größe der Benutzerdaten angezeigt, die auf dem inaktiven (kalten) Volume gespeichert sind. In einigen Fällen identifiziert Unified Manager bestimmte Volumes, die von einer Auslagerung der inaktiven Daten in die Cloud-Ebene (Cloud-Anbieter oder StorageGRID) eines FabricPool-fähigen 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. Darüber hinaus **`auto`** Die Tiering-Richtlinie wurde in ONTAP 9.4 eingeführt, und die **`all`** Die Tiering-Richtlinie wurde in ONTAP 9.6 eingeführt. Wenn also die Verwendung der Auto-Tiering-Richtlinie empfohlen wird, müssen Sie auf ONTAP 9.4 oder höher aktualisieren.

Die folgenden drei Felder in der Ansicht „Leistung: Alle Volumes“ bieten Informationen darüber, ob Sie die Festplattenauslastung Ihres Speichersystems verbessern und Speicherplatz auf der Leistungsebene sparen können, indem Sie inaktive Daten in die Cloudebene verschieben.

- **Stufenrichtlinie**

  Die Tiering-Richtlinie bestimmt, ob die Daten auf dem Volume auf der Leistungsebene verbleiben oder ob einige der Daten von der Leistungsebene in die Cloudebene verschoben werden.

  Der Wert in diesem Feld gibt die für das Volume festgelegte Tiering-Richtlinie an, auch wenn sich das Volume derzeit nicht auf einem FabricPool -Aggregat befindet. Die Tiering-Richtlinie wird nur wirksam, wenn sich das Volume auf einem FabricPool -Aggregat befindet.

- **Kalte Daten**

  Die kalten Daten zeigen die Größe der auf dem inaktiven (kalten) Volume gespeicherten Benutzerdaten an.

  Ein Wert wird hier nur angezeigt, wenn Sie ONTAP 9.4 oder eine höhere Software verwenden, da dies erfordert, dass das Aggregat, auf dem das Volume bereitgestellt wird, über die **`inactive data reporting parameter`** eingestellt auf **`enabled`** und dass die Mindestanzahl an Kühltagen erreicht wurde (für Mengen, die die **`snapshot-only`** oder **`auto`** Tiering-Richtlinie). Andernfalls wird der Wert als „N/A“ aufgeführt.

- **Cloud-Empfehlung**

Nachdem genügend Informationen zur Datenaktivität auf dem Datenträger erfasst wurden, kann Unified Manager feststellen, dass keine Aktion erforderlich ist oder dass Sie Speicherplatz auf der Leistungsebene sparen können, indem Sie inaktive Daten auf die Cloudebene verschieben.

Das Feld „Cold Data“ wird alle 15 Minuten aktualisiert, das Feld „Cloud Recommendation“ jedoch alle 7 Tage, wenn die Cold Data-Analyse auf dem Datenträger durchgeführt wird. Daher kann die genaue Menge kalter Daten zwischen den Feldern unterschiedlich sein. Im Feld „Cloud-Empfehlung“ wird das Datum angezeigt, an dem die Analyse ausgeführt wurde.

Wenn die Berichterstattung über inaktive Daten aktiviert ist, zeigt das Feld „Kalte Daten“ die genaue Menge inaktiver Daten an. Ohne die Funktion zur Meldung inaktiver Daten verwendet Unified Manager Leistungsstatistiken, um zu ermitteln, ob Daten auf einem Volume inaktiv sind. Die Menge der inaktiven Daten wird in diesem Fall nicht im Feld „Cold Data“ angezeigt, sie wird jedoch angezeigt, wenn Sie mit dem Cursor über das Wort „Tier“ fahren, um die Cloud-Empfehlung anzuzeigen.

Die Cloud-Empfehlungen, die Sie sehen werden, sind:

- **Lernen**. Es wurden nicht genügend Daten gesammelt, um eine Empfehlung abzugeben.
- **Stufe**. Die Analyse hat ergeben, dass das Volume inaktive (kalte) Daten enthält und dass Sie das Volume so konfigurieren sollten, dass diese Daten in die Cloud-Ebene verschoben werden. In einigen Fällen kann es erforderlich sein, 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 verfügt das Volume über sehr wenige inaktive Daten, das Volume ist bereits auf die Tiering-Richtlinie „auto“ auf einem FabricPool -Aggregat eingestellt oder das Volume ist ein Datenschutzvolume. Dieser Wert wird auch angezeigt, wenn das Volume offline ist oder in einer MetroCluster -Konfiguration verwendet wird.

Um ein Volume zu verschieben oder die Volume-Tiering-Richtlinie oder die Einstellungen für die aggregierte Berichterstattung inaktiver Daten zu ändern, verwenden Sie ONTAP System Manager, die ONTAP CLI-Befehle oder eine Kombination dieser Tools.

Wenn Sie bei Unified Manager mit der Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ angemeldet sind, ist der Link „Volume konfigurieren“ in der Cloud-Empfehlung verfügbar, wenn Sie mit dem Cursor über das Wort „Tier“ fahren. Klicken Sie auf diese Schaltfläche, um die Seite „Volumes“ im System Manager zu öffnen und die empfohlene Änderung vorzunehmen.

Überwachen der Leistung mithilfe der Performance Explorer-Seiten

Auf den Seiten des Performance Explorers werden detaillierte Informationen zur Leistung jedes Objekts in einem Cluster angezeigt. Die Seite bietet einen detaillierten Einblick in die Leistung aller Clusterobjekte und ermöglicht Ihnen, die Leistungsdaten bestimmter Objekte über verschiedene Zeiträume hinweg auszuwählen und zu vergleichen.

Sie können auch die Gesamtleistung aller Objekte beurteilen und die Leistungsdaten der Objekte nebeneinander vergleichen.

Verstehen Sie das Stammobjekt

Das Stammobjekt ist die Basislinie, anhand derer andere Objektvergleiche durchgeführt werden. Auf diese Weise können Sie die Daten anderer Objekte mit denen des Stammobjekts vergleichen und anzeigen. Dadurch erhalten Sie eine Leistungsdatenanalyse, die Ihnen bei der Fehlerbehebung und Verbesserung der Objektleistung hilft.

Der Name des Stammobjekts wird oben im Vergleichsbereich angezeigt. Zusätzliche Objekte werden unterhalb des Stammobjekts angezeigt. Obwohl es keine Begrenzung für die Anzahl zusätzlicher Objekte gibt, die Sie zum Vergleichsbereich hinzufügen können, ist nur ein Stammobjekt zulässig. Daten für das Stammobjekt werden automatisch in den Diagrammen im Bereich „Zählerdiagramme“ angezeigt.

Sie können das Stammobjekt nicht ändern. Es ist immer auf die Objektseite eingestellt, die Sie gerade anzeigen. Wenn Sie beispielsweise die Volume Performance Explorer-Seite von Volume1 öffnen, ist Volume1 das Stammobjekt und kann nicht geändert werden. Wenn Sie einen Vergleich mit einem anderen Stammobjekt durchführen möchten, müssen Sie auf den Link für ein Objekt klicken und dessen Zielseite öffnen.

Ereignisse und Schwellenwerte werden nur für Stammobjekte angezeigt.

Wenden Sie Filter an, um die Liste der korrelierten Objekte im Raster zu reduzieren

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 die Volumes anzeigen, deren Durchsatz unter 90 MBps liegt oder deren Latenz über 1 ms/Operation liegt.

Festlegen eines Zeitbereichs für korrelierte Objekte

Mit der Zeitbereichsauswahl auf der Seite „Performance Explorer“ können Sie den Zeitbereich für den Objektdatenvergleich angeben. Durch die Angabe eines Zeitbereichs wird der Inhalt der Performance Explorer-Seiten verfeinert, sodass nur die Objektdaten innerhalb des von Ihnen angegebenen Zeitbereichs angezeigt werden.

Durch die Verfeinerung des Zeitbereichs können Sie auf effiziente Weise nur die Leistungsdaten anzeigen, die Sie interessieren. Sie können einen vordefinierten Zeitraum auswählen oder einen benutzerdefinierten Zeitraum angeben. Der Standardzeitraum sind die vorangegangenen 72 Stunden.

Wählen Sie einen vordefinierten Zeitraum

Durch die Auswahl eines vordefinierten Zeitbereichs können Sie die Datenausgabe beim Anzeigen von Leistungsdaten von Clusterobjekten schnell und effizient anpassen und fokussieren. Bei Auswahl eines vordefinierten Zeitraums stehen Daten für bis zu 13 Monate zur Verfügung.

Schritte

1. Klicken Sie oben rechts auf der Seite **Performance Explorer** auf **Zeitbereich**.
2. Wählen Sie auf der rechten Seite des Bereichs **Zeitbereichsauswahl** einen vordefinierten Zeitraum aus.

3. Klicken Sie auf **Bereich anwenden**.

Geben Sie einen benutzerdefinierten Zeitraum an

Auf der Seite „Performance Explorer“ können Sie den Datums- und Zeitbereich für Ihre Leistungsdaten angeben. Durch die Angabe eines benutzerdefinierten Zeitbereichs ist die Flexibilität bei der Verfeinerung von Clusterobjektdaten größer als bei der Verwendung vordefinierter Zeitbereiche.

Sie können einen Zeitraum zwischen einer Stunde und 390 Tagen auswählen. 13 Monate entsprechen 390 Tagen, da jeder Monat als 30 Tage gezählt wird. Durch die Angabe eines Datums- und Zeitbereichs erhalten Sie mehr Details und können bestimmte Leistungsereignisse oder Ereignisreihen näher betrachten. Die Angabe eines Zeitbereichs hilft auch bei der Behebung potenzieller Leistungsprobleme, da durch die Angabe eines Datums- und Zeitbereichs die Daten rund um das Leistungsereignis detaillierter angezeigt werden. Verwenden Sie die Steuerung **Zeitbereich**, um vordefinierte Datums- und Zeitbereiche auszuwählen, oder geben Sie Ihren eigenen benutzerdefinierten Datums- und Zeitbereich von bis zu 390 Tagen an. Die Schaltflächen für vordefinierte Zeiträume variieren 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 Sie darauf hinweist, dass die für einen Zeitraum von mehr als 30 Tagen angezeigten Leistungsdaten anhand von Stundendurchschnitten und nicht anhand einer 5-Minuten-Datenabfrage dargestellt werden. Daher kann es zu einem Verlust der visuellen Granularität der Zeitleiste 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 angeben, der größer als 30 Tage ist. Zusammenfassende Daten gelten auch für einen kleineren Zeitraum, wenn der Zeitraum eine Uhrzeit/ein Datum umfasst, die/das mehr als 30 Tage nach dem heutigen Tag liegt.

Bei der Auswahl eines Zeitbereichs (entweder benutzerdefiniert oder vordefiniert) basieren Zeitbereiche von 30 Tagen oder weniger auf Datenproben im 5-Minuten-Intervall. Zeiträume von mehr als 30 Tagen basieren auf Datenproben im Ein-Stunden-Intervall.

1. Klicken Sie auf das Dropdown-Feld **Zeitbereich**, und das Fenster „Zeitbereich“ wird angezeigt.
2. Um einen vordefinierten Zeitraum auszuwählen, klicken Sie auf eine der Schaltflächen **Letzte…** rechts neben dem Bereich **Zeitraum**. Bei Auswahl eines vordefinierten Zeitraums stehen Daten für bis zu 13 Monate zur Verfügung. Die von Ihnen ausgewählte Schaltfläche für den vordefinierten Zeitraum wird hervorgehoben und die entsprechenden Tage und Uhrzeiten werden in den Kalendern und Zeitauswahlfeldern angezeigt.
3. Um einen benutzerdefinierten Datumsbereich auszuwählen, klicken Sie links im Kalender **Von** auf das Startdatum. Klicken Sie auf **<** oder **>**, um im Kalender vorwärts oder rückwärts zu navigieren. Um das Enddatum festzulegen, klicken Sie im Kalender **Bis** rechts auf ein Datum. Beachten Sie, dass das Standardenddatum heute ist, sofern Sie kein anderes Enddatum angeben. Die Schaltfläche **Benutzerdefinierter Bereich** rechts neben dem Bereich „Zeitbereich“ ist hervorgehoben und zeigt damit an, dass Sie einen benutzerdefinierten Datumsbereich ausgewählt haben.
4. Um einen benutzerdefinierten Zeitraum auszuwählen, klicken Sie auf das Steuerelement **Zeit** unter dem Kalender **Von** und wählen Sie die Startzeit aus. Um die Endzeit festzulegen, klicken Sie auf das Steuerelement **Zeit** unter dem Kalender **Bis** auf der rechten Seite und wählen Sie die Endzeit aus. Die Schaltfläche **Benutzerdefinierter Bereich** rechts neben dem Bereich „Zeitbereich“ ist hervorgehoben und zeigt damit an, dass Sie einen benutzerdefinierten Zeitbereich ausgewählt haben.
5. Optional können Sie bei der Auswahl eines vordefinierten Datumsbereichs die Start- und Endzeit angeben. Wählen Sie den vordefinierten Datumsbereich wie zuvor beschrieben aus und wählen Sie dann die Start-

und Endzeiten wie zuvor beschrieben aus. Die ausgewählten Daten werden in den Kalendern hervorgehoben, Ihre angegebenen Start- und Endzeiten werden in den **Zeit**-Steuerelementen angezeigt und die Schaltfläche **Benutzerdefinierter Bereich** wird hervorgehoben.

6. Nachdem Sie den Datums- und Zeitbereich ausgewählt haben, klicken Sie auf **Bereich anwenden**. Die Leistungsstatistiken für diesen Zeitraum werden in den Diagrammen und in der Ereigniszeitleiste angezeigt.

Definieren Sie die Liste der korrelierten Objekte für die grafische Vergleichsdarstellung

Sie können im Bereich „Zählerdiagramm“ eine Liste korrelierter Objekte für den Daten- und Leistungsvergleich definieren. Wenn beispielsweise bei Ihrer Storage Virtual Machine (SVM) ein Leistungsproblem auftritt, können Sie alle Volumes in der SVM vergleichen, um zu ermitteln, welches Volume das Problem möglicherweise verursacht.

Sie können den Bereichen „Vergleichsdiagramm“ und „Zählerdiagramm“ jedes beliebige Objekt im Raster „Korrelierte Objekte“ hinzufügen. Dadurch können Sie Daten mehrerer Objekte und mit dem Stammobjekt anzeigen und vergleichen. Sie können Objekte zum 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 Leistung auswirken. Um die Leistung aufrechtzuerhalten, sollten Sie eine begrenzte Anzahl von Diagrammen für den Datenvergleich auswählen.

Schritte

1. Suchen Sie im Objektraster das Objekt, das Sie hinzufügen möchten, und klicken Sie auf die Schaltfläche **Hinzufügen**.

   Die Schaltfläche **Hinzufügen** wird grau und das Objekt wird der Liste der zusätzlichen Objekte im Vergleichsbereich hinzugefügt. Die Daten des Objekts werden den Diagrammen in den Zählerdiagrammbereichen hinzugefügt. Die Farbe des Augensymbols des Objekts ( ) entspricht der Farbe der Datentrendlinie des Objekts in den Diagrammen.

2. **Optional:** Daten für ausgewählte Objekte ausblenden oder anzeigen:

Um dies zu tun…	Führen Sie diese Aktion aus …
Ausblenden eines ausgewählten Objekts	Klicken Sie auf das Augensymbol des ausgewählten Objekts ( ) im Vergleichsbereich. Die Daten des Objekts werden ausgeblendet und das Augensymbol für dieses Objekt wird grau.
Ein verstecktes Objekt anzeigen	Klicken Sie im Vergleichsbereich auf das graue Augensymbol des ausgewählten Objekts. Das Augensymbol nimmt wieder seine ursprüngliche Farbe an und die Objektdaten werden wieder zu den Diagrammen im Bereich „Zählerdiagramme“ hinzugefügt.

3. **Optional:** Entfernen Sie ausgewählte Objekte aus dem **Vergleichsbereich**:

Um dies zu tun…	Führen Sie diese Aktion aus …
Ein ausgewähltes Objekt entfernen	Bewegen Sie den Mauszeiger über den Namen des ausgewählten Objekts im Vergleichsbereich, um die Schaltfläche zum Entfernen des Objekts (**X**) anzuzeigen, und klicken Sie dann auf die Schaltfläche. Das Objekt wird aus dem Vergleichsbereich entfernt und seine Daten werden aus den Zählerdiagrammen gelöscht.
Alle ausgewählten Objekte entfernen	Klicken Sie oben im Vergleichsbereich auf die Schaltfläche „Alle Objekte entfernen“ (**X**). Alle ausgewählten Objekte und ihre Daten werden entfernt, sodass nur das Stammobjekt übrig bleibt.

Zählerdiagramme verstehen

Mithilfe der Diagramme im Bereich „Zählerdiagramme“ können Sie Leistungsdaten für das Stammobjekt und für Objekte anzeigen und vergleichen, die Sie aus dem Raster „Korrelierte Objekte“ hinzugefügt haben. Dies kann Ihnen dabei helfen, Leistungstrends zu verstehen und Leistungsprobleme zu isolieren und zu beheben.

Standardmäßig werden die Zählerdiagramme Ereignisse, Latenz, IOPS und MBps angezeigt. Optionale Diagramme, die Sie anzeigen können, sind Auslastung, genutzte Leistungskapazität, verfügbare IOPS, IOPS/TB und Cache-Fehlerquote. Darüber hinaus können Sie Gesamtwerte oder aufgeschlüsselte Werte für die Diagramme „Latenz“, „IOPS“, „MBps“ und „Verwendete Leistungskapazität“ anzeigen.

Der Performance Explorer zeigt standardmäßig bestimmte Zählerdiagramme an, unabhängig davon, ob das Speicherobjekt 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 Leistungstrends für das Stammobjekt und für alle Objekte an, die Sie im Vergleichsbereich ausgewählt haben. Die Daten in jedem Diagramm sind wie folgt angeordnet:

- **X-Achse**

  Zeigt den angegebenen Zeitraum an. Wenn Sie keinen Zeitraum angegeben haben, wird standardmäßig der vorangegangene 72-Stunden-Zeitraum verwendet.

- **Y-Achse**

  Zeigt Zählereinheiten an, die für das bzw. die ausgewählte(n) Objekt(e) eindeutig sind.

Die Farben der Trendlinien entsprechen der Farbe des Objektnamens, wie er im Vergleichsbereich angezeigt wird. Sie können Ihren Cursor über einen Punkt auf einer beliebigen Trendlinie positionieren, um Details zu Zeit und Wert für diesen Punkt anzuzeigen.

Wenn Sie einen bestimmten Zeitraum innerhalb eines Diagramms untersuchen möchten, können Sie eine der folgenden Methoden verwenden:

- Verwenden Sie die Schaltfläche **<**, um den Bereich „Zählerdiagramme“ auf die gesamte Seitenbreite zu

erweitern.

- Verwenden Sie den Cursor (wenn er sich in eine Lupe verwandelt), um einen Teil des Zeitrahmens im Diagramm auszuwählen, um diesen Bereich zu fokussieren und zu vergrößern. Sie können auf „Diagrammzoom zurücksetzen“ klicken, um das Diagramm auf den Standardzeitrahmen zurückzusetzen.
- Verwenden Sie die Schaltfläche **Zoom-Ansicht**, um ein großes Einzelzählerdiagramm anzuzeigen, das erweiterte Details und Schwellenwertindikatoren enthält.

Gelegentlich treten Lücken in den Trendlinien auf. Lücken bedeuten, dass Unified Manager entweder keine Leistungsdaten vom Speichersystem erfassen konnte oder dass Unified Manager möglicherweise ausgefallen war.

Arten von Leistungsindikatordiagrammen

Es gibt Standard-Leistungsdiagramme, die die Zählerwerte für das ausgewählte Speicherobjekt anzeigen. Jedes der Aufschlüsselungszählerdiagramme zeigt die Gesamtwerte getrennt nach Lese-, Schreib- und anderen Kategorien an. Darüber hinaus zeigen einige Breakdown-Counter-Diagramme zusätzliche Details an, wenn das Diagramm in der Zoomansicht angezeigt wird.

Die folgende Tabelle zeigt die verfügbaren Leistungsindikatordiagramme.

Verfügbare Diagramme	Diagrammbeschreibung
Veranstaltungen	Zeigt kritische Ereignisse, Fehler-, Warn- und Informationsereignisse in Korrelation mit den statistischen Diagrammen für das Stammobjekt an. Zusätzlich zu den Leistungsereignissen werden auch Integritätsereignisse angezeigt, um ein vollständiges Bild der Gründe zu liefern, warum die Leistung beeinträchtigt sein kann.
Latenz – Gesamt	Anzahl der Millisekunden, die zum Antworten auf Anwendungsanforderungen benötigt werden. Beachten Sie, dass die durchschnittlichen Latenzwerte E/A-gewichtet sind.
Latenz - Aufschlüsselung	Dieselben Informationen werden in „Latenz gesamt“ angezeigt, allerdings sind die Leistungsdaten in Lese-, Schreib- und sonstige Latenzen unterteilt. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein SVM, Knoten, Aggregat, Volume, LUN oder Namespace ist.
Latenz – Clusterkomponenten	Dieselben Informationen werden in „Latenz gesamt“ angezeigt, die Leistungsdaten sind jedoch nach Latenz nach Clusterkomponente aufgeschlüsselt. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volumen ist.

Verfügbare Diagramme	Diagrammbeschreibung
IOPS – Gesamt	Anzahl der pro Sekunde verarbeiteten Eingabe-/Ausgabevorgänge. Wenn für einen Knoten „Gesamt“ angezeigt wird, werden durch Auswahl von „Gesamt“ die IOPS für Daten angezeigt, die durch diesen Knoten übertragen werden und sich auf dem lokalen oder Remote-Knoten befinden können. Durch Auswahl von „Gesamt (Lokal)“ werden die IOPS für Daten angezeigt, die sich nur auf dem aktuellen Knoten befinden.
IOPS – Aufschlüsselung	Dieselben Informationen werden in „IOPS gesamt“ angezeigt, allerdings sind die Leistungsdaten in Lese-, Schreib- und andere IOPS unterteilt. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein SVM, Knoten, Aggregat, Volume, LUN oder Namespace ist. In der Zoomansicht zeigt das Volume-Diagramm die minimalen und maximalen QoS-Durchsatzwerte an, sofern diese in ONTAP konfiguriert sind. Wenn für einen Knoten „Aufschlüsselung“ angezeigt wird, wird durch Auswahl von „Aufschlüsselung“ die IOPS-Aufschlüsselung für Daten angezeigt, die durch diesen Knoten übertragen werden und sich auf dem lokalen oder dem Remote-Knoten befinden können. Durch Auswahl von „Aufschlüsselung (Lokal)“ wird die IOPS-Aufschlüsselung für Daten angezeigt, die sich nur auf dem aktuellen Knoten befinden.
IOPS – Protokolle	Dieselben Informationen werden in „IOPS gesamt“ angezeigt, die Leistungsdaten sind jedoch in einzelne Diagramme für CIFS-, NFS-, FCP-, NVMe- und iSCSI-Protokollverkehr unterteilt. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein SVM ist.
IOPS/TB – Gesamt	Anzahl der pro Sekunde verarbeiteten Eingabe-/Ausgabevorgänge basierend auf dem gesamten von der Arbeitslast belegten Speicherplatz in Terabyte. Dieser Zähler, auch E/A-Dichte genannt, misst, wie viel Leistung mit einer bestimmten Speicherkapazität bereitgestellt werden kann. In der Zoomansicht zeigt das Volumendiagramm die erwarteten QoS- und Spitzendurchsatzwerte an, sofern diese in ONTAP konfiguriert sind. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volumen ist.

Verfügbare Diagramme	Diagrammbeschreibung
MB/s – Gesamt	Anzahl der Megabyte an Daten, die pro Sekunde zum und vom Objekt übertragen werden.
MB/s – Aufschlüsselung	Dieselben Informationen werden im MB/s-Diagramm angezeigt, allerdings sind die Durchsatzdaten in Festplattenlesevorgänge, Flash-Cache-Lesevorgänge, Schreibvorgänge und Sonstiges unterteilt. In der Zoomansicht zeigt das Volume-Diagramm die maximalen QoS-Durchsatzwerte an, sofern diese in ONTAP konfiguriert sind. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein SVM, Knoten, Aggregat, Volume, LUN oder Namespace ist. Flash-Cache-Daten werden nur für Knoten angezeigt und nur, wenn im Knoten ein Flash-Cache-Modul installiert ist.
Ausgenutzte Leistungskapazität – Gesamt	Prozentsatz der Leistungskapazität, die vom Knoten oder Aggregat verbraucht wird.
Ausgenutzte Leistungsfähigkeit - Aufschlüsselung	Leistungskapazität Verwendete Daten getrennt nach Benutzerprotokollen und Systemhintergrundprozessen. Zusätzlich wird die Höhe der freien Leistungskapazität angezeigt.
Verfügbare IOPS – Gesamt	Anzahl der Eingabe-/Ausgabevorgänge pro Sekunde, die derzeit für dieses Objekt verfügbar (frei) sind. Diese Zahl ergibt sich aus der Subtraktion der aktuell verwendeten IOPS von 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	Verfügbarer Ressourcenprozentsatz des verwendeten Objekts. Die Auslastung gibt die Knotenauslastung für Knoten, die Festplattenauslastung für Aggregate und die Bandbreitenauslastung für Ports an. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Knoten, ein Aggregat oder ein Port ist.
Cache-Fehlerquote – Gesamt	Prozentsatz der Leseanforderungen von Clientanwendungen, die von der Festplatte und nicht aus dem Cache zurückgegeben werden. Diese Diagrammoption gilt nur, wenn das ausgewählte Objekt ein Volumen ist.

Wählen Sie die anzuzeigenden Leistungsdiagramme aus

Über die Dropdownliste „Diagramme auswählen“ können Sie die Typen von Leistungsindikatordiagrammen auswählen, die im Bereich „Indikatordiagramme“ angezeigt werden sollen. Auf diese Weise können Sie je nach Ihren Leistungsanforderungen bestimmte Daten und Zähler anzeigen.

Schritte

1. Klicken Sie im Bereich **Zählerdiagramme** auf die Dropdownliste **Diagramme auswählen**.
2. Diagramme hinzufügen oder entfernen:

Zu…	Machen Sie Folgendes…
Einzelne Diagramme hinzufügen oder entfernen	Klicken Sie auf die Kontrollkästchen neben den Diagrammen, die Sie ein- oder ausblenden möchten
Alle Diagramme hinzufügen	Klicken Sie auf **Alles auswählen**
Alle Diagramme entfernen	Klicken Sie auf **Auswahl aufheben**

Ihre Diagrammauswahl wird im Bereich „Zählerdiagramme“ angezeigt. Beachten Sie, dass beim Hinzufügen von Diagrammen die neuen Diagramme in den Bereich „Zählerdiagramme“ eingefügt werden, um der Reihenfolge der in der Dropdownliste „Diagramme auswählen“ aufgeführten Diagramme zu entsprechen. Zum Auswählen weiterer Diagramme ist möglicherweise zusätzliches Scrollen erforderlich.

Erweitern Sie den Bereich „Zählerdiagramme“

Sie können den Bereich „Zählerdiagramme“ erweitern, damit die Diagramme größer und besser lesbar sind.

Nachdem Sie die Vergleichsobjekte und den Zeitbereich für die Zähler definiert haben, können Sie einen größeren Bereich mit Zählerdiagrammen anzeigen. Mit der Schaltfläche **<** in der Mitte des Performance Explorer-Fensters können Sie den Bereich erweitern.

Schritt

1. Erweitern oder verkleinern Sie den Bereich **Zählerdiagramme**.

Zu…	Machen Sie Folgendes…
Erweitern Sie den Bereich „Zählerdiagramme“, sodass er der Seitenbreite entspricht.	Klicken Sie auf die Schaltfläche **<**
Reduzieren Sie den Bereich „Counter Charts“ auf die rechte Hälfte der Seite	Klicken Sie auf die Schaltfläche **>**

Ändern Sie den Fokus der Counter Charts auf einen kürzeren Zeitraum

Sie können den Zeitbereich mit der Maus verkleinern, um sich auf einen bestimmten

Zeitraum im Bereich „Zählerdiagramm“ oder im Fenster „Zählerdiagramm-Zoomansicht“ zu konzentrieren. Dadurch erhalten Sie eine detailliertere und mikroskopischere Ansicht aller Teile der Zeitleiste mit Leistungsdaten, Ereignissen und Schwellenwerten.

Bevor Sie beginnen

Um anzuzeigen, dass diese Funktionalität aktiv ist, muss sich der Cursor in eine Lupe verwandelt haben.

> Bei Verwendung dieser Funktion, die die Zeitleiste ändert, um Werte anzuzeigen, die der detaillierteren Anzeige entsprechen, ändert sich der Zeit- und Datumsbereich im **Zeitbereich** -Selektor nicht gegenüber den ursprünglichen Werten für das Diagramm.

Schritte

1. Um in einen bestimmten Zeitraum hineinzuzoomen, klicken Sie mit der Lupe und ziehen Sie die Maus, um den Bereich hervorzuheben, den Sie im Detail sehen möchten.

   Die Zählerwerte für den von Ihnen ausgewählten Zeitraum füllen das Zählerdiagramm.

2. Um zum ursprünglichen Zeitraum zurückzukehren, der im Auswahlfeld **Zeitbereich** festgelegt wurde, klicken Sie auf die Schaltfläche **Diagrammzoom zurücksetzen**.

   Das Zählerdiagramm wird in seinem ursprünglichen Zustand angezeigt.

Ereignisdetails in der Ereigniszeitleiste anzeigen

Sie können alle Ereignisse und die zugehörigen Details im Bereich „Ereigniszeitleiste“ des Performance Explorers anzeigen. Dies ist eine schnelle und effiziente Methode zum Anzeigen aller Integritäts- und Leistungsereignisse, die während eines angegebenen Zeitraums beim Stammobjekt aufgetreten sind. Dies kann bei der Behebung von Leistungsproblemen hilfreich sein.

Im Bereich „Ereigniszeitleiste“ werden kritische Ereignisse, Fehler-, Warn- und Informationsereignisse angezeigt, die während des ausgewählten Zeitraums beim Stammobjekt aufgetreten sind. Jeder Ereignisschweregrad hat seinen eigenen Zeitrahmen. Einzelne und mehrere Ereignisse werden durch einen Ereignispunkt auf der Zeitachse dargestellt. Sie können Ihren Cursor über einen Ereignispunkt positionieren, um die Ereignisdetails anzuzeigen. Um die visuelle Granularität mehrerer Ereignisse zu erhöhen, können Sie den Zeitbereich verringern. Dadurch werden mehrere Ereignisse in einzelne Ereignisse aufgeteilt, sodass Sie jedes Ereignis separat anzeigen und untersuchen können.

Jeder Performance-Ereignispunkt auf der Ereignis-Zeitleiste ist vertikal mit einer entsprechenden Spitze in den Trendlinien der Zählerdiagramme ausgerichtet, die unter der Ereignis-Zeitleiste angezeigt werden. Dies ermöglicht eine direkte visuelle Korrelation zwischen Ereignissen und der Gesamtleistung. Gesundheitsereignisse werden ebenfalls auf der Zeitachse angezeigt, diese Ereignistypen müssen jedoch nicht unbedingt mit einem Spitzenwert in einem der Leistungsdiagramme übereinstimmen.

Schritte

1. Positionieren Sie im Bereich **Ereigniszeitleiste** den Cursor über einem Ereignispunkt auf einer Zeitleiste, um eine Zusammenfassung des Ereignisses bzw. der Ereignisse an diesem Ereignispunkt anzuzeigen.

   In einem Popup-Dialogfeld werden Informationen zu den Ereignistypen, Datum und Uhrzeit des Auftretens der Ereignisse, der Status und die Ereignisdauer angezeigt.

2. Vollständige Ereignisdetails für ein oder mehrere Ereignisse anzeigen:

Um dies zu tun…	Klicken Sie hier…
Details zu einem einzelnen Ereignis anzeigen	**Ereignisdetails anzeigen** im Popup-Dialog.
Details für mehrere Ereignisse anzeigen	**Ereignisdetails anzeigen** im Popup-Dialog. Wenn Sie im Dialogfeld „Mehrere Ereignisse“ auf ein einzelnes Ereignis klicken, wird die entsprechende Seite mit den Ereignisdetails angezeigt.

Zählerdiagramme Zoomansicht

Die Zählerdiagramme bieten eine Zoomansicht, mit der Sie Leistungsdetails über den von Ihnen angegebenen Zeitraum vergrößern können. Dadurch können Sie Leistungsdetails und Ereignisse mit einer viel höheren Granularität anzeigen, was bei der Behebung von Leistungsproblemen von Vorteil ist.

Bei der Anzeige in der Zoom-Ansicht bieten einige der Aufschlüsselungsdiagramme zusätzliche Informationen als die, die angezeigt werden, wenn sich das Diagramm nicht in der Zoom-Ansicht befindet. Beispielsweise werden auf den Zoom-Ansichtsseiten des Aufschlüsselungsdiagramms „IOPS“, „IOPS/TB“ und „MBps“ QoS-Richtlinienwerte für Volumes und LUNs angezeigt, wenn diese in ONTAP festgelegt wurden.

Für systemdefinierte Richtlinien für Leistungsschwellenwerte sind in der Liste **Richtlinien** nur die Richtlinien „Knotenressourcen überlastet“ und „QoS-Durchsatzlimit überschritten“ verfügbar. Die anderen systemdefinierten Schwellenwertrichtlinien sind derzeit nicht verfügbar.

Anzeigen der Zoomansicht der Zählerdiagramme

Die Zoomansicht der Zählerdiagramme bietet eine höhere Detailgenauigkeit für das ausgewählte Zählerdiagramm und die zugehörige Zeitleiste. Dadurch werden die Daten des Zählerdiagramms vergrößert, sodass Sie einen besseren Einblick in Leistungsereignisse und deren zugrunde liegende Ursachen erhalten.

Sie können die Zoomansicht der Zählerdiagramme für jedes Zählerdiagramm anzeigen.

Schritte

1. Klicken Sie auf **Zoom-Ansicht**, um das ausgewählte Diagramm in einem neuen Browserfenster zu öffnen.
2. Wenn Sie ein Aufschlüsselungsdiagramm anzeigen und dann auf **Zoom-Ansicht** klicken, wird das Aufschlüsselungsdiagramm in der Zoom-Ansicht angezeigt. Sie können in der Zoomansicht **Gesamt** auswählen, wenn Sie die Ansichtsoption ändern möchten.

Geben Sie den Zeitbereich in der Zoomansicht an

Mit der Steuerung **Zeitbereich** im Fenster „Zoomansicht der Zählerdiagramme“ können

Sie einen Datums- und Zeitbereich für das ausgewählte Diagramm angeben. Auf diese Weise können Sie schnell bestimmte Daten basierend auf einem voreingestellten Zeitbereich oder Ihrem eigenen benutzerdefinierten Zeitbereich finden.

Sie können einen Zeitraum zwischen einer Stunde und 390 Tagen auswählen. 13 Monate entsprechen 390 Tagen, da jeder Monat als 30 Tage gezählt wird. Durch die Angabe eines Datums- und Zeitbereichs erhalten Sie mehr Details und können bestimmte Leistungsereignisse oder Ereignisreihen näher betrachten. Die Angabe eines Zeitbereichs hilft auch bei der Behebung potenzieller Leistungsprobleme, da durch die Angabe eines Datums- und Zeitbereichs die Daten rund um das Leistungsereignis detaillierter angezeigt werden. Verwenden Sie die Steuerung **Zeitbereich**, um vordefinierte Datums- und Zeitbereiche auszuwählen, oder geben Sie Ihren eigenen benutzerdefinierten Datums- und Zeitbereich von bis zu 390 Tagen an. Die Schaltflächen für vordefinierte Zeiträume variieren 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 Sie darauf hinweist, dass die für einen Zeitraum von mehr als 30 Tagen angezeigten Leistungsdaten anhand von Stundendurchschnitten und nicht anhand einer 5-Minuten-Datenabfrage dargestellt werden. Daher kann es zu einem Verlust der visuellen Granularität der Zeitleiste 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 angeben, der größer als 30 Tage ist. Zusammenfassende Daten gelten auch für einen kleineren Zeitraum, wenn der Zeitraum eine Uhrzeit/ein Datum umfasst, die/das mehr als 30 Tage nach dem heutigen Tag liegt.

Bei der Auswahl eines Zeitbereichs (entweder benutzerdefiniert oder vordefiniert) basieren Zeitbereiche von 30 Tagen oder weniger auf Datenproben im 5-Minuten-Intervall. Zeiträume von mehr als 30 Tagen basieren auf Datenproben im Ein-Stunden-Intervall.

1. Klicken Sie auf das Dropdown-Feld **Zeitbereich**, und das Fenster „Zeitbereich“ wird angezeigt.
2. Um einen vordefinierten Zeitraum auszuwählen, klicken Sie auf eine der Schaltflächen **Letzte…** rechts neben dem Bereich **Zeitraum**. Bei Auswahl eines vordefinierten Zeitraums stehen Daten für bis zu 13 Monate zur Verfügung. Die von Ihnen ausgewählte Schaltfläche für den vordefinierten Zeitraum wird hervorgehoben und die entsprechenden Tage und Uhrzeiten werden in den Kalendern und Zeitauswahlfeldern angezeigt.
3. Um einen benutzerdefinierten Datumsbereich auszuwählen, klicken Sie links im Kalender **Von** auf das Startdatum. Klicken Sie auf **<** oder **>**, um im Kalender vorwärts oder rückwärts zu navigieren. Um das Enddatum festzulegen, klicken Sie im Kalender **Bis** rechts auf ein Datum. Beachten Sie, dass das Standardenddatum heute ist, sofern Sie kein anderes Enddatum angeben. Die Schaltfläche **Benutzerdefinierter Bereich** rechts neben dem Bereich „Zeitbereich“ ist hervorgehoben und zeigt damit an, dass Sie einen benutzerdefinierten Datumsbereich ausgewählt haben.
4. Um einen benutzerdefinierten Zeitraum auszuwählen, klicken Sie auf das Steuerelement **Zeit** unter dem Kalender **Von** und wählen Sie die Startzeit aus. Um die Endzeit festzulegen, klicken Sie auf das Steuerelement **Zeit** unter dem Kalender **Bis** auf der rechten Seite und wählen Sie die Endzeit aus. Die Schaltfläche **Benutzerdefinierter Bereich** rechts neben dem Bereich „Zeitbereich“ ist hervorgehoben und zeigt damit an, dass Sie einen benutzerdefinierten Zeitbereich ausgewählt haben.
5. Optional können Sie bei der Auswahl eines vordefinierten Datumsbereichs die Start- und Endzeit angeben. Wählen Sie den vordefinierten Datumsbereich wie zuvor beschrieben aus und wählen Sie dann die Start- und Endzeiten wie zuvor beschrieben aus. Die ausgewählten Daten werden in den Kalendern hervorgehoben, Ihre angegebenen Start- und Endzeiten werden in den **Zeit**-Steuerelementen angezeigt und die Schaltfläche **Benutzerdefinierter Bereich** wird hervorgehoben.
6. Nachdem Sie den Datums- und Zeitbereich ausgewählt haben, klicken Sie auf **Bereich anwenden**. Die Leistungsstatistiken für diesen Zeitraum werden in den Diagrammen und in der Ereigniszeitleiste

angezeigt.

Wählen Sie Leistungsschwellenwerte in der Zoomansicht der Zählerdiagramme aus

Durch Anwenden von Schwellenwerten in der Zoomansicht der Zählerdiagramme erhalten Sie eine detaillierte Ansicht des Auftretens von Leistungsschwellenwertereignissen. Auf diese Weise können Sie Schwellenwerte anwenden oder entfernen und die Ergebnisse sofort anzeigen. Dies kann bei der Entscheidung hilfreich sein, ob die Fehlerbehebung Ihr nächster Schritt sein sollte.

Durch die Auswahl von Schwellenwerten in der Zoomansicht der Zählerdiagramme können Sie präzise Daten zu Leistungsschwellenwertereignissen 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. Aktivieren oder deaktivieren Sie die das mit einer Richtlinie verknüpft ist.

   Der ausgewählte Schwellenwert wird auf die Zoomansicht der Zählerdiagramme angewendet. Kritische Schwellenwerte werden als rote Linie angezeigt, Warnschwellen als gelbe Linie.

Anzeigen der Volume-Latenz nach Clusterkomponente

Sie können detaillierte Latenzinformationen für ein Volume mithilfe der Seite „Volume Performance Explorer“ anzeigen. Das Zählerdiagramm „Latenz – Gesamt“ zeigt die Gesamtlatenz auf dem Datenträger an und das Zählerdiagramm „Latenz – Aufschlüsselung“ ist hilfreich, um die Auswirkungen der Lese- und Schreiblatenz auf den Datenträger zu bestimmen.

Darüber hinaus zeigt das Diagramm „Latenz – Clusterkomponenten“ einen detaillierten Vergleich der Latenz jeder Clusterkomponente, um zu bestimmen, wie jede Komponente zur Gesamtlatenz auf dem Datenträger beiträgt. Die folgenden Clusterkomponenten werden angezeigt:

- Netzwerk
- QoS-Limit Max
- QoS-Limit Min
- Netzwerkverarbeitung
- Cluster-Verbindung
- Data Processing
- Aggregierte Operationen
- Volumenaktivierung
- MetroCluster -Ressourcen
- Cloud-Latenz
- SnapMirror synchronisieren

Schritte

1. Wählen Sie auf der Seite **Volume Performance Explorer** für Ihr ausgewähltes Volume im Latenzdiagramm im Dropdownmenü **Clusterkomponenten** aus.

   Das Diagramm „Latenz – Clusterkomponenten“ wird angezeigt.

2. Um eine größere Version des Diagramms anzuzeigen, wählen Sie **Zoom-Ansicht**.

   Das Vergleichsdiagramm der Clusterkomponenten wird angezeigt. Sie können den Vergleich einschränken, indem Sie die das mit jeder Clusterkomponente verknüpft ist.

3. Um die spezifischen Werte anzuzeigen, bewegen Sie den Cursor in den Diagrammbereich, um das Popup-Fenster anzuzeigen.

SVM-IOPS-Verkehr nach Protokoll anzeigen

Sie können detaillierte IOPS-Informationen für eine SVM auf der Seite „Leistung/SVM-Explorer“ anzeigen. Das IOPS-Gesamtzählerdiagramm zeigt die gesamte IOPS-Nutzung auf der SVM und das IOPS-Aufschlüsselungszählerdiagramm ist hilfreich, um die Auswirkungen von Lese-, Schreib- und anderen IOPS auf die SVM zu bestimmen.

Darüber hinaus zeigt das Diagramm „IOPS – Protokolle“ einen detaillierten Vergleich des IOPS-Verkehrs für jedes Protokoll, das auf der SVM verwendet wird. Folgende Protokolle stehen zur Verfügung:

- CIFS
- NFS
- FCP
- iSCSI
- NVMe-FC

Schritte

1. Wählen Sie auf der Seite **Leistung/SVM-Explorer** für Ihr ausgewähltes SVM im IOPS-Diagramm im Dropdown-Menü **Protokolle** aus.

   Das Diagramm „IOPS – Protokolle“ wird angezeigt.

2. Um eine größere Version des Diagramms anzuzeigen, wählen Sie **Zoom-Ansicht**.

   Das Vergleichsdiagramm für erweiterte IOPS-Protokolle wird angezeigt. Sie können den Vergleich einschränken, indem Sie die das mit einem Protokoll verknüpft ist.

3. Um die spezifischen Werte anzuzeigen, bewegen Sie den Cursor in den Diagrammbereich eines der Diagramme, um das Popup-Fenster anzuzeigen.

Zeigen Sie Volume- und LUN-Latenzdiagramme an, um die Leistungsgarantie zu überprüfen

Sie können die Volumes und LUNs anzeigen, für die Sie das Programm „Leistungsgarantie“ abonniert haben, um zu überprüfen, ob die Latenz das Ihnen garantierte Niveau nicht überschritten hat.

Die Latenzleistungsgarantie ist ein Wert von Millisekunden pro Vorgang, der nicht überschritten werden sollte.

Es basiert auf einem Stundendurchschnitt und nicht auf dem standardmäßigen fünfminütigen Leistungserfassungszeitraum.

Schritte

1. Wählen Sie in der Ansicht **Leistung: Alle Volumes** oder **Leistung: Alle LUNs** das Volume oder die LUN aus, an dem/der Sie interessiert sind.
2. Wählen Sie auf der Seite **Performance Explorer** für Ihr ausgewähltes Volume oder LUN im Selektor **Statistiken anzeigen in** die Option **Stundendurchschnitt** aus.

   Die horizontale Linie im Latenzdiagramm wird glatter, da die fünfminütigen Erfassungen durch den Stundendurchschnitt ersetzt werden.

3. Wenn Sie auf demselben Aggregat weitere Volumes haben, die der Leistungsgarantie unterliegen, können Sie diese Volumes hinzufügen, um ihren Latenzwert im selben Diagramm anzuzeigen.

Leistung aller SAN-Array-Cluster anzeigen

Sie können die Ansicht „Leistung: Alle Cluster“ verwenden, um den Leistungsstatus aller Ihrer SAN-Array-Cluster anzuzeigen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können Übersichtsinformationen für alle SAN-Array-Cluster in der Ansicht „Leistung: Alle Cluster“ und Details auf der Seite „Cluster-/Leistungs-Explorer“ anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Cluster**.
2. Stellen Sie sicher, dass die Spalte „Persönlichkeit“ in der Ansicht **Gesundheit: Alle Cluster** angezeigt wird, oder fügen Sie sie mithilfe des Steuerelements **Einblenden/Ausblenden** hinzu.

   In dieser Spalte wird „All SAN Array“ für Ihre All SAN Array-Cluster angezeigt.

3. Um Informationen zur Leistung in diesen Clustern anzuzeigen, wählen Sie die Ansicht **Leistung: Alle Cluster**.

   Zeigen Sie die Leistungsinformationen für den All-SAN-Array-Cluster an.

4. Um detaillierte Informationen zur Leistung in diesen Clustern anzuzeigen, klicken Sie auf den Namen eines All-SAN-Array-Clusters.
5. Klicken Sie auf die Registerkarte **Explorer**.
6. Wählen Sie auf der Seite **Cluster-/Leistungs-Explorer** im Menü **Anzeigen und Vergleichen** die Option **Knoten in diesem Cluster** aus.

   Sie können die Leistungsstatistiken beider Knoten in diesem Cluster vergleichen, um sicherzustellen, dass die Last auf beiden Knoten nahezu identisch ist. Wenn zwischen den beiden Knoten große Abweichungen bestehen, können Sie den Diagrammen den zweiten Knoten hinzufügen und die Werte über einen längeren Zeitraum vergleichen, um etwaige Konfigurationsprobleme zu identifizieren.

Anzeigen von Knoten-IOPS basierend auf Workloads, die sich nur auf dem lokalen Knoten befinden

Das Knoten-IOPS-Zählerdiagramm kann hervorheben, wo Vorgänge nur über den lokalen Knoten laufen, indem ein Netzwerk-LIF verwendet wird, um Lese-/Schreibvorgänge auf Volumes auf einem Remoteknoten durchzuführen. Die Diagramme „IOPS – Gesamt (lokal)“ und „Aufschlüsselung (lokal)“ zeigen die IOPS für Daten an, die sich nur auf dem aktuellen Knoten in lokalen Volumes befinden.

Die „lokalen“ Versionen dieser Zählerdiagramme ähneln den Knotendiagrammen für Leistungskapazität und -auslastung, da sie ebenfalls nur die Statistiken für Daten anzeigen, die sich auf lokalen Datenträgern befinden.

Durch Vergleichen der „Lokalen“ Versionen dieser Zählerdiagramme mit den regulären Gesamtversionen dieser Zählerdiagramme können Sie erkennen, ob viel Datenverkehr über den lokalen Knoten fließt, um auf Volumes auf dem Remoteknoten zuzugreifen. Diese Situation kann zu Leistungsproblemen führen, die sich möglicherweise durch eine hohe Auslastung des Knotens bemerkbar machen, wenn zu viele Vorgänge über den lokalen Knoten laufen, um ein Volume auf einem Remoteknoten zu erreichen. In diesen Fällen möchten Sie möglicherweise ein Volume auf den lokalen Knoten verschieben oder ein LIF auf dem Remoteknoten erstellen, wo der Datenverkehr von Hosts, die auf dieses Volume zugreifen, verbunden werden kann.

Schritte

1. Wählen Sie auf der Seite **Leistung/Knoten-Explorer** für Ihren ausgewählten Knoten im IOPS-Diagramm im Dropdown-Menü die Option **Gesamt** aus.

   Das IOPS-Gesamtdiagramm wird angezeigt.

2. Klicken Sie auf **Zoom-Ansicht**, um eine größere Version des Diagramms in einem neuen Browser-Tab anzuzeigen.
3. Zurück auf der Seite **Leistung/Knoten-Explorer** wählen Sie im IOPS-Diagramm im Dropdown-Menü die Option **Gesamt (Lokal)** aus.

   Das Diagramm „IOPS – Gesamt (lokal)“ wird angezeigt.

4. Klicken Sie auf **Zoom-Ansicht**, um eine größere Version des Diagramms in einem neuen Browser-Tab anzuzeigen.
5. Sehen Sie sich beide Diagramme nebeneinander an und identifizieren Sie Bereiche, in denen die IOPS-Werte deutlich unterschiedlich zu sein scheinen.
6. Bewegen Sie den Cursor über diese Bereiche, um die lokalen und gesamten IOPS für einen bestimmten Zeitpunkt zu vergleichen.

Komponenten der Objekt-Landingpages

Die Objekt-Landingpages bieten Details zu allen kritischen, Warn- und Informationsereignissen. Sie bieten einen detaillierten Einblick in die Leistung aller Clusterobjekte und ermöglichen Ihnen die Auswahl und den Vergleich einzelner Objekte über verschiedene Zeiträume hinweg.

Auf den Objekt-Landingpages können Sie die Gesamtleistung aller Objekte prüfen und die Leistungsdaten der Objekte nebeneinander vergleichen. Dies ist bei der Leistungsbewertung und der Fehlerbehebung von Ereignissen hilfreich.

Die in den Zählerübersichtsfeldern und in den Zählerdiagrammen angezeigten Daten basieren auf einem fünfminütigen Abtastintervall. Die im Objektinventarraster auf der linken Seite der Seite angezeigten Daten basieren auf einem einstündigen Stichprobenintervall.

Das folgende Bild zeigt ein Beispiel einer Objekt-Landingpage, auf der die Explorer-Informationen angezeigt werden:

Abhängig vom angezeigten Speicherobjekt kann die Objekt-Landingpage die folgenden Registerkarten enthalten, die Leistungsdaten zum Objekt bereitstellen:

- Zusammenfassung

  Zeigt drei oder vier Zählerdiagramme mit den Ereignissen und der Leistung pro Objekt für den vorangegangenen 72-Stunden-Zeitraum an, einschließlich einer Trendlinie, die die Höchst- und Tiefstwerte während dieses Zeitraums anzeigt.

- Forscher

  Zeigt ein Raster der Speicherobjekte an, die mit dem aktuellen Objekt in Beziehung stehen, sodass Sie die Leistungswerte des aktuellen Objekts mit denen der zugehörigen Objekte vergleichen können. Diese Registerkarte enthält bis zu elf Zählerdiagramme und einen Zeitbereichswähler, mit denen Sie verschiedene Vergleiche durchführen können.

- Information

  Zeigt Werte für nicht leistungsbezogene Konfigurationsattribute zum Speicherobjekt an, einschließlich der installierten Version der ONTAP -Software, des HA-Partnernamens und der Anzahl der Ports und LIFs.

- Top-Performer

  Für Cluster: Zeigt die Speicherobjekte mit der höchsten oder niedrigsten Leistung an, basierend auf dem von Ihnen ausgewählten Leistungsindikator.

- Failover-Planung

  Für Knoten: Zeigt die Schätzung der Leistungseinbußen für einen Knoten an, wenn der HA-Partner des Knotens ausfällt.

- Details

  Für Volumes: Zeigt detaillierte Leistungsstatistiken für alle E/A-Aktivitäten und Vorgänge für die ausgewählte Volume-Arbeitslast an. Diese Registerkarte ist für FlexVol -Volumes, FlexGroup -Volumes und Bestandteile von FlexGroups verfügbar.

Zusammenfassungsseite

Auf der Seite „Zusammenfassung“ werden Zählerdiagramme angezeigt, die Details zu den Ereignissen und der Leistung pro Objekt für den vorangegangenen 72-Stunden-Zeitraum enthalten. Diese Daten werden nicht automatisch aktualisiert, sind aber zum Zeitpunkt des letzten Seitenaufrufs aktuell. Die Diagramme auf der Übersichtsseite beantworten die Frage: „Muss ich weiter suchen?“

Diagramme und Zählerstatistiken

Die Übersichtsdiagramme bieten einen schnellen Überblick über die letzten 72 Stunden und helfen Ihnen, mögliche Probleme zu erkennen, die einer weiteren Untersuchung bedürfen.

Die Zählerstatistiken der Zusammenfassungsseite werden in Diagrammen angezeigt.

Sie können Ihren Cursor über der Trendlinie in einem Diagramm positionieren, um die Zählerwerte für einen bestimmten Zeitpunkt anzuzeigen. Die Übersichtsdiagramme zeigen außerdem die Gesamtzahl der aktiven kritischen Ereignisse und Warnereignisse für den vorangegangenen 72-Stunden-Zeitraum für die folgenden Zähler an:

- **Latenz**

  Durchschnittliche Antwortzeit für alle E/A-Anfragen; ausgedrückt in Millisekunden pro Vorgang.

  Wird für alle Objekttypen angezeigt.

- **IOPS**

  Durchschnittliche Betriebsgeschwindigkeit, ausgedrückt in Eingabe-/Ausgabevorgängen pro Sekunde.

  Wird für alle Objekttypen angezeigt.

- **MB/s**

  Durchschnittlicher Durchsatz; ausgedrückt in Megabyte pro Sekunde.

  Wird für alle Objekttypen angezeigt.

- **Ausgenutzte Leistungskapazität**

  Prozentsatz der Leistungskapazität, die von einem Knoten oder Aggregat verbraucht wird.

  Wird nur für Knoten und Aggregate angezeigt.

- **Verwendung**

  Prozentsatz der Objektauslastung für Knoten und Aggregate oder Bandbreitenauslastung für Ports.

  Wird nur für Knoten, Aggregate und Ports angezeigt.

Wenn Sie den Cursor über die Ereignisanzahl für aktive Ereignisse positionieren, werden Typ und Anzahl der Ereignisse angezeigt. Kritische Ereignisse werden rot angezeigt ( ) und Warnereignisse werden gelb angezeigt ( ).

Die Zahl oben rechts im Diagramm im grauen Balken ist der Durchschnittswert der letzten 72 Stunden. Die unten und oben im Trendliniendiagramm angezeigten Zahlen stellen die Mindest- und Höchstwerte für den letzten 72-Stunden-Zeitraum dar. Der graue Balken unter dem Diagramm enthält die Anzahl der aktiven (neuen und bestätigten) Ereignisse und veralteten Ereignisse aus dem letzten 72-Stunden-Zeitraum.

- **Latenzzählerdiagramm**

  Das Latenzzählerdiagramm bietet einen allgemeinen Überblick über die Objektlatenz für den vorangegangenen 72-Stunden-Zeitraum. Latenz bezieht sich auf die durchschnittliche Antwortzeit für alle

E/A-Anfragen; ausgedrückt in Millisekunden pro Vorgang, die Servicezeit, Wartezeit oder beides, die ein Datenpaket oder Block in der betreffenden Cluster-Speicherkomponente erfährt.

Oben (Zählerwert): Die Zahl in der Kopfzeile zeigt den Durchschnitt der letzten 72 Stunden an.

Mitte (Leistungsdiagramm): Die Zahl unten im Diagramm zeigt die niedrigste Latenz und die Zahl oben im Diagramm zeigt die höchste Latenz für den vorangegangenen 72-Stunden-Zeitraum an. Positionieren Sie den Cursor über der Trendlinie des Diagramms, um den Latenzwert für einen bestimmten Zeitpunkt anzuzeigen.

Unten (Ereignisse): Beim Darüberfahren zeigt das Popup die Details der Ereignisse an. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinventar“ zu navigieren und alle Ereignisdetails anzuzeigen.

- **IOPS-Zählerdiagramm**

  Das IOPS-Zählerdiagramm bietet einen umfassenden Überblick über den IOPS-Zustand des Objekts für den vorangegangenen 72-Stunden-Zeitraum. IOPS gibt die Geschwindigkeit des Speichersystems in Anzahl der Eingabe-/Ausgabevorgänge pro Sekunde an.

  Oben (Zählerwert): Die Zahl in der Kopfzeile zeigt den Durchschnitt der letzten 72 Stunden an.

  Mitte (Leistungsdiagramm): Die Zahl unten im Diagramm zeigt die niedrigsten IOPS und die Zahl oben im Diagramm zeigt die höchsten IOPS für den vorangegangenen 72-Stunden-Zeitraum an. Positionieren Sie den Cursor über der Trendlinie des Diagramms, um den IOPS-Wert für einen bestimmten Zeitraum anzuzeigen.

  Unten (Ereignisse): Beim Darüberfahren zeigt das Popup die Details der Ereignisse an. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinventar“ zu navigieren und alle Ereignisdetails anzuzeigen.

- **MB/s-Zählerdiagramm**

  Das MB/s-Zählerdiagramm zeigt die MB/s-Leistung des Objekts an und gibt an, wie viele Daten in Megabyte pro Sekunde zum und vom Objekt übertragen wurden. Das MB/s-Zählerdiagramm bietet einen umfassenden Überblick über den MB/s-Zustand des Objekts für den vorangegangenen 72-Stunden-Zeitraum.

  Oben (Zählerwert): Die Zahl in der Kopfzeile zeigt die durchschnittliche Anzahl an MB/s für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Leistungsdiagramm): Der Wert unten im Diagramm zeigt die niedrigste Anzahl an MB/s und der Wert oben im Diagramm zeigt die höchste Anzahl an MB/s für den vorangegangenen 72-Stunden-Zeitraum. Positionieren Sie Ihren Cursor über der Trendlinie des Diagramms, um den MB/s-Wert für einen bestimmten Zeitraum anzuzeigen.

  Unten (Ereignisse): Beim Darüberfahren zeigt das Popup die Details der Ereignisse an. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinventar“ zu navigieren und alle Ereignisdetails anzuzeigen.

- **Leistungskapazitäts-Zählerdiagramm**

  Das Zählerdiagramm „Verwendete Leistungskapazität“ zeigt den Prozentsatz der Leistungskapazität an, die vom Objekt verbraucht wird.

  Oben (Zählerwert): Die Zahl in der Kopfzeile zeigt die durchschnittlich genutzte Leistungskapazität der

letzten 72 Stunden an.

Mitte (Leistungsdiagramm): Der Wert unten im Diagramm zeigt den niedrigsten Prozentsatz der genutzten Leistungskapazität und der Wert oben im Diagramm zeigt den höchsten Prozentsatz der genutzten Leistungskapazität für den vorangegangenen 72-Stunden-Zeitraum. Positionieren Sie den Cursor über der Trendlinie des Diagramms, um den Wert der genutzten Leistungskapazität für einen bestimmten Zeitraum anzuzeigen.

Unten (Ereignisse): Beim Darüberfahren zeigt das Popup die Details der Ereignisse an. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinventar“ zu navigieren und alle Ereignisdetails anzuzeigen.

- **Auslastungszählerdiagramm**

  Das Auslastungszählerdiagramm zeigt den Prozentsatz der Objektauslastung an. Das Auslastungszählerdiagramm bietet einen umfassenden Überblick über den Prozentsatz der Objekt- oder Bandbreitenauslastung für den vorangegangenen 72-Stunden-Zeitraum.

  Oben (Zählerwert): Die Zahl in der Kopfzeile zeigt den durchschnittlichen Auslastungsprozentsatz für den vorangegangenen 72-Stunden-Zeitraum an.

  Mitte (Leistungsdiagramm): Der Wert unten im Diagramm zeigt den niedrigsten Auslastungsprozentsatz und der Wert oben im Diagramm zeigt den höchsten Auslastungsprozentsatz für den vorangegangenen 72-Stunden-Zeitraum. Positionieren Sie den Cursor über der Trendlinie des Diagramms, um den Auslastungswert für einen bestimmten Zeitraum anzuzeigen.

  Unten (Ereignisse): Beim Darüberfahren zeigt das Popup die Details der Ereignisse an. Klicken Sie unter dem Diagramm auf den Link **Aktive Ereignisse**, um zur Seite „Ereignisinventar“ zu navigieren und alle Ereignisdetails anzuzeigen.

Veranstaltungen

In der Ereignisverlaufstabelle werden, sofern zutreffend, die aktuellsten Ereignisse aufgelistet, die bei diesem Objekt aufgetreten sind. Wenn Sie auf den Ereignisnamen klicken, werden auf der Seite „Ereignisdetails“ Details zum Ereignis angezeigt.

Komponenten der Performance Explorer-Seite

Auf der Seite „Performance Explorer“ können Sie die Leistung ähnlicher Objekte in einem Cluster vergleichen, beispielsweise aller Volumes in einem Cluster. Dies ist hilfreich bei der Fehlerbehebung bei Leistungsereignissen und der Feinabstimmung der Objektleistung. Sie können Objekte auch mit dem Stammobjekt vergleichen, das die Basislinie darstellt, anhand derer andere Objektvergleiche durchgeführt werden.

Sie können auf die Schaltfläche **Zur Integritätsansicht wechseln** klicken, um die Seite mit den Integritätsdetails für dieses Objekt anzuzeigen. In einigen Fällen können Sie wichtige Informationen zu den Speicherkonfigurationseinstellungen für dieses Objekt erhalten, die bei der Fehlerbehebung hilfreich sein können.

Auf der Seite „Performance Explorer“ wird eine Liste der Clusterobjekte und ihrer Leistungsdaten angezeigt. Auf dieser Seite werden alle Clusterobjekte desselben Typs (z. B. Volumes und ihre objektspezifischen Leistungsstatistiken) in einem tabellarischen Format angezeigt. Diese Ansicht bietet einen effizienten Überblick über die Leistung von Clusterobjekten.

Wenn in einer beliebigen Zelle der Tabelle „N/A“ erscheint, bedeutet dies, dass für diesen Zähler kein Wert verfügbar ist, da derzeit kein E/A für dieses Objekt stattfindet.

Die Seite „Performance Explorer“ enthält die folgenden Komponenten:

- **Zeitraum**

  Ermöglicht Ihnen, einen Zeitbereich für die Objektdaten auszuwählen.

  Sie können einen vordefinierten Bereich auswählen oder Ihren eigenen benutzerdefinierten Zeitbereich angeben.

- **Ansehen und Vergleichen**

  Ermöglicht Ihnen die Auswahl, welcher Typ korrelierter Objekte im Raster angezeigt wird.

  Die verfügbaren Optionen hängen vom Stammobjekttyp und den verfügbaren Daten ab. Sie können auf die Dropdown-Liste „Anzeigen und vergleichen“ klicken, um einen Objekttyp auszuwählen. Der von Ihnen ausgewählte Objekttyp wird in der Liste angezeigt.

- **Filtern**

  Ermöglicht es Ihnen, die Menge der Daten, die Sie erhalten, entsprechend Ihren Präferenzen einzugrenzen.

  Sie können Filter erstellen, die auf die Objektdaten angewendet werden, beispielsweise IOPS größer als 4. Sie können bis zu vier Filter gleichzeitig hinzufügen.

- **Vergleichen**

  Zeigt eine Liste der Objekte an, die Sie zum Vergleich mit dem Stammobjekt ausgewählt haben.

  Daten für die Objekte im Vergleichsbereich werden in den Zählerdiagrammen angezeigt.

- **Statistiken anzeigen in**

  Ermöglicht Ihnen für Volumes und LUNs auszuwählen, ob die Statistiken nach jedem Erfassungszyklus (Standard 5 Minuten) angezeigt werden oder ob die Statistiken als Stundendurchschnitt angezeigt werden. Mit dieser Funktion können Sie das Latenzdiagramm zur Unterstützung des NetApp -Programms „Performance Guarantee“ anzeigen.

- **Zählerdiagramme**

  Zeigt grafische Daten für jede Objektleistungskategorie an.

  Normalerweise werden standardmäßig nur drei oder vier Diagramme angezeigt. Mit der Komponente „Diagramme auswählen“ können Sie zusätzliche Diagramme anzeigen oder bestimmte Diagramme ausblenden. Sie können die Ereigniszeitleiste auch ein- oder ausblenden.

- **Zeitleiste der Ereignisse**

  Zeigt Leistungs- und Integritätsereignisse an, die über die Zeitachse hinweg auftreten, die Sie in der Komponente „Zeitbereich“ ausgewählt haben.

Verwalten der Leistung mithilfe von QoS-Richtliniengruppeninformationen

Mit Unified Manager können Sie die Quality of Service (QoS)-Richtliniengruppen anzeigen, die auf allen von Ihnen überwachten Clustern verfügbar sind. Die Richtlinien wurden möglicherweise mithilfe der ONTAP -Software (System Manager oder ONTAP CLI) oder durch Richtlinien des Unified Manager Performance Service Level definiert. Unified Manager zeigt auch an, welchen Volumes und LUNs eine QoS-Richtliniengruppe zugewiesen ist.

Weitere Informationen zum Anpassen der QoS-Einstellungen finden Sie unter "Übersicht zum Leistungsmanagement"

So kann Speicher-QoS den Workload-Durchsatz steuern

Sie können eine Quality of Service (QoS)-Richtliniengruppe erstellen, um die E/A-pro-Sekunde-Grenze (IOPS) oder den Durchsatz (MB/s) für die darin enthaltenen Workloads zu steuern. Wenn sich die Workloads in einer Richtliniengruppe ohne festgelegtes Limit befinden, beispielsweise in der Standardrichtliniengruppe, oder das festgelegte Limit Ihren Anforderungen nicht entspricht, können Sie das Limit erhöhen oder die Workloads in eine neue oder vorhandene Richtliniengruppe verschieben, die über das gewünschte Limit verfügt.

„Traditionelle“ QoS-Richtliniengruppen können einzelnen Workloads zugewiesen werden, beispielsweise einem einzelnen Volume oder LUN. In diesem Fall kann die Arbeitslast das volle Durchsatzlimit nutzen. QoS-Richtliniengruppen können auch mehreren Workloads zugewiesen werden. In diesem Fall wird die Durchsatzgrenze unter den Workloads „geteilt“. Beispielsweise würde ein QoS-Limit von 9.000 IOPS, das drei Workloads zugewiesen wird, die kombinierten IOPS daran hindern, 9.000 IOPS zu überschreiten.

„Adaptive“ QoS-Richtliniengruppen können auch einzelnen oder mehreren Workloads zugewiesen werden. Allerdings erhält auch bei der Zuweisung zu mehreren Workloads jeder Workload das volle Durchsatzlimit, anstatt den Durchsatzwert mit anderen Workloads zu teilen. Darüber hinaus passen adaptive QoS-Richtlinien die Durchsatzeinstellung automatisch basierend auf der Volumegröße pro Arbeitslast an und behalten so das Verhältnis von IOPS zu Terabyte bei, wenn sich die Volumegröße 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 die Größe des Volumes später auf 20 TB geändert wird, passt die adaptive QoS das Maximum auf 100.000 IOPS an.

Ab ONTAP 9.5 können Sie die Blockgröße beim Definieren einer adaptiven QoS-Richtlinie berücksichtigen. Dadurch wird die Richtlinie effektiv von einem IOPS/TB-Schwellenwert in einen MB/s-Schwellenwert umgewandelt, wenn Workloads sehr große Blockgrößen verwenden und letztendlich einen großen Prozentsatz des Durchsatzes verbrauchen.

Bei gemeinsam genutzten Gruppen-QoS-Richtlinien gilt: Wenn die IOPS oder MB/s aller Workloads in einer Richtliniengruppe den festgelegten Grenzwert überschreiten, drosselt die Richtliniengruppe die Workloads, um ihre Aktivität einzuschränken. Dies kann die Leistung aller Workloads in der Richtliniengruppe verringern. Wenn durch die Drosselung einer Richtliniengruppe ein dynamisches Leistungsereignis generiert wird, wird in der Ereignisbeschreibung der Name der betroffenen Richtliniengruppe angezeigt.

In der Ansicht „Leistung: Alle Volumes“ können Sie die betroffenen Volumes nach IOPS und MB/s sortieren, um zu sehen, welche Workloads die höchste Auslastung aufweisen, die möglicherweise zu dem Ereignis

beigetragen hat. Auf der Seite „Leistung/Volumes-Explorer“ können Sie andere Volumes oder LUNs auf dem Volume auswählen, um sie mit der IOPS- oder MBps-Durchsatznutzung der betroffenen Arbeitslast zu vergleichen.

Indem Sie den Workloads, die die Knotenressourcen übermäßig beanspruchen, eine restriktivere Richtliniengruppeneinstellung zuweisen, drosselt die Richtliniengruppe die Workloads, um ihre Aktivität einzuschränken, wodurch die Nutzung der Ressourcen auf diesem Knoten reduziert werden kann. Wenn Sie jedoch möchten, dass die Arbeitslast mehr Knotenressourcen nutzen kann, können Sie den Wert der Richtliniengruppe erhöhen.

Sie können System Manager, die ONTAP -Befehle oder Unified Manager Performance Service Levels verwenden, um Richtliniengruppen zu verwalten, einschließlich der folgenden Aufgaben:

- Erstellen einer Richtliniengruppe
- Hinzufügen oder Entfernen von Workloads in einer Richtliniengruppe
- Verschieben einer Arbeitslast zwischen Richtliniengruppen
- Ändern des Durchsatzlimits einer Richtliniengruppe
- Verschieben einer Arbeitslast auf ein anderes Aggregat und/oder einen anderen Knoten

Alle auf allen Clustern verfügbaren QoS-Richtliniengruppen anzeigen

Sie können eine Liste aller QoS-Richtliniengruppen anzeigen, die auf den von Unified Manager überwachten Clustern verfügbar sind. Dazu gehören herkömmliche QoS-Richtlinien, adaptive QoS-Richtlinien und QoS-Richtlinien, die von Unified Manager Performance Service Level-Richtlinien verwaltet werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **QoS-Richtliniengruppen**.

   Die Ansicht „Leistung: Traditionelle QoS-Richtliniengruppen“ wird standardmäßig angezeigt.

2. Zeigen Sie die detaillierten Konfigurationseinstellungen für jede verfügbare traditionelle QoS-Richtliniengruppe an.
3. Klicken Sie auf die Schaltfläche „Erweitern“ (⌄) neben dem Namen der QoS-Richtliniengruppe, um weitere Details zur Richtliniengruppe anzuzeigen.
4. Wählen Sie im Menü „Ansicht“ eine der zusätzlichen Optionen aus, um alle adaptiven QoS-Richtliniengruppen anzuzeigen oder um alle QoS-Richtliniengruppen anzuzeigen, die mit Unified Manager Performance Service Levels erstellt wurden.

Anzeigen von Volumes oder LUNs, die sich in derselben QoS-Richtliniengruppe befinden

Sie können eine Liste der Volumes und LUNs anzeigen, die derselben QoS-Richtliniengruppe zugewiesen wurden.

Bei herkömmlichen QoS-Richtliniengruppen, die von mehreren Volumes gemeinsam genutzt werden, kann dies hilfreich sein, um festzustellen, ob bestimmte Volumes den für die Richtliniengruppe definierten Durchsatz überbeanspruchen. Es kann Ihnen auch bei der Entscheidung helfen, ob Sie der Richtliniengruppe weitere Volumes hinzufügen können, ohne dass sich dies negativ auf die anderen Volumes auswirkt.

Bei adaptiven QoS-Richtlinien und Unified Manager Performance Service Levels-Richtlinien kann dies hilfreich sein, um alle Volumes oder LUNs anzuzeigen, die eine Richtliniengruppe verwenden, sodass Sie sehen können, welche Objekte betroffen wären, wenn Sie die Konfigurationseinstellungen für die QoS-Richtlinie ändern würden.

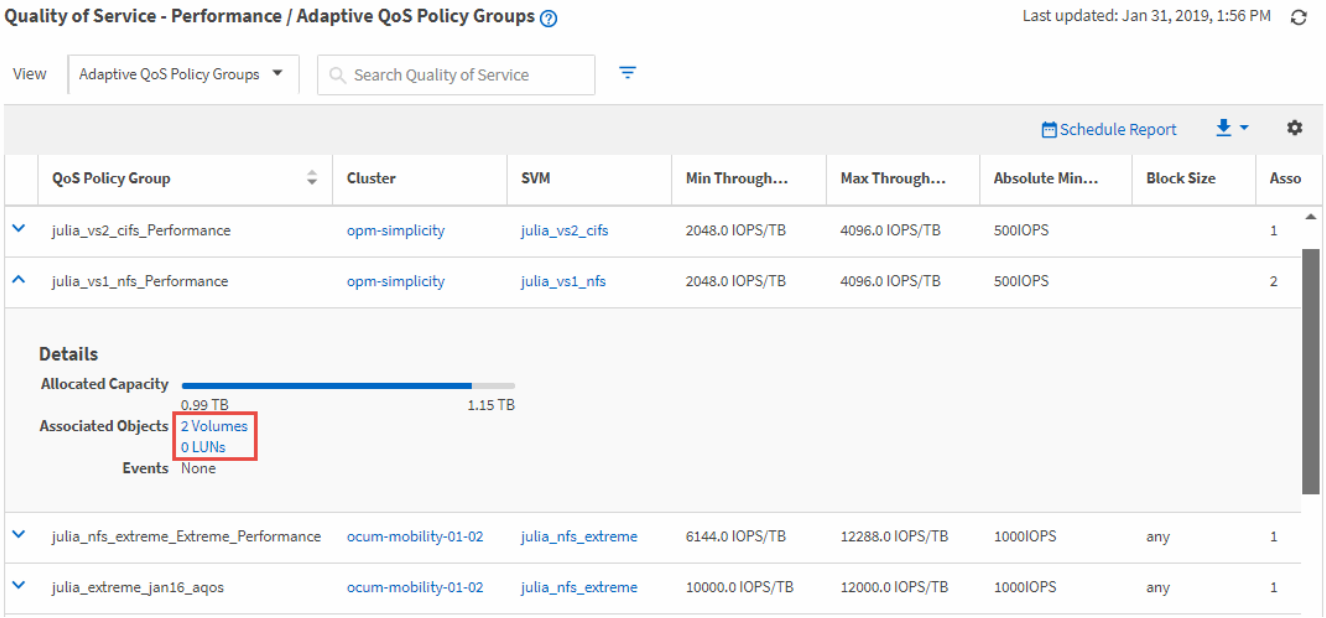
Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **QoS-Richtliniengruppen**.

   Die Ansicht „Leistung: Traditionelle QoS-Richtliniengruppen“ wird standardmäßig angezeigt.

2. Wenn Sie an einer traditionellen Politikgruppe interessiert sind, bleiben Sie auf dieser Seite. Wählen Sie andernfalls eine der zusätzlichen Anzeigeoptionen aus, um alle adaptiven QoS-Richtliniengruppen oder alle QoS-Richtliniengruppen anzuzeigen, die von Unified Manager Performance Service Levels erstellt wurden.

3. Klicken Sie in der QoS-Richtlinie, die Sie interessiert, auf die Schaltfläche zum Erweitern ( ) neben dem Namen der QoS-Richtliniengruppe, um weitere Details anzuzeigen.



4. Klicken Sie auf den Link „Volumes“ oder „LUNs“, um die Objekte anzuzeigen, die diese QoS-Richtlinie verwenden.

   Die Seite „Leistungsinventar“ für Volumes oder LUNs wird mit der sortierten Liste der Objekte angezeigt, die die QoS-Richtlinie verwenden.

Anzeigen der QoS-Richtliniengruppeneinstellungen, die auf bestimmte Volumes oder LUNs angewendet werden

Sie können die QoS-Richtliniengruppen anzeigen, die auf Ihre Volumes und LUNs angewendet wurden, und Sie können eine Verknüpfung zur Ansicht „Leistungs-/QoS-Richtliniengruppen“ herstellen, um die detaillierten Konfigurationseinstellungen für jede QoS-Richtlinie anzuzeigen.

Die Schritte zum Anzeigen der auf ein Volume angewendeten QoS-Richtlinie werden unten angezeigt. Die Schritte zum Anzeigen dieser Informationen für eine LUN sind ähnlich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.

   Die Ansicht „Health: Alle Volumes“ wird standardmäßig angezeigt.

2. Wählen Sie im Menü „Ansicht“ die Option „Leistung: Volumes in der QoS-Richtliniengruppe“ aus.
3. Suchen Sie das Volume, das Sie überprüfen möchten, und scrollen Sie nach rechts, bis Sie die Spalte **QoS-Richtliniengruppe** sehen.
4. Klicken Sie auf den Namen der QoS-Richtliniengruppe.

   Die entsprechende Seite „Quality of Service“ wird angezeigt, je nachdem, ob es sich um eine herkömmliche QoS-Richtlinie, eine adaptive QoS-Richtlinie oder eine QoS-Richtlinie handelt, die mit Unified Manager Performance Service Levels erstellt wurde.

5. Zeigen Sie die detaillierten Konfigurationseinstellungen für die QoS-Richtliniengruppe an.
6. Klicken Sie auf die Schaltfläche „Erweitern“ ( ) neben dem Namen der QoS-Richtliniengruppe, um weitere Details zur Richtliniengruppe anzuzeigen.

Zeigen Sie Leistungsdiagramme an, um Volumes oder LUNs zu vergleichen, die sich in derselben QoS-Richtliniengruppe befinden

Sie können die Volumes und LUNs anzeigen, die sich in denselben QoS-Richtliniengruppen befinden, und dann die Leistung anhand eines einzelnen IOPS-, MB/s- oder IOPS/TB-Diagramms vergleichen, um etwaige Probleme zu identifizieren.

Die Schritte zum Vergleichen der Leistung von Volumes in derselben QoS-Richtliniengruppe werden unten angezeigt. Die Schritte zum Anzeigen dieser Informationen für eine LUN sind ähnlich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.

   Die Ansicht „Health: Alle Volumes“ wird standardmäßig angezeigt.

2. Wählen Sie im Menü „Ansicht“ die Option „Leistung: Volumes in der QoS-Richtliniengruppe“ aus.
3. Klicken Sie auf den Namen des Bandes, den Sie überprüfen möchten.

   Für das Volume wird die Seite „Performance Explorer“ angezeigt.

4. Wählen Sie im Menü „Anzeigen und Vergleichen“ die Option „Volumes in derselben QoS-Richtliniengruppe“ aus.

   Die anderen Volumes mit derselben QoS-Richtlinie sind in der folgenden Tabelle aufgeführt.

5. Klicken Sie auf die Schaltfläche **Hinzufügen**, um diese Volumes zu den Diagrammen hinzuzufügen, damit Sie die IOPS, MB/s, IOPS/TB und andere Leistungsindikatoren für alle ausgewählten Volumes in den Diagrammen vergleichen können.

   Sie können den Zeitbereich ändern, um die Leistung über andere Zeitintervalle als die Standardeinstellung von 72 Stunden anzuzeigen.

So werden verschiedene Arten von QoS-Richtlinien in den Durchsatzdiagrammen angezeigt

Sie können die von ONTAP definierten Quality of Service (QoS)-Richtlinieneinstellungen, die auf ein Volume oder eine LUN angewendet wurden, in den IOPS-, IOPS/TB- und MB/s-Diagrammen des Performance Explorers und der Workload-Analyse anzeigen. Die in den Diagrammen angezeigten Informationen unterscheiden sich je nach Art der QoS-Richtlinie, die auf die Arbeitslast angewendet wurde.

Eine Durchsatzmaximumeinstellung (oder „Spitzenwert“) definiert den maximalen Durchsatz, den die Arbeitslast verbrauchen kann, und begrenzt dadurch die Auswirkungen konkurrierender Arbeitslasten auf die Systemressourcen. Eine Durchsatzminimumeinstellung (oder „erwartete“ Einstellung) definiert den Mindestdurchsatz, der für die Arbeitslast verfügbar sein muss, damit eine kritische Arbeitslast die Mindestdurchsatzziele unabhängig von der Nachfrage durch konkurrierende Arbeitslasten erreicht.

Gemeinsam genutzte 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 „erwartet“ und „Spitze“, um die Unter- und Obergrenze zu definieren.

Während ONTAP Ihnen die Erstellung dieser beiden Arten von QoS-Richtlinien ermöglicht, gibt es je nach Anwendung auf Workloads drei Möglichkeiten, wie die QoS-Richtlinie in den Leistungsdiagrammen angezeigt wird.

Art der Police	Funktionalität	Indikator in der Unified Manager-Schnittstelle
Gemeinsame QoS-Richtlinie, die einer einzelnen Arbeitslast zugewiesen ist, oder nicht gemeinsam genutzte QoS-Richtlinie, die einer einzelnen Arbeitslast oder mehreren Arbeitslasten zugewiesen ist	Jede Arbeitslast kann die angegebene Durchsatzeinstellung verbrauchen	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 verbrauchen	Zeigt „`(QoS Adaptive)`“ an

Die folgende Abbildung zeigt beispielhaft, wie die drei Optionen in den Zählerdiagrammen dargestellt werden.

Wenn im IOPS/TB-Diagramm für eine Arbeitslast eine normale, in IOPS definierte QoS-Richtlinie 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, definiert in IOPS`“ an.

Wenn im IOPS-Diagramm für eine Arbeitslast eine adaptive QoS-Richtlinie angezeigt wird, die in IOPS/TB definiert wurde, 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 – Verwendet, definiert in IOPS/TB“ oder „QoS Adaptive – Zugewiesen, definiert in IOPS/TB“ an, je nachdem, wie die Einstellung für die Spitzen-IOPS-Zuweisung konfiguriert ist. Wenn die Zuweisungseinstellung auf „allocated-space“ eingestellt ist, wird der Spitzen-IOPS basierend auf der Größe des Volumes berechnet. Wenn die Zuordnungseinstellung auf „used-space“ eingestellt ist, wird der Spitzen-IOPS basierend auf der im Volume gespeicherten Datenmenge berechnet, wobei die Speichereffizienz berücksichtigt wird.

Das IOPS/TB-Diagramm zeigt Leistungsdaten nur an, wenn die vom Volume verwendete logische Kapazität größer oder gleich 128 GB ist. Im Diagramm werden Lücken angezeigt, wenn die genutzte Kapazität im ausgewählten Zeitraum unter 128 GB fällt.

Anzeigen der minimalen und maximalen QoS-Einstellungen für die Arbeitslast im Performance Explorer

Sie können die von ONTAP definierten Quality of Service (QoS)-Richtlinieneinstellungen auf einem Volume oder LUN in den Performance Explorer-Diagrammen anzeigen. Eine maximale Durchsatzeinstellung begrenzt die Auswirkungen konkurrierender Arbeitslasten auf die Systemressourcen. Eine Mindestdurchsatzeinstellung stellt sicher, dass eine kritische Arbeitslast die Mindestdurchsatzziele erreicht, unabhängig von der Nachfrage durch konkurrierende Arbeitslasten.

Die IOPS- und MB/s-Einstellungen für den QoS-Durchsatz „minimal“ und „maximal“ werden in den Zählerdiagrammen nur angezeigt, wenn sie in ONTAP konfiguriert wurden. Die Mindestdurchsatzeinstellungen sind nur auf Systemen mit ONTAP 9.2 oder neuerer Software und nur auf AFF -Systemen verfügbar und können derzeit nur für IOPS festgelegt werden.

Adaptive QoS-Richtlinien sind ab ONTAP 9.3 verfügbar und werden mit IOPS/TB statt IOPS ausgedrückt. Diese Richtlinien passen den QoS-Richtlinienwert automatisch basierend auf der Volumegröße pro Arbeitslast an und behalten so das Verhältnis von IOPS zu Terabyte bei, wenn sich die Volumegröße ändert. Sie können eine adaptive QoS-Richtliniengruppe nur auf Volumes anwenden. Für adaptive QoS-Richtlinien werden anstelle von Minimum und Maximum die QoS-Terminologien „erwartet“ und „Spitze“ verwendet.

Unified Manager generiert Warnereignisse für Verstöße gegen die QoS-Richtlinie, wenn der Workload-Durchsatz während jedes Leistungserfassungszeitraums der vorherigen Stunde die definierte maximale QoS-Richtlinieneinstellung überschritten hat. Der Workload-Durchsatz kann den QoS-Schwellenwert während jedes Erfassungszeitraums nur für einen kurzen Zeitraum überschreiten, Unified Manager zeigt jedoch den „durchschnittlichen“ Durchsatz während des Erfassungszeitraums im Diagramm an. Aus diesem Grund werden möglicherweise QoS-Ereignisse angezeigt, obwohl der Durchsatz für eine Arbeitslast den im Diagramm angezeigten Richtlinienschwellenwert möglicherweise nicht überschritten hat.

Schritte

1. Führen Sie auf der Seite **Performance Explorer** für Ihr ausgewähltes Volume oder LUN die folgenden Aktionen aus, um die QoS-Ober- und Untergrenzeneinstellungen anzuzeigen:

Wenn Sie wollen…	Machen Sie Folgendes…
Sehen Sie sich die IOPS-Obergrenze (das QoS-Maximum) an.	Klicken Sie im IOPS-Gesamt- oder Aufschlüsselungsdiagramm auf **Zoom-Ansicht**.
Sehen Sie sich die MB/s-Obergrenze (das QoS-Maximum) an.	Klicken Sie im MB/s-Gesamt- oder Aufschlüsselungsdiagramm auf **Zoom-Ansicht**.

Wenn Sie wollen…	Machen Sie Folgendes…
Zeigen Sie den IOPS-Mindestwert an (das QoS-Mindestniveau).	Klicken Sie im IOPS-Gesamt- oder Aufschlüsselungsdiagramm auf **Zoom-Ansicht**.
Anzeigen der IOPS/TB-Obergrenze (der QoS-Spitze)	Klicken Sie für Volumes im IOPS/TB-Diagramm auf **Zoom-Ansicht**.
Zeigen Sie den IOPS/TB-Mindestwert an (die erwartete QoS).	Klicken Sie für Volumes im IOPS/TB-Diagramm auf **Zoom-Ansicht**.

Die gestrichelte, horizontale Linie zeigt den in ONTAP eingestellten maximalen oder minimalen Durchsatzwert an. Sie können auch sehen, wann Änderungen an den QoS-Werten implementiert wurden.

2. Um die spezifischen IOPS- und MB/s-Werte im Vergleich zur QoS-Einstellung anzuzeigen, bewegen Sie den Cursor in den Diagrammbereich, um das Popup-Fenster anzuzeigen.

Wenn Sie feststellen, dass bestimmte Volumes oder LUNs sehr hohe IOPS oder MB/s aufweisen und die Systemressourcen belasten, können Sie mit System Manager oder der ONTAP CLI die QoS-Einstellungen anpassen, sodass diese Workloads die Leistung anderer Workloads nicht beeinträchtigen.

Weitere Informationen zum Anpassen der QoS-Einstellungen finden Sie unter "Übersicht zum Leistungsmanagement"

Verwalten Sie die Leistung mithilfe von Leistungskapazität und verfügbaren IOPS-Informationen

Die *Leistungskapazität* gibt an, wie viel Durchsatz Sie aus einer Ressource herausholen können, ohne die Nutzleistung dieser Ressource zu überschreiten. Bei der Betrachtung mithilfe vorhandener Leistungsindikatoren ist die Leistungskapazität der Punkt, an dem Sie die maximale Auslastung eines Knotens oder Aggregats erreichen, bevor die Latenz zum Problem wird.

Unified Manager sammelt Leistungskapazitätsstatistiken von Knoten und Aggregaten in jedem Cluster. *Ausgenutzte Leistungskapazität* ist der Prozentsatz der Leistungskapazität, der aktuell genutzt wird, und *Freie Leistungskapazität* ist der Prozentsatz der Leistungskapazität, der noch verfügbar ist.

Während die freie Leistungskapazität einen Prozentsatz der noch verfügbaren Ressource angibt, gibt *verfügbare IOPS* die Anzahl der IOPS an, die der Ressource hinzugefügt werden können, bevor die maximale Leistungskapazität erreicht wird. Durch die Verwendung dieser Metrik können Sie sicher sein, dass Sie einer Ressource Workloads mit einer vorgegebenen Anzahl von IOPS hinzufügen können.

Die Überwachung der Leistungskapazitätsinformationen bietet folgende Vorteile:

- Hilft bei der Bereitstellung und dem Ausgleich von Arbeitsabläufen.
- Hilft Ihnen, die Überlastung eines Knotens oder die Nutzung seiner Ressourcen über den optimalen Punkt hinaus zu verhindern und so den Bedarf an Fehlerbehebung zu reduzieren.
- Hilft Ihnen, präziser zu bestimmen, wo zusätzliche Speicherausrüstung benötigt werden könnte.

Welche Leistungsfähigkeit wird genutzt

Mithilfe des Leistungsindikators „Verwendete Leistungskapazität“ können Sie feststellen, ob die Leistung eines Knotens oder eines Aggregats einen Punkt erreicht, an dem die Leistung bei zunehmender Arbeitslast nachlassen könnte. Es kann Ihnen auch zeigen, ob ein Knoten oder Aggregat derzeit während bestimmter Zeiträume überbeansprucht wird. Die verwendete Leistungskapazität ähnelt der Auslastung, bietet jedoch mehr Einblick in die verfügbaren Leistungskapazitäten einer physischen Ressource für eine bestimmte Arbeitslast.

Die optimal genutzte Leistungskapazität ist der Punkt, an dem ein Knoten oder ein Aggregat eine optimale Auslastung und Latenz (Reaktionszeit) aufweist und effizient genutzt wird. In der folgenden Abbildung wird eine Beispielkurve der Latenz im Vergleich zur Auslastung für ein Aggregat angezeigt.

In diesem Beispiel gibt der *Betriebspunkt* an, dass das Aggregat derzeit mit einer Auslastung von 50 % und einer Latenz von 1,0 ms/Operation arbeitet. Basierend auf den aus dem Aggregat erfassten Statistiken ermittelt Unified Manager, dass für dieses Aggregat zusätzliche Leistungskapazität verfügbar ist. In diesem Beispiel wird der *optimale Punkt* als der Punkt identifiziert, an dem das Aggregat zu 80 % ausgelastet ist und eine Latenz von 2,0 ms/Operation aufweist. Daher können Sie diesem Aggregat weitere Volumes und LUNs hinzufügen, sodass Ihre Systeme effizienter genutzt werden.

Der Zähler für die genutzte Leistungskapazität dürfte einen höheren Wert aufweisen als der Zähler „Auslastung“, da die Leistungskapazität die Latenz zusätzlich beeinflusst. Wenn beispielsweise ein Knoten oder Aggregat zu 70 % ausgelastet ist, kann der Leistungskapazitätswert je nach Latenzwert im Bereich von 80 % bis 100 % liegen.

In einigen Fällen kann der Auslastungszähler auf der Dashboard-Seite jedoch höher sein. Dies ist normal, da das Dashboard die aktuellen Zählerwerte in jedem Erfassungszeitraum aktualisiert. Es zeigt keine Durchschnittswerte über einen bestimmten Zeitraum an, wie die anderen Seiten in der Benutzeroberfläche von Unified Manager. Der Leistungskapazitätszähler eignet sich am besten als Indikator für die über einen bestimmten Zeitraum gemittelte Leistung, während der Auslastungszähler am besten zur Ermittlung der momentanen Nutzung einer Ressource verwendet wird.

Was der Leistungskapazitäts-Gebrauchswert bedeutet

Der Wert der genutzten Leistungskapazität hilft Ihnen, die Knoten und Aggregate zu identifizieren, die derzeit über- oder unterausgelastet sind. Auf diese Weise können Sie Arbeitslasten neu verteilen, um Ihre Speicherressourcen effizienter zu nutzen.

Die folgende Abbildung zeigt die Latenz-Auslastungskurve für eine Ressource und identifiziert mit farbigen Punkten drei Bereiche, in denen sich der aktuelle Betriebspunkt befinden könnte.

- Ein Prozentsatz der Leistungsauslastung von 100 liegt am optimalen Punkt.

  Ressourcen werden an dieser Stelle effizient genutzt.

- Ein Prozentsatz der genutzten Leistungskapazität über 100 weist darauf hin, dass der Knoten oder das Aggregat überlastet ist und die Leistung der Workloads nicht optimal ist.

  Der Ressource sollten keine neuen Workloads hinzugefügt werden und die vorhandenen Workloads müssen möglicherweise neu verteilt werden.

- Ein Prozentsatz der genutzten Leistungskapazität unter 100 weist darauf hin, dass der Knoten oder das Aggregat nicht ausreichend ausgelastet ist und die Ressourcen nicht effektiv genutzt werden.

  Der Ressource können weitere Workloads hinzugefügt werden.

Im Gegensatz zur Auslastung kann der Prozentsatz der genutzten Leistungskapazität über 100 % liegen. Es gibt keinen maximalen Prozentsatz, aber bei einer Überauslastung der Ressourcen liegen diese normalerweise im Bereich zwischen 110 % und 140 %. Höhere Prozentsätze weisen auf eine Ressource mit schwerwiegenden Problemen hin.

Welche IOPS sind verfügbar?

Der Zähler für verfügbare IOPS gibt die verbleibende Anzahl an IOPS an, die einem Knoten oder einem Aggregat hinzugefügt werden können, bevor die Ressource ihr Limit erreicht.

Die Gesamt-IOPS, die ein Knoten bereitstellen kann, basieren auf den physischen Eigenschaften des Knotens, beispielsweise der Anzahl der CPUs, der CPU-Geschwindigkeit und der RAM-Menge. Die Gesamt-IOPS, die ein Aggregat bereitstellen kann, basieren auf den physischen Eigenschaften der Datenträger, beispielsweise einem SATA-, SAS- oder SSD-Datenträger.

Die Gesamt-IOPS aller Volumes in einem Aggregat stimmen möglicherweise nicht mit der Gesamt-IOPS des Aggregats überein. Dies wird im folgenden Knowledge Base-Artikel erläutert: KB"Warum stimmt die Summe aller Volume-IOPs in einem Aggregat nicht mit den aggregierten IOPs überein?"

Während der Zähler für die freie Leistungskapazität den Prozentsatz einer Ressource angibt, der noch verfügbar ist, gibt der Zähler für verfügbare IOPS die genaue Anzahl an IOPS (Workloads) an, die einer Ressource hinzugefügt werden können, bevor die maximale Leistungskapazität erreicht wird.

Wenn Sie beispielsweise ein Paar FAS2520- und FAS8060-Speichersysteme verwenden, bedeutet ein freier Leistungskapazitätswert von 30 %, dass Sie über freie Leistungskapazität verfügen. Dieser Wert gibt jedoch keinen Aufschluss darüber, wie viele weitere Workloads Sie auf diesen Knoten bereitstellen können. Der Zähler für verfügbare IOPS zeigt möglicherweise an, dass auf dem FAS8060 500 IOPS verfügbar sind, auf dem FAS2520 jedoch nur 100 IOPS.

In der folgenden Abbildung wird eine Beispielkurve der Latenz im Vergleich zu IOPS für einen Knoten angezeigt.

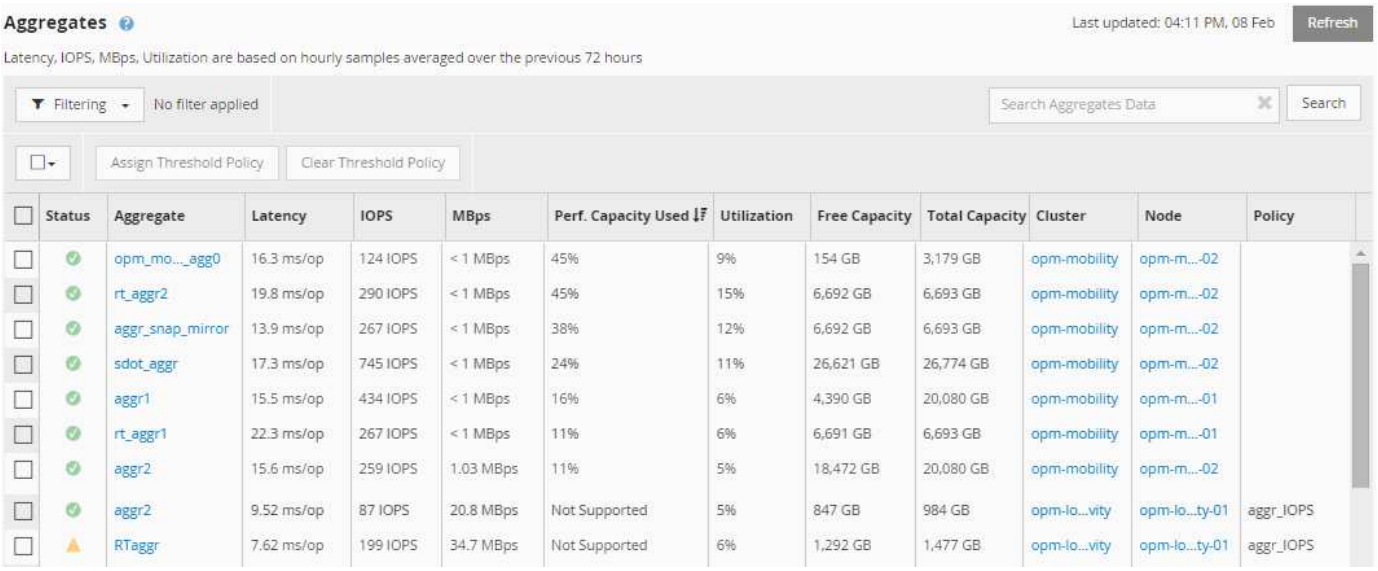
Die maximale Anzahl an IOPS, die eine Ressource bereitstellen kann, ist die Anzahl an IOPS, wenn der Leistungskapazitätszähler bei 100 % liegt (dem optimalen Punkt). Der Betriebspunkt gibt an, dass der Knoten derzeit mit 100.000 IOPS und einer Latenz von 1,0 ms/Operation arbeitet. Basierend auf den vom Knoten erfassten Statistiken ermittelt Unified Manager, dass die maximalen IOPS für den Knoten 160.000 betragen, was bedeutet, dass 60.000 freie oder verfügbare IOPS vorhanden sind. Daher können Sie diesem Knoten weitere Workloads hinzufügen, sodass Ihre Systeme effizienter genutzt werden.

Bei minimaler Benutzeraktivität in der Ressource wird der verfügbare IOPS-Wert unter der Annahme einer allgemeinen Arbeitslast berechnet, die auf etwa 4.500 IOPS pro CPU-Kern basiert. Dies liegt daran, dass Unified Manager nicht über die Daten verfügt, um die Eigenschaften der zu verarbeitenden Arbeitslast genau einzuschätzen.

Anzeigen der verwendeten Knoten- und aggregierten Leistungskapazitätswerte

Sie können die Werte der genutzten Leistungskapazität für alle Knoten oder für alle Aggregate in einem Cluster überwachen oder Details für einen einzelnen Knoten oder ein Aggregat anzeigen.

Die Werte für die genutzte Leistungskapazität werden im Dashboard, auf den Seiten „Leistungsinventar“, auf der Seite „Top-Performer“, auf der Seite „Schwellenwertrichtlinie erstellen“, auf den Seiten des Leistungs-Explorers und in Detaildiagrammen angezeigt. Beispielsweise enthält die Seite „Leistung: Alle Aggregate“ eine Spalte „Verwendete Leistungskapazität“, um den Wert der verwendeten Leistungskapazität für alle Aggregate anzuzeigen.



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

Durch die Überwachung des Leistungskapazitätsverbrauchsindikators können Sie Folgendes ermitteln:

- Ob Knoten oder Aggregate auf Clustern einen hohen Leistungskapazitätswert aufweisen
- Ob Knoten oder Aggregate auf Clustern aktive Ereignisse zur Nutzung der Leistungskapazität haben
- Die Knoten und Aggregate mit dem höchsten und niedrigsten Leistungskapazitätswert in einem Cluster
- Latenz- und Auslastungsindikatorwerte in Verbindung mit Knoten oder Aggregaten, die über hohe Leistungskapazitätswerte verfügen
- Wie sich der Ausfall eines Knotens auf die Werte der genutzten Leistungskapazität für Knoten in einem HA-Paar auswirkt
- Die am stärksten ausgelasteten Volumes und LUNs auf einem Aggregat mit einem hohen Leistungskapazitätswert

Knoten anzeigen und verfügbare IOPS-Werte aggregieren

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 Aggregat anzeigen.

Verfügbare IOPS-Werte werden auf den Seiten „Leistungsinventar“ und in den Diagrammen der Seite „Leistungs-Explorer“ für Knoten und Aggregate angezeigt. Wenn Sie beispielsweise einen Knoten auf der Seite „Knoten-/Leistungs-Explorer“ anzeigen, können Sie das Zählerdiagramm „Verfügbare IOPS“ aus der Liste auswählen, um die verfügbaren IOPS-Werte für den Knoten und mehrere Aggregate auf diesem Knoten zu vergleichen.

Durch die Überwachung des verfügbaren IOPS-Zählers können Sie Folgendes ermitteln:

- Die Knoten oder Aggregate mit den höchsten verfügbaren IOPS-Werten helfen bei der Bestimmung, wo zukünftige Workloads bereitgestellt werden können.
- Die Knoten oder Aggregate mit den kleinsten verfügbaren IOPS-Werten, um die Ressourcen zu identifizieren, die Sie auf potenzielle zukünftige Leistungsprobleme überwachen sollten.
- Die am stärksten ausgelasteten Volumes und LUNs auf einem Aggregat mit einem kleinen verfügbaren IOPS-Wert.

Zeigen Sie Leistungskapazitätsindikatordiagramme an, um Probleme zu identifizieren

Sie können Diagramme zur genutzten Leistungskapazität für Knoten und Aggregate auf der Seite „Performance Explorer“ anzeigen. Auf diese Weise können Sie detaillierte Leistungskapazitätsdaten für die ausgewählten Knoten und Aggregate für einen bestimmten Zeitraum anzeigen.

Das Standard-Zählerdiagramm zeigt die Werte der genutzten Leistungskapazität für die ausgewählten Knoten oder Aggregate an. Das Diagramm „Aufschlüsselungszähler“ zeigt die Gesamtleistungskapazitätswerte für das Stammobjekt an, getrennt nach Nutzung basierend auf Benutzerprotokollen und Hintergrundsystemprozessen. Zusätzlich wird auch die Höhe der freien Leistungskapazität angezeigt.

> Da einige Hintergrundaktivitäten im Zusammenhang mit der System- und Datenverwaltung als Benutzerarbeitslasten identifiziert und als Benutzerprotokolle kategorisiert werden, kann der Prozentsatz der Benutzerprotokolle bei der Ausführung dieser Prozesse künstlich hoch erscheinen. Diese Prozesse werden normalerweise gegen Mitternacht ausgeführt, wenn die Clusterauslastung gering ist. Wenn Sie gegen Mitternacht einen Anstieg der Benutzerprotokollaktivität feststellen, überprüfen Sie, ob Cluster-Sicherungsaufträge oder andere Hintergrundaktivitäten für die Ausführung zu dieser Zeit konfiguriert sind.

Schritte

1. Wählen Sie die Registerkarte **Explorer** auf einer Knoten- oder aggregierten **Landingpage** aus.
2. Klicken Sie im Bereich **Zählerdiagramme** auf **Diagramme auswählen** und wählen Sie dann **Perf. Diagramm „Genutzte Kapazität**“.
3. Scrollen Sie nach unten, bis Sie das Diagramm anzeigen können.

   Die Farben des Standarddiagramms zeigen an, wann sich das Objekt im optimalen Bereich befindet (gelb), wann das Objekt unterausgelastet ist (grün) und wann das Objekt überausgelastet ist (rot). Das Aufschlüsselungsdiagramm zeigt detaillierte Leistungskapazitätsdetails nur für das Stammobjekt.

4. Wenn Sie eines der Diagramme in voller Größe anzeigen möchten, klicken Sie auf **Zoom-Ansicht**.

   Auf diese Weise können Sie mehrere Zählerdiagramme in einem separaten Fenster öffnen, um die Werte der genutzten Leistungskapazität mit IOPS- oder MBps-Werten über denselben Zeitraum zu vergleichen.

Leistungskapazität genutzte Leistungsschwellenbedingungen

Sie können benutzerdefinierte Richtlinien für Leistungsschwellenwerte erstellen, sodass Ereignisse ausgelöst werden, wenn der Wert für die genutzte Leistungskapazität für

einen Knoten oder ein Aggregat die definierte Einstellung für den Schwellenwert für die genutzte Leistungskapazität überschreitet.

Darüber hinaus können Knoten mit einer Schwellenwertrichtlinie „`Übernahme der genutzten Leistungskapazität`“ konfiguriert werden. Diese Schwellenwertrichtlinie summiert die Statistiken zur verwendeten Leistungskapazität für beide Knoten in einem HA-Paar, um zu bestimmen, ob einem der Knoten bei einem Ausfall des anderen Knotens die Kapazität fehlen würde. Da die Arbeitslast während des Failovers die Kombination der Arbeitslasten der beiden Partnerknoten ist, kann auf beide Knoten dieselbe Übernahmerichtlinie für die genutzte Leistungskapazität angewendet werden.

> Diese Äquivalenz der genutzten Leistungskapazität gilt im Allgemeinen zwischen Knoten. Wenn jedoch über den Failover-Partner deutlich mehr knotenübergreifender Datenverkehr für einen der Knoten bestimmt ist, kann die Gesamtleistungskapazität, die beim Ausführen aller Workloads auf einem Partnerknoten im Vergleich zum anderen Partnerknoten verwendet wird, je nachdem, welcher Knoten ausgefallen ist, leicht unterschiedlich sein.

Die Bedingungen für die genutzte Leistungskapazität können auch als sekundäre Leistungsschwellenwerteinstellungen verwendet werden, um beim Definieren von Schwellenwerten für LUNs und Volumes eine kombinierte Schwellenwertrichtlinie zu erstellen. Die Bedingung „Leistungskapazität genutzt“ wird auf das Aggregat oder den Knoten angewendet, auf dem sich das Volume oder die LUN befindet. Sie können beispielsweise eine kombinierte Schwellenwertrichtlinie anhand der folgenden Kriterien erstellen:

Speicherobjekt	Leistungsindikator	Warnschwelle	Kritischer Schwellenwert	Dauer
Volumen	Latenz	15 ms/Operation	25 ms/Operation	20 Minuten
Aggregat	Ausgenutzte Leistungskapazität	80 %	95 %	

Kombinationsschwellenwertrichtlinien führen dazu, dass ein Ereignis nur dann generiert wird, wenn beide Bedingungen während der gesamten Dauer verletzt werden.

Verwenden Sie den Leistungskapazitätszähler, um die Leistung zu verwalten

Normalerweise möchten Unternehmen mit einem Prozentsatz der genutzten Leistungskapazität von unter 100 arbeiten, damit die Ressourcen effizient genutzt werden und gleichzeitig zusätzliche Leistungskapazität zur Unterstützung der Nachfrage in Spitzenzeiten reserviert bleibt. Mithilfe von Schwellenwertrichtlinien können Sie anpassen, wann Warnmeldungen für Werte zur Kapazitätsauslastung bei hoher Leistung gesendet werden.

Sie können anhand Ihrer Leistungsanforderungen konkrete Ziele festlegen. Beispielsweise könnten Finanzdienstleistungsunternehmen mehr Leistungskapazität reservieren, um die rechtzeitige Ausführung von Handelsgeschäften zu gewährleisten. Diese Unternehmen möchten möglicherweise Schwellenwerte für die genutzte Leistungskapazität im Bereich von 70–80 Prozent festlegen. Fertigungsunternehmen mit geringeren Margen könnten sich dafür entscheiden, weniger Leistungskapazität zu reservieren, wenn sie bereit sind, Leistungsrisiken einzugehen, um die IT-Kosten besser im Griff zu haben. Diese Unternehmen legen möglicherweise Schwellenwerte für die Auslastung der Leistungskapazität im Bereich von 85 bis 95 Prozent fest.

Wenn der Wert der genutzten Leistungskapazität den in einer benutzerdefinierten Schwellenwertrichtlinie festgelegten Prozentsatz überschreitet, sendet Unified Manager eine Warn-E-Mail und fügt das Ereignis der Seite „Ereignisinventar“ hinzu. Auf diese Weise können Sie potenzielle Probleme beheben, bevor sie die Leistung beeinträchtigen. Diese Ereignisse können auch als Indikatoren dafür verwendet werden, dass Sie Workload-Verschiebungen und Änderungen innerhalb Ihrer Knoten und Aggregate vornehmen müssen.

Verstehen und Verwenden der Seite „Knoten-Failover-Planung“

Auf der Seite „Leistung/Knoten-Failover-Planung“ werden die Leistungseinbußen für einen Knoten geschätzt, wenn der Hochverfügbarkeits-Partnerknoten (HA) des Knotens ausfällt. Unified Manager stützt seine Schätzungen auf die historische Leistung der Knoten im HA-Paar.

Durch die Abschätzung der Auswirkungen eines Failovers auf die Leistung können Sie in den folgenden Szenarien planen:

- Wenn ein Failover die geschätzte Leistung des Übernahmeknotens dauerhaft auf ein inakzeptables Niveau verschlechtert, können Sie Korrekturmaßnahmen in Betracht ziehen, um die Leistungseinbußen durch ein Failover zu reduzieren.
- Bevor Sie ein manuelles Failover zur Durchführung von Hardwarewartungsaufgaben einleiten, können Sie abschätzen, wie sich das Failover auf die Leistung des Übernahmeknotens auswirkt, um den besten Zeitpunkt für die Durchführung der Aufgabe zu bestimmen.

Verwenden Sie die Seite „Knoten-Failover-Planung“, um Korrekturmaßnahmen festzulegen

Basierend auf den Informationen, die auf der Seite „Leistungs-/Knoten-Failover-Planung“ angezeigt werden, können Sie Maßnahmen ergreifen, um sicherzustellen, dass ein Failover nicht dazu führt, dass die Leistung eines HA-Paares unter ein akzeptables Niveau fällt.

Um beispielsweise die geschätzten Auswirkungen eines Failovers auf die Leistung zu reduzieren, 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 Leistung liefern kann.

Komponenten der Seite „Knoten-Failover-Planung“

Die Komponenten der Seite „Leistung/Knoten-Failover-Planung“ werden in einem Raster und im Vergleichsbereich angezeigt. Mithilfe dieser Abschnitte können Sie die Auswirkungen eines Knoten-Failovers auf die Leistung des Übernahmeknotens beurteilen.

Leistungsstatistikraster

Auf der Seite „Leistung/Knoten-Failover-Planung“ wird ein Raster mit Statistiken zu Latenz, IOPS, Auslastung und verwendeter Leistungskapazität angezeigt.

Die auf dieser Seite und auf der Seite „Leistung/Knotenleistungs-Explorer“ angezeigten Latenz- und IOPS-Werte stimmen möglicherweise nicht überein, da zum Berechnen der Werte zur Vorhersage des Knoten-Failovers unterschiedliche Leistungsindikatoren verwendet werden.

Im Raster wird jedem Knoten eine der folgenden Rollen zugewiesen:

- Primär

  Der Knoten, der die Aufgaben 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 der primäre Knoten. Die für diesen Knoten angezeigten Leistungsstatistiken zeigen die Leistung des Übernahmeknotens, nachdem er den ausgefallenen Partner übernommen hat.

Obwohl die Arbeitslast des Übernahmeknotens nach einem Failover der kombinierten Arbeitslast beider Knoten entspricht, sind die Statistiken für den geschätzten Übernahmeknoten nicht die Summe der Statistiken des primären Knotens und des Partnerknotens. Wenn beispielsweise die Latenz des primären Knotens 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 Partnerknotens klicken, wenn dieser zum Stammobjekt werden soll. Nachdem die Seite „Leistung/Knotenleistungs-Explorer“ angezeigt wurde, können Sie auf die Registerkarte **Failover-Planung** klicken, um zu sehen, wie sich die Leistung in diesem Knotenausfallszenario ändert. Wenn beispielsweise Knoten1 der primäre Knoten und Knoten2 der Partnerknoten ist, können Sie auf Knoten2 klicken, um ihn zum primären Knoten zu machen. Auf diese Weise können Sie sehen, wie sich die geschätzte Leistung ändert, je nachdem, welcher Knoten ausfällt.

Vergleichsbereich

Die folgende Liste beschreibt die Komponenten, die standardmäßig im Vergleichsbereich angezeigt werden:

- **Ereignisdiagramme**

  Sie werden im gleichen Format wie auf der Seite „Performance/Node Performance Explorer“ angezeigt. Sie beziehen sich nur auf den primären Knoten.

- **Zählerdiagramme**

  Sie zeigen historische Statistiken für den im Raster angezeigten Leistungsindikator an. In jedem Diagramm zeigt das Diagramm für den Knoten „Geschätzte Übernahme“ die geschätzte Leistung, wenn zu einem bestimmten Zeitpunkt ein Failover stattgefunden hätte.

  Nehmen wir beispielsweise an, dass das Auslastungsdiagramm für den Knoten „Geschätzte Übernahme“ am 8. Februar um 11 Uhr 73 % anzeigt. Wenn zu diesem Zeitpunkt ein Failover stattgefunden hätte, hätte die Auslastung des Übernahmeknotens 73 % betragen.

  Mithilfe der Verlaufsstatistiken können Sie den optimalen Zeitpunkt für die Einleitung eines Failovers

ermitteln und so die Möglichkeit einer Überlastung des Übernahmeknotens minimieren. Sie können ein Failover nur zu Zeiten planen, zu denen die prognostizierte Leistung des Übernahmeknotens akzeptabel ist.

Standardmäßig werden im Vergleichsbereich Statistiken sowohl für das Stammobjekt als auch für den Partnerknoten angezeigt. Anders als auf der Seite „Leistung/Knotenleistungs-Explorer“ wird auf dieser Seite nicht die Schaltfläche **Hinzufügen** angezeigt, mit der Sie Objekte zum Statistikvergleich hinzufügen können.

Sie können den Vergleichsbereich auf die gleiche Weise anpassen wie auf der Seite „Leistung/Knotenleistungs-Explorer“. Die folgende Liste zeigt Beispiele für die Anpassung der Diagramme:

- Klicken Sie auf einen Knotennamen, um die Statistiken des Knotens in den Zählerdiagrammen anzuzeigen oder auszublenden.
- Klicken Sie auf **Zoom-Ansicht**, um ein detailliertes Diagramm für einen bestimmten Zähler in einem neuen Fenster anzuzeigen.

Verwenden einer Schwellenwertrichtlinie mit der Seite „Knoten-Failover-Planung“

Sie können eine Knotenschwellenwertrichtlinie erstellen, sodass Sie auf der Seite „Leistung/Knoten-Failover-Planung“ benachrichtigt werden, wenn ein potenzielles Failover die Leistung des Übernahmeknotens auf ein inakzeptables Niveau beeinträchtigen würde.

Die systemdefinierte Leistungsschwellenwertrichtlinie mit dem Namen „Node HA pair over-utilized“ generiert ein Warnereignis, wenn der Schwellenwert sechs aufeinanderfolgende Erfassungszeiträume (30 Minuten) lang überschritten wird. Der Schwellenwert gilt als überschritten, wenn die kombinierte Leistungskapazität der Knoten in einem HA-Paar 200 % überschreitet.

Das Ereignis aus der systemdefinierten Schwellenwertrichtlinie weist Sie darauf hin, dass ein Failover dazu führt, dass die Latenz des Übernahmeknotens auf ein inakzeptables Niveau ansteigt. Wenn Sie ein Ereignis sehen, das von dieser Richtlinie für einen bestimmten Knoten generiert wird, können Sie zur Seite „Leistung/Knoten-Failover-Planung“ für diesen Knoten navigieren, um den vorhergesagten Latenzwert aufgrund eines Failovers anzuzeigen.

Zusätzlich zur Verwendung dieser systemdefinierten Schwellenwertrichtlinie können Sie Schwellenwertrichtlinien mithilfe des Zählers „Verwendete Leistungskapazität – Übernahme“ erstellen und die Richtlinie dann auf ausgewählte Knoten anwenden. Wenn Sie einen Schwellenwert unter 200 % angeben, können Sie ein Ereignis empfangen, bevor der Schwellenwert für die systemdefinierte Richtlinie überschritten wird. Sie können den Mindestzeitraum, für den der Schwellenwert überschritten wird, auch auf weniger als 30 Minuten festlegen, wenn Sie benachrichtigt werden möchten, bevor das systemdefinierte Richtlinienereignis generiert wird.

Sie können beispielsweise eine Schwellenwertrichtlinie definieren, um ein Warnereignis zu generieren, wenn die kombinierte Leistungskapazität der Knoten in einem HA-Paar länger als 10 Minuten 175 % überschreitet. Sie können diese Richtlinie auf Knoten1 und Knoten2 anwenden, die ein HA-Paar bilden. Nachdem Sie eine Warnereignisbenachrichtigung für Knoten1 oder Knoten2 erhalten haben, können Sie die Seite „Leistung/Knoten-Failover-Planung“ für diesen Knoten anzeigen, um die geschätzten Auswirkungen auf die Leistung des Übernahmeknotens zu beurteilen. Sie können Korrekturmaßnahmen ergreifen, um eine Überlastung des Übernahmeknotens zu vermeiden, wenn es zu einem Failover kommt. Wenn Sie Maßnahmen ergreifen, wenn die kombinierte Leistungskapazität der Knoten unter 200 % liegt, erreicht die Latenz des Übernahmeknotens kein inakzeptables Niveau, selbst wenn während dieser Zeit ein Failover stattfindet.

Verwenden Sie das Diagramm „Aufschlüsselung der genutzten Leistungskapazität“ für die Failover-Planung

Das detaillierte Diagramm „Verwendete Leistungskapazität – Aufschlüsselung“ zeigt die für den primären Knoten und den Partnerknoten verwendete Leistungskapazität. Außerdem wird die Menge der freien Leistungskapazität auf dem geschätzten Übernahmeknoten angezeigt. Mithilfe dieser Informationen können Sie feststellen, ob bei einem Ausfall des Partnerknotens möglicherweise ein Leistungsproblem auftritt.

Das Aufschlüsselungsdiagramm zeigt nicht nur die gesamte für die Knoten genutzte Leistungskapazität an, sondern unterteilt die Werte für jeden Knoten auch in Benutzerprotokolle und Hintergrundprozesse.

- Benutzerprotokolle sind die E/A-Vorgänge von Benutzeranwendungen zum und vom Cluster.
- Hintergrundprozesse sind die internen Systemprozesse, die an der Speichereffizienz, der Datenreplikation und der Systemintegrität beteiligt sind.

Mit dieser zusätzlichen Detailebene können Sie feststellen, ob ein Leistungsproblem durch die Anwendungsaktivität des Benutzers oder durch Hintergrundsystemprozesse wie Deduplizierung, RAID-Rekonstruktion, Festplattenbereinigung und SnapMirror Kopien verursacht wird.

Schritte

1. Gehen Sie zur Seite **Leistung/Knoten-Failover-Planung** für den Knoten, der als geschätzter Übernahmeknoten dienen soll.
2. Wählen Sie im Auswahlfeld **Zeitbereich** den Zeitraum aus, für den die historischen Statistiken im Zählerraster und in den Zählerdiagrammen angezeigt werden.

   Die Zählerdiagramme mit Statistiken für den Primärknoten, den Partnerknoten und den geschätzten Übernahmeknoten werden angezeigt.
3. Wählen Sie aus der Liste **Diagramme auswählen** die Option **Perf. Verwendete Kapazität**.
4. Im *Perf. Wählen Sie im Diagramm „Kapazitätsnutzung“ die Option „Aufschlüsselung“ und klicken Sie auf „Zoom-Ansicht“.

   Das detaillierte Diagramm für Perf. Die verwendete Kapazität wird angezeigt.
5. Bewegen Sie den Cursor über das detaillierte Diagramm, um die Informationen zur genutzten Leistungskapazität im Popup-Fenster anzuzeigen.

   Die Perf. Der Prozentsatz der freien Kapazität ist die auf dem geschätzten Übernahmeknoten verfügbare Leistungskapazität. Es gibt an, wie viel Leistungskapazität nach einem Failover auf dem Übernahmeknoten übrig bleibt. Wenn der Wert 0 % beträgt, führt ein Failover dazu, dass die Latenz auf dem Übernahmeknoten auf ein inakzeptables Niveau ansteigt.
6. Erwägen Sie Korrekturmaßnahmen, um einen niedrigen Leistungskapazitäts-Freiprozentsatz zu vermeiden.

   Wenn Sie planen, zur Knotenwartung ein Failover einzuleiten, wählen Sie einen Zeitpunkt für den Ausfall des Partnerknotens, bei dem der Prozentsatz der freien Leistungskapazität nicht bei 0 liegt.

Sammeln Sie Daten und überwachen Sie die Workload-Leistung

Unified Manager erfasst und analysiert alle 5 Minuten die Workload-Aktivität, um Leistungsereignisse zu identifizieren, und erkennt alle 15 Minuten Konfigurationsänderungen. Es speichert maximal 30 Tage lang 5-minütige historische Leistungs- und Ereignisdaten und verwendet diese Daten, um den erwarteten Latenzbereich für alle überwachten Workloads vorherzusagen.

Unified Manager muss mindestens 3 Tage Workload-Aktivität erfassen, bevor es mit der Analyse beginnen kann und bevor die Latenzprognose für die E/A-Reaktionszeit auf der Seite „Workload-Analyse“ und auf der Seite „Ereignisdetails“ angezeigt werden kann. Während diese Aktivität erfasst wird, zeigt die Latenzprognose nicht alle Änderungen an, die durch die Workload-Aktivität auftreten. Nach der Erfassung der Aktivität von drei Tagen passt Unified Manager die Latenzprognose alle 24 Stunden um 0:00 Uhr an, um Änderungen der Arbeitslastaktivität widerzuspiegeln und einen genaueren dynamischen Leistungsschwellenwert festzulegen.

Wenn während der ersten vier Tage, in denen Unified Manager eine Arbeitslast überwacht, seit der letzten Datenerfassung mehr als 24 Stunden vergangen sind, zeigen die Latenzdiagramme die Latenzprognose für diese Arbeitslast nicht an. Vor der letzten Erfassung erkannte Ereignisse sind weiterhin verfügbar.

Durch die Sommerzeit (DST) wird die Systemzeit geändert, wodurch sich die Latenzprognose der Leistungsstatistiken für überwachte Workloads ändert. Unified Manager beginnt sofort mit der Korrektur der Latenzprognose, was etwa 15 Tage dauert. Während dieser Zeit können Sie Unified Manager weiterhin verwenden. Da Unified Manager jedoch die Latenzprognose zum Erkennen dynamischer Ereignisse verwendet, sind einige Ereignisse möglicherweise nicht genau. Vor der Zeitumstellung erkannte Ereignisse sind davon nicht betroffen.

Von Unified Manager überwachte Workloadtypen

Mit Unified Manager können Sie die Leistung von zwei Arten von Workloads überwachen: benutzerdefiniert und systemdefiniert.

- ***Benutzerdefinierte Workloads***

  Der E/A-Durchsatz von Anwendungen 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 Arbeitslast sind benutzerdefinierte Arbeitslasten.

  Unified Manager überwacht nur die Workload-Aktivität im Cluster. Es überwacht weder die Anwendungen, die Clients noch die Pfade zwischen den Anwendungen und dem Cluster.

  Wenn eine oder mehrere der folgenden Bedingungen für eine Arbeitslast zutreffen, kann sie nicht von Unified Manager überwacht werden:

  - Es handelt sich um eine Datenschutzkopie (DP) im schreibgeschützten 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, die mit Speichereffizienz, Datenreplikation und Systemintegrität verbunden sind, einschließlich:

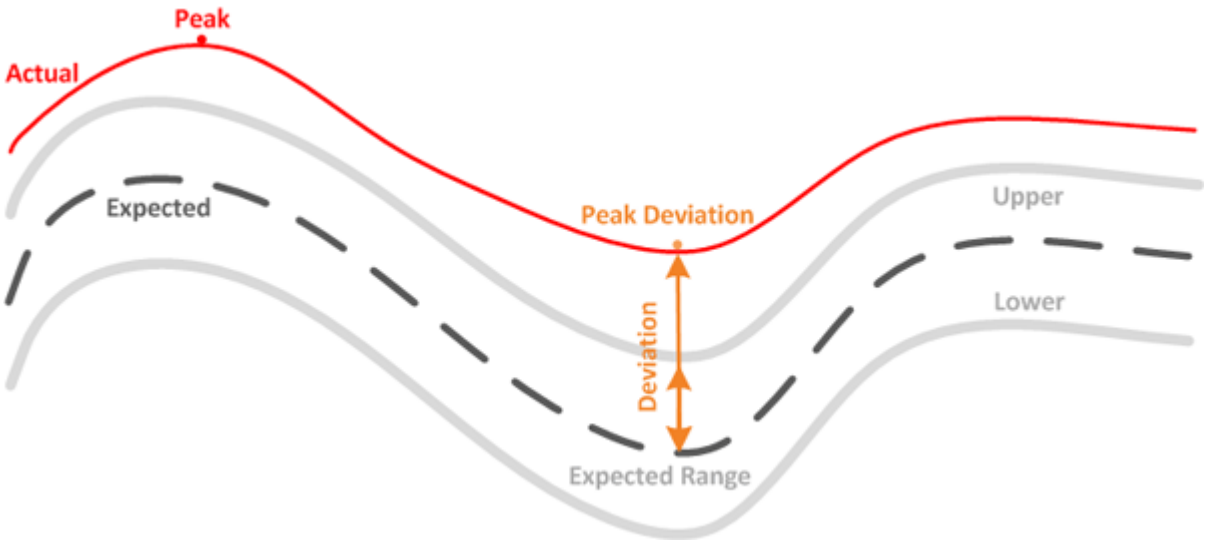
- Speichereffizienz, z. B. Deduplizierung
- Festplattenzustand, einschließlich RAID-Rekonstruktion, Festplattenbereinigung usw.
- Datenreplikation, beispielsweise SnapMirror -Kopien
- Managementaktivitäten
- Integrität des Dateisystems, einschließlich verschiedener WAFL Aktivitäten
- Dateisystem-Scanner, wie z. B. WAFL -Scan
- Copy-Offload, z. B. Auslagerung von Speichereffizienzvorgängen von VMware-Hosts
- Systemzustand, z. B. Datenträgerverschiebungen, Datenkomprimierung usw.
- Nicht überwachte Volumes

Leistungsdaten für systemdefinierte Workloads werden in der GUI nur dann angezeigt, wenn die von diesen Workloads verwendete Clusterkomponente im Konflikt steht. Sie können beispielsweise nicht nach dem Namen einer systemdefinierten Arbeitslast suchen, um deren Leistungsdaten in der GUI anzuzeigen.

Messwerte für die Workload-Leistung

Unified Manager misst die Leistung von Workloads auf einem Cluster basierend auf historischen und erwarteten statistischen Werten, die die Latenzprognose der Werte für die Workloads bilden. Es vergleicht die tatsächlichen statistischen Arbeitslastwerte mit der Latenzprognose, um festzustellen, wann die Arbeitslastleistung zu hoch oder zu niedrig ist. Eine Arbeitslast, die nicht die erwartete Leistung erbringt, löst ein dynamisches Leistungsereignis aus, um Sie zu benachrichtigen.

In der folgenden Abbildung stellt der tatsächliche Wert in Rot die tatsächliche Leistungsstatistik im Zeitrahmen dar. Der tatsächliche Wert hat die Leistungsschwelle überschritten, die die Obergrenze der Latenzprognose darstellt. Der Peak ist der höchste tatsächliche Wert im Zeitrahmen. Die Abweichung misst die Änderung zwischen den erwarteten Werten (der Prognose) und den tatsächlichen Werten, während die Spitzenabweichung die größte Änderung zwischen den erwarteten Werten und den tatsächlichen Werten angibt.



In der folgenden Tabelle sind die Messwerte für die Workload-Leistung aufgeführt.

Messung	Beschreibung
Aktivität	Der Prozentsatz des QoS-Limits, der von den Workloads in der Richtliniengruppe verwendet wird. Wenn Unified Manager eine Änderung an einer Richtliniengruppe erkennt, z. B. das Hinzufügen oder Entfernen eines Volumes oder das Ändern des QoS-Limits, können die tatsächlichen und erwarteten Werte 100 % des festgelegten Limits überschreiten. Übersteigt ein Wert 100 % des eingestellten Grenzwertes, wird dieser als >100 % angezeigt. Wenn ein Wert weniger als 1 % des eingestellten Grenzwerts beträgt, wird er als <1 % angezeigt.
Tatsächlich	Der gemessene Leistungswert zu einem bestimmten Zeitpunkt für eine bestimmte Arbeitslast.
Abweichung	Die Änderung zwischen den erwarteten Werten und den tatsächlichen Werten. Es handelt sich um das Verhältnis des tatsächlichen Werts abzüglich des erwarteten Werts zum oberen Wert des erwarteten Bereichs abzüglich des erwarteten Werts. Ein negativer Abweichungswert zeigt an, dass die Arbeitslastleistung niedriger als erwartet ist, während ein positiver Abweichungswert anzeigt, dass die Arbeitslastleistung höher als erwartet ist.
Erwartet	Die erwarteten Werte basieren auf der Analyse historischer Leistungsdaten 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 zu einem bestimmten Zeitpunkt zu erwartenden oberen und unteren Leistungswerte. Bei der Workload-Latenz bilden die oberen Werte die Leistungsschwelle. Wenn der tatsächliche Wert den Leistungsschwellenwert überschreitet, löst Unified Manager ein dynamisches Leistungsereignis aus.

Messung	Beschreibung
Gipfel	Der über einen bestimmten Zeitraum gemessene Maximalwert.
Spitzenabweichung	Der über einen bestimmten Zeitraum gemessene maximale Abweichungswert.
Warteschlangentiefe	Die Anzahl der ausstehenden E/A-Anforderungen, die an der Verbindungskomponente warten.
Verwendung	Für die Netzwerkverarbeitung, Datenverarbeitung und Aggregatkomponenten ist dies der Prozentsatz der Auslastungszeit, die zum Abschließen von Workloadvorgängen über einen bestimmten Zeitraum benötigt wird. Beispielsweise der Prozentsatz der Zeit, die die Netzwerkverarbeitungs- oder Datenverarbeitungskomponenten benötigen, um eine E/A-Anforderung zu verarbeiten, oder der Prozentsatz der Zeit, die ein Aggregat benötigt, um eine Lese- oder Schreibanforderung zu erfüllen.
Schreibdurchsatz	Die Menge des Schreibdurchsatzes in Megabyte pro Sekunde (MB/s) von Workloads auf einem lokalen Cluster zum Partnercluster in einer MetroCluster -Konfiguration.

Was ist der erwartete Leistungsbereich

Die Latenzprognose ist eine Vorhersage der zu einem bestimmten Zeitpunkt zu erwartenden oberen und unteren Leistungswerte. Bei der Workload-Latenz bilden die oberen Werte die Leistungsschwelle. Wenn der tatsächliche Wert den Leistungsschwellenwert überschreitet, löst Unified Manager ein dynamisches Leistungsereignis aus.

Während der regulären Geschäftszeiten zwischen 9:00 und 17:00 Uhr überprüfen die meisten Mitarbeiter ihre E-Mails beispielsweise zwischen 9:00 und 10:30 Uhr. Die erhöhte Nachfrage nach den E-Mail-Servern bedeutet in dieser Zeit eine erhöhte Arbeitslast im Back-End-Speicher. Mitarbeitern fällt möglicherweise eine langsame Reaktionszeit ihrer E-Mail-Clients auf.

Während der Mittagspause zwischen 12:00 und 13:00 Uhr und am Ende des Arbeitstages nach 17:00 Uhr sind die meisten Mitarbeiter wahrscheinlich nicht an ihren Computern. Die Nachfrage nach E-Mail-Servern sinkt in der Regel, wodurch auch die Nachfrage nach Back-End-Speicher sinkt. Alternativ könnten geplante Arbeitslastvorgänge wie Speichersicherungen oder Virenscans nach 17:00 Uhr beginnen und die Aktivität auf dem Back-End-Speicher erhöhen.

Über mehrere Tage hinweg bestimmt die Zunahme und Abnahme der Arbeitslastaktivität den erwarteten Aktivitätsbereich (Latenzprognose) mit oberen und unteren Grenzen für eine Arbeitslast. Wenn die tatsächliche Arbeitslastaktivität für ein Objekt außerhalb der oberen oder unteren Grenzen liegt und für einen bestimmten Zeitraum außerhalb der Grenzen bleibt, kann dies darauf hinweisen, dass das Objekt über- oder unterbeansprucht wird.

Wie die Latenzprognose erstellt wird

Unified Manager muss mindestens 3 Tage Workload-Aktivität erfassen, bevor er mit der Analyse beginnen kann und bevor die Latenzprognose für die E/A-Reaktionszeit in der GUI angezeigt werden kann. Die erforderliche Mindestdatenerfassung berücksichtigt nicht alle Änderungen, die durch die Arbeitslastaktivität entstehen. Nach der Erfassung der Aktivitäten der ersten drei Tage passt Unified Manager die Latenzprognose alle 24 Stunden um 0:00 Uhr an, um Änderungen der Arbeitslastaktivität widerzuspiegeln und einen genaueren dynamischen Leistungsschwellenwert festzulegen.

Durch die Sommerzeit (DST) wird die Systemzeit geändert, wodurch sich die Latenzprognose der Leistungsstatistiken für überwachte Workloads ändert. Unified Manager beginnt sofort mit der Korrektur der Latenzprognose, was etwa 15 Tage dauert. Während dieser Zeit können Sie Unified Manager weiterhin verwenden. Da Unified Manager jedoch die Latenzprognose zum Erkennen dynamischer Ereignisse verwendet, sind einige Ereignisse möglicherweise nicht genau. Vor der Zeitumstellung erkannte Ereignisse sind davon nicht betroffen.

Wie die Latenzprognose in der Leistungsanalyse verwendet wird

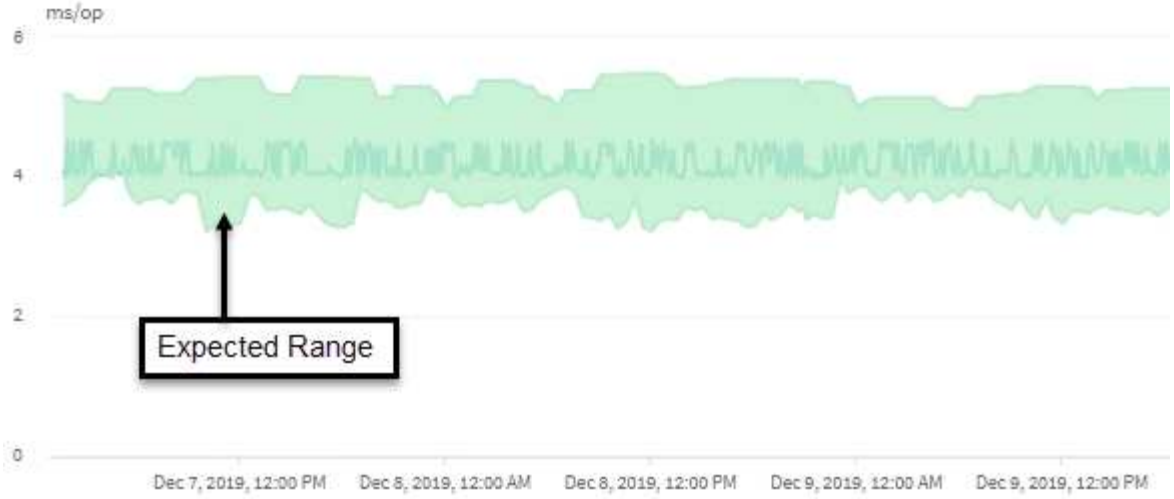
Unified Manager verwendet die Latenzprognose, um die typische E/A-Latenz (Reaktionszeit) der Aktivität für Ihre überwachten Workloads darzustellen. Sie werden benachrichtigt, wenn die tatsächliche Latenz für eine Arbeitslast über den oberen Grenzen der Latenzprognose liegt. Dadurch wird ein dynamisches Leistungsereignis ausgelöst, sodass Sie das Leistungsproblem analysieren und Korrekturmaßnahmen zu seiner Behebung ergreifen können.

Die Latenzprognose legt die Leistungsbasis für die Arbeitslast fest. Im Laufe der Zeit lernt Unified Manager aus früheren Leistungsmessungen, um die erwarteten Leistungs- und Aktivitätsniveaus für die Arbeitslast vorherzusagen. Die Obergrenze des erwarteten Bereichs legt die dynamische Leistungsschwelle fest. Unified Manager verwendet die Basislinie, um zu bestimmen, wann die tatsächliche Latenz über oder unter einem Schwellenwert oder außerhalb der Grenzen des erwarteten Bereichs liegt. Durch den Vergleich der Ist-Werte mit den Soll-Werten wird ein Leistungsprofil für die Arbeitsbelastung erstellt.

Wenn die tatsächliche Latenz für eine Arbeitslast den dynamischen Leistungsschwellenwert überschreitet, ist die Latenz aufgrund von Konflikten bei einer Clusterkomponente hoch und die Arbeitslast wird langsamer ausgeführt als erwartet. Auch die Leistung anderer Workloads, die dieselben Clusterkomponenten gemeinsam nutzen, kann langsamer sein als erwartet.

Unified Manager analysiert das Ereignis der Schwellenwertüberschreitung und ermittelt, ob es sich bei der Aktivität um ein Leistungsereignis handelt. Wenn die hohe Arbeitslastaktivität über einen längeren Zeitraum, beispielsweise mehrere Stunden, konstant bleibt, betrachtet Unified Manager die Aktivität als normal und passt die Latenzprognose dynamisch an, um den neuen dynamischen Leistungsschwellenwert zu bilden.

Bei manchen Workloads kann die Aktivität konstant niedrig sein, sodass die Latenzprognose im Zeitverlauf keine hohe Änderungsrate aufweist. Um die Anzahl der Ereignisse während der Analyse von Leistungsereignissen zu minimieren, löst Unified Manager nur für Volumes mit geringer Aktivität ein Ereignis aus, deren Vorgänge und Latenzen viel höher als erwartet sind.



In diesem Beispiel beträgt die Latenz für ein Volume in Grau höchstens 3,5 Millisekunden pro Vorgang (ms/op) und höchstens 5,5 ms/op. Wenn die tatsächliche Latenz (blau) aufgrund einer zeitweiligen Spitze im Netzwerkverkehr oder einer Konfliktsituation bei einer Clusterkomponente plötzlich auf 10 ms/Operation ansteigt, liegt sie über der Latenzprognose und hat den dynamischen Leistungsschwellenwert überschritten.

Wenn der Netzwerkverkehr abgenommen hat oder die Clusterkomponente nicht mehr im Konflikt steht, kehrt die Latenz in den Bereich der Latenzprognose zurück. Wenn die Latenz über einen längeren Zeitraum bei oder über 10 ms/Operation bleibt, müssen Sie möglicherweise Korrekturmaßnahmen ergreifen, um das Ereignis zu beheben.

So nutzt Unified Manager die Workload-Latenz, um Leistungsprobleme zu identifizieren

Die Workload-Latenz (Antwortzeit) ist die Zeit, die ein Volume in einem Cluster benötigt, um auf E/A-Anfragen von Clientanwendungen zu antworten. Unified Manager nutzt die Latenz, um Leistungsereignisse zu erkennen und Sie darauf aufmerksam zu machen.

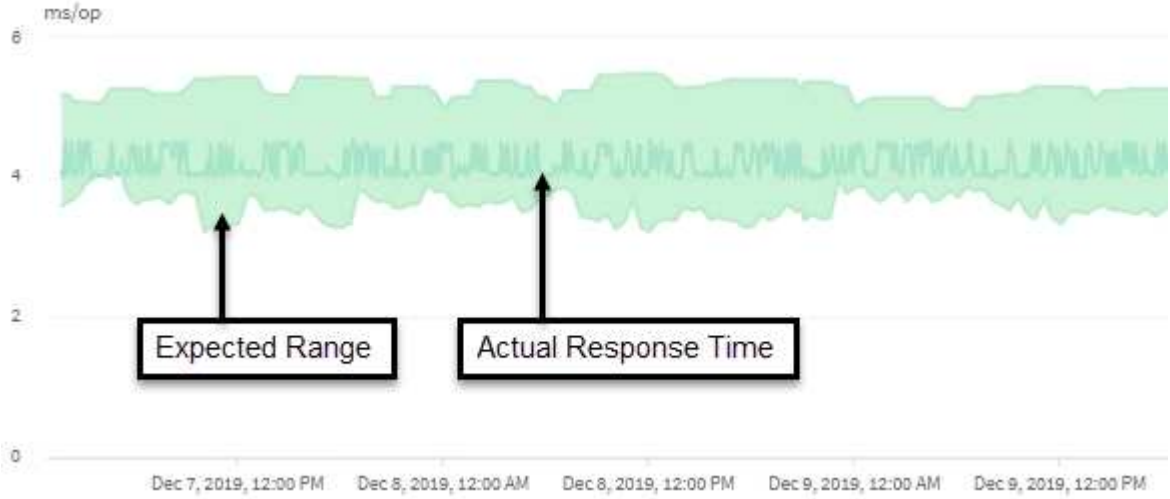
Eine hohe Latenz bedeutet, dass Anfragen von Anwendungen an ein Volume in einem Cluster länger als üblich dauern. Die Ursache für die hohe Latenz könnte im Cluster selbst liegen, da es zu Konflikten bei einer oder mehreren Clusterkomponenten kommt. Eine hohe Latenz kann auch durch Probleme außerhalb des Clusters verursacht werden, beispielsweise Netzwerkengpässe, Probleme mit dem Client, der die Anwendungen hostet, oder Probleme mit den Anwendungen selbst.

Unified Manager überwacht nur die Workload-Aktivität im Cluster. Es überwacht weder die Anwendungen, die Clients noch die Pfade zwischen den Anwendungen und dem Cluster.

Vorgänge im Cluster, wie etwa das Erstellen von Sicherungen oder Ausführen einer Deduplizierung, die den Bedarf an Clusterkomponenten erhöhen, die von anderen Workloads gemeinsam genutzt werden, können ebenfalls zu einer hohen Latenz beitragen. Wenn die tatsächliche Latenz den dynamischen Leistungsschwellenwert des erwarteten Bereichs (Latenzprognose) überschreitet, analysiert Unified Manager das Ereignis, um festzustellen, ob es sich um ein Leistungsereignis handelt, das Sie möglicherweise beheben müssen. Die Latenz wird in Millisekunden pro Vorgang (ms/op) gemessen.

Im Diagramm „Gesamtlatenz“ auf der Seite „Arbeitslastanalyse“ können Sie eine Analyse der Latenzstatistiken anzeigen, um zu sehen, wie die Aktivität einzelner Prozesse, z. B. Lese- und Schreibanforderungen, im Vergleich zur Gesamtlatenzstatistik abschneidet. Mithilfe des Vergleichs können Sie feststellen, welche Vorgänge die höchste Aktivität aufweisen oder ob bei bestimmten Vorgängen eine anormale Aktivität auftritt,

die sich auf die Latenz eines Datenträgers auswirkt. Beim Analysieren von Leistungsereignissen können Sie anhand der Latenzstatistiken feststellen, ob ein Ereignis durch ein Problem im Cluster verursacht wurde. Sie können auch die spezifischen Workload-Aktivitäten oder Clusterkomponenten identifizieren, die an dem Ereignis beteiligt sind.



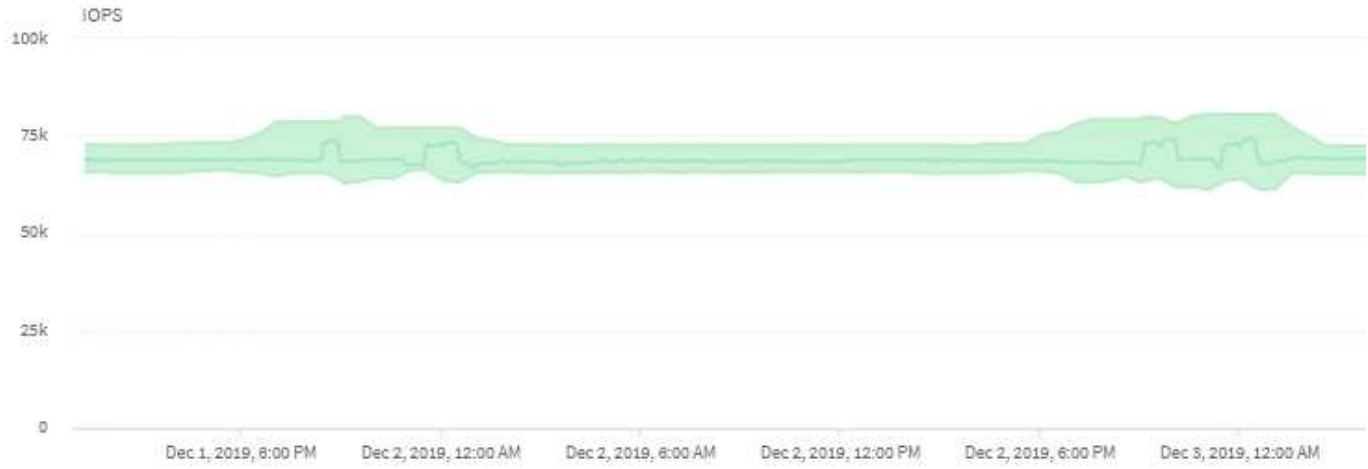
Dieses Beispiel zeigt das Latenzdiagramm. Die tatsächliche Reaktionszeit (Latenz) ist eine blaue Linie und die Latenzprognose (erwarteter Bereich) ist grün.

Wenn Unified Manager keine Daten erfassen konnte, können Lücken in der blauen Linie vorhanden sein. Dies kann auftreten, weil der Cluster oder das Volume nicht erreichbar war, Unified Manager während dieser Zeit ausgeschaltet war oder die Erfassung länger als die 5-Minuten-Erfassungsdauer dauerte.

Wie Clustervorgänge die Workload-Latenz beeinflussen können

Operationen (IOPS) stellen die Aktivität aller benutzerdefinierten und systemdefinierten Workloads auf einem Cluster dar. Mithilfe der IOPS-Statistiken können Sie feststellen, ob Clusterprozesse, wie etwa das Erstellen von Sicherungen oder das Ausführen von Deduplizierungen, die Arbeitslastlatenz (Reaktionszeit) beeinträchtigen oder ein Leistungsereignis verursacht oder dazu beigetragen haben könnten.

Beim Analysieren von Leistungsereignissen können Sie mithilfe der IOPS-Statistiken feststellen, ob ein Leistungsereignis durch ein Problem im Cluster verursacht wurde. Sie können die spezifischen Arbeitslastaktivitäten identifizieren, die möglicherweise am meisten zum Leistungsereignis beigetragen haben. IOPS werden in Operationen pro Sekunde (Ops/Sek.) gemessen.



Dieses Beispiel zeigt das IOPS-Diagramm. Die tatsächliche Betriebsstatistik ist eine blaue Linie und die IOPS-Prognose der Betriebsstatistik ist grün.

In einigen Fällen, in denen ein Cluster überlastet ist, zeigt Unified Manager möglicherweise die Meldung an `Data collection is taking too long on Cluster cluster_name`. Dies bedeutet, dass nicht genügend Statistiken für die Analyse durch Unified Manager gesammelt wurden. Sie müssen die vom Cluster verwendeten Ressourcen reduzieren, damit Statistiken erfasst werden können.

Leistungsüberwachung von MetroCluster -Konfigurationen

Mit Unified Manager können Sie den Schreibdurchsatz zwischen Clustern in einer MetroCluster -Konfiguration überwachen, um Workloads mit einem hohen Schreibdurchsatz zu identifizieren.

Wenn diese Hochleistungs-Workloads dazu führen, dass andere Volumes im lokalen Cluster hohe E/A-Reaktionszeiten aufweisen, löst Unified Manager Leistungsereignisse aus, um Sie zu benachrichtigen.

Unified Manager behandelt die Cluster in einer MetroCluster -Konfiguration als einzelne Cluster. Es wird nicht zwischen Partnerclustern unterschieden und der Schreibdurchsatz der einzelnen Cluster wird nicht korreliert.

Wenn ein lokaler Cluster in einer MetroCluster -Konfiguration seine Daten auf seinen Partnercluster spiegelt, werden die Daten in den NVRAM geschrieben und dann über die Interswitch-Links (ISLs) an die Remote-Aggregate übertragen. Unified Manager analysiert den NVRAM , um die Arbeitslasten zu identifizieren, deren hoher Schreibdurchsatz den NVRAM überlastet und so zu einem Konflikt um den NVRAM führt.

Workloads, deren Abweichung in der Antwortzeit den Leistungsschwellenwert überschritten hat, werden als *Opfer* bezeichnet, und Workloads, deren Abweichung im Schreibdurchsatz zum NVRAM höher als üblich ist und so zu Konflikten führt, werden als *Bullies* bezeichnet. Da nur die Schreibanforderungen auf den Partnercluster gespiegelt werden, analysiert Unified Manager den Lesedurchsatz nicht.

Sie können den Durchsatz aller Cluster in einer MetroCluster -Konfiguration anzeigen, indem Sie die Arbeitslasten der entsprechenden LUNs und Volumes auf den folgenden Bildschirmen analysieren. Sie können die Ergebnisse nach Cluster filtern. Aus dem linken Navigationsbereich:

- **Speicher > Cluster > Leistung: Alle Cluster** anzeigen. Siehe

- **Speicher > Volumes > Leistung: Alle Volumes** anzeigen.
- **Speicher > LUNs > Leistung: Alle LUNs** anzeigen.
- **Workload-Analyse > Alle Workloads**

Verwandte Informationen

"Analyse und Benachrichtigung von Leistungsereignissen"

"Leistungsereignisanalyse für eine MetroCluster -Konfiguration"

"Rollen der an einem Leistungsereignis beteiligten Workloads"

"Identifizierung der Arbeitslasten der Opfer, die an einem Leistungsereignis beteiligt sind"

"Identifizierung von Mobbing-Arbeitsbelastungen bei einem Leistungsereignis"

"Identifizieren der an einem Leistungsereignis beteiligten Shark-Workloads"

Leistungsereignisse und Warnungen verstehen

Leistungsereignisse sind Vorfälle im Zusammenhang mit der Arbeitslastleistung auf einem Cluster. Sie helfen Ihnen, Arbeitslasten mit langsamen Reaktionszeiten zu identifizieren. Zusammen mit den gleichzeitig aufgetretenen Integritätsereignissen können Sie die Probleme ermitteln, die möglicherweise die langsamen Reaktionszeiten verursacht oder dazu beigetragen haben.

Wenn Unified Manager mehrere Vorkommen derselben Ereignisbedingung für dieselbe Clusterkomponente erkennt, behandelt er alle Vorkommen als ein einzelnes Ereignis und nicht als separate Ereignisse.

Sie können Warnmeldungen so konfigurieren, dass automatisch E-Mail-Benachrichtigungen gesendet werden, wenn Leistungsereignisse bestimmter Schweregrade auftreten.

Quellen von Leistungsereignissen

Leistungsereignisse sind Probleme im Zusammenhang mit der Arbeitslastleistung auf einem Cluster. Sie helfen Ihnen, Speicherobjekte mit langsamen Reaktionszeiten (auch als hohe Latenz bezeichnet) zu identifizieren. Zusammen mit anderen gleichzeitig aufgetretenen Integritätsereignissen können Sie die Probleme ermitteln, die möglicherweise die langsamen Reaktionszeiten verursacht oder dazu beigetragen haben.

Unified Manager empfängt Leistungsereignisse aus den folgenden Quellen:

- **Benutzerdefinierte Leistungsschwellenwert-Richtlinienereignisse**

  Leistungsprobleme aufgrund von benutzerdefinierten Schwellenwerten, die Sie festgelegt haben. Sie konfigurieren Richtlinien für Leistungsschwellenwerte für Speicherobjekte, beispielsweise Aggregate und Volumes, sodass Ereignisse generiert werden, wenn ein Schwellenwert für einen Leistungsindikator überschritten wurde.

  Sie müssen eine Richtlinie für Leistungsschwellenwerte definieren und sie einem Speicherobjekt zuweisen, um diese Ereignisse zu empfangen.

- **Systemdefinierte Richtlinienereignisse für Leistungsschwellenwerte**

  Leistungsprobleme basierend auf systemdefinierten Schwellenwerten. Diese Schwellenwertrichtlinien sind in der Installation von Unified Manager enthalten, um häufige Leistungsprobleme abzudecken.

  Diese Schwellenwertrichtlinien sind standardmäßig aktiviert und möglicherweise werden kurz nach dem Hinzufügen eines Clusters Ereignisse angezeigt.

- **Dynamische Leistungsschwellenereignisse**

  Leistungsprobleme, die auf Ausfälle oder Fehler in einer IT-Infrastruktur oder auf eine Überbeanspruchung der Clusterressourcen durch Workloads zurückzuführen sind. Die Ursache dieser Ereignisse kann ein einfaches Problem sein, das sich im Laufe 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 Nutzung gemeinsam genutzter Clusterkomponenten langsam sind.

  Diese Schwellenwerte sind standardmäßig aktiviert und Sie sehen möglicherweise Ereignisse, nachdem drei Tage lang Daten aus einem neuen Cluster erfasst wurden.

Schweregradtypen von Leistungsereignissen

Jedem Leistungsereignis ist ein Schweregrad zugeordnet, der Ihnen dabei hilft, die Ereignisse zu priorisieren, die sofortige Korrekturmaßnahmen erfordern.

- **Kritisch**

  Es ist ein Leistungsereignis aufgetreten, das zu einer Dienstunterbrechung führen kann, wenn nicht sofort Abhilfemaßnahmen ergriffen werden.

  Kritische Ereignisse werden nur ab benutzerdefinierten Schwellenwerten gesendet.

- **Warnung**

  Ein Leistungsindikator für ein Clusterobjekt liegt außerhalb des normalen Bereichs und sollte überwacht werden, um sicherzustellen, dass er nicht den kritischen Schweregrad erreicht. Ereignisse dieses Schweregrads verursachen keine Dienstunterbrechung und es sind möglicherweise keine sofortigen Korrekturmaßnahmen erforderlich.

  Warnereignisse werden von benutzerdefinierten, systemdefinierten oder dynamischen Schwellenwerten gesendet.

- **Information**

  Das Ereignis tritt ein, wenn ein neues Objekt erkannt oder eine Benutzeraktion ausgeführt wird. Wenn beispielsweise ein Speicherobjekt gelöscht wird oder Konfigurationsänderungen vorgenommen werden, wird das Ereignis mit dem Schweregrad „Informationen“ generiert.

  Informationsereignisse werden direkt von ONTAP gesendet, wenn eine Konfigurationsänderung erkannt wird.

Weitere Informationen finden Sie unter den folgenden Links:

- "Was passiert, wenn ein Ereignis empfangen wird?"

- "Welche Informationen sind in einer Warn-E-Mail enthalten?"
- "Hinzufügen von Warnungen"
- "Hinzufügen von Warnungen für Leistungsereignisse"

Von Unified Manager erkannte Konfigurationsänderungen

Unified Manager überwacht Ihre Cluster auf Konfigurationsänderungen, damit Sie feststellen können, ob eine Änderung ein Leistungsereignis verursacht oder dazu beigetragen hat. Auf den Seiten des Performance Explorers wird ein Symbol für Änderungsereignisse angezeigt ( ), um das Datum und die Uhrzeit anzugeben, wann die Änderung erkannt wurde.

Sie können die Leistungsdiagramme auf den Seiten des Leistungs-Explorers und auf der Seite „Arbeitslastanalyse“ überprüfen, um zu sehen, ob sich das Änderungsereignis auf die Leistung des ausgewählten Clusterobjekts ausgewirkt hat. Wenn die Änderung ungefähr zur gleichen Zeit wie ein Leistungsereignis erkannt wurde, hat die Änderung möglicherweise zu dem Problem beigetragen, das zur Auslösung der Ereigniswarnung geführt hat.

Unified Manager kann die folgenden Änderungsereignisse erkennen, die als Informationsereignisse kategorisiert werden:

- Ein Volumen wird zwischen Aggregaten verschoben.

  Unified Manager kann erkennen, wann die Verschiebung läuft, abgeschlossen ist oder fehlgeschlagen ist. Wenn Unified Manager während einer Volumeverschiebung ausfällt, erkennt es die Volumeverschiebung, wenn es wieder verfügbar ist, und zeigt ein Änderungsereignis dafür an.

- Die Durchsatzgrenze (MB/s oder IOPS) einer QoS-Richtliniengruppe, die eine oder mehrere überwachte Workloads enthält, ändert sich.

  Das Ändern eines Richtliniengruppenlimits kann zu zeitweiligen Spitzen in der Latenz (Reaktionszeit) führen, die auch Ereignisse für die Richtliniengruppe auslösen können. Die Latenz normalisiert sich allmählich und alle durch die Spitzen verursachten Ereignisse werden obsolet.

- Ein Knoten in einem HA-Paar übernimmt den Speicher seines Partnerknotens oder gibt ihn zurück.

  Unified Manager kann erkennen, wann die Übernahme-, Teilübernahme- oder Rückgabeoperation abgeschlossen ist. Wenn die Übernahme durch einen in Panik geratenen Knoten verursacht wird, erkennt Unified Manager das Ereignis nicht.

- Ein ONTAP -Upgrade- oder Wiederherstellungsvorgang wurde erfolgreich abgeschlossen.

  Es werden die vorherige und die neue Version angezeigt.

Arten systemdefinierter Richtlinien für Leistungsschwellenwerte

Unified Manager bietet einige Standard-Schwellenwertrichtlinien, die die Clusterleistung überwachen und automatisch Ereignisse generieren. Diese Richtlinien sind standardmäßig aktiviert und generieren Warn- oder Informationsereignisse, wenn die überwachten Leistungsschwellenwerte überschritten werden.

Systemdefinierte Richtlinien für Leistungsschwellenwerte sind auf Cloud Volumes ONTAP, ONTAP Edge- oder ONTAP Select Systemen nicht aktiviert.

Wenn Sie unnötige Ereignisse von systemdefinierten Richtlinien für Leistungsschwellenwerte erhalten, können Sie die Ereignisse für einzelne Richtlinien auf der Seite „Ereigniseinrichtung“ deaktivieren.

Cluster-Schwellenwertrichtlinien

Die systemdefinierten Richtlinien für Cluster-Leistungsschwellenwerte werden standardmäßig jedem Cluster zugewiesen, der von Unified Manager überwacht wird:

- **Ungleichgewicht der Clusterlast**

  Identifiziert Situationen, in denen ein Knoten mit einer viel höheren Last arbeitet als andere Knoten im Cluster und daher möglicherweise die Arbeitslastlatenzen beeinflusst.

  Dies geschieht durch Vergleichen des Werts der genutzten Leistungskapazität für alle Knoten in einem Cluster, um festzustellen, ob ein Knoten den Schwellenwert von 30 % länger als 24 Stunden überschritten hat. Dies ist ein Warnereignis.

- **Ungleichgewicht der Clusterkapazität**

  Identifiziert Situationen, in denen ein Aggregat eine viel höhere genutzte Kapazität aufweist als andere Aggregate im Cluster und daher möglicherweise den für Vorgänge erforderlichen Speicherplatz beeinträchtigt.

  Dies geschieht durch Vergleichen des verwendeten Kapazitätswerts für alle Aggregate im Cluster, um festzustellen, ob zwischen den Aggregaten ein Unterschied von 70 % besteht. Dies ist ein Warnereignis.

Knotenschwellenwertrichtlinien

Die systemdefinierten Richtlinien für Knotenleistungsschwellenwerte werden standardmäßig jedem Knoten in den Clustern zugewiesen, die von Unified Manager überwacht werden:

- **Schwellenwert für genutzte Leistungskapazität überschritten**

  Identifiziert Situationen, in denen ein einzelner Knoten über die Grenzen seiner Betriebseffizienz hinaus arbeitet und daher möglicherweise die Arbeitslastlatenzen beeinträchtigt.

  Dies geschieht durch die Suche nach Knoten, die länger als 12 Stunden mehr als 100 % ihrer Leistungskapazität nutzen. Dies ist ein Warnereignis.

- **Knoten-HA-Paar überbeansprucht**

  Identifiziert Situationen, in denen Knoten in einem HA-Paar über die Grenzen der Betriebseffizienz des HA-Paares hinaus arbeiten.

  Dies geschieht durch Betrachtung des Werts der genutzten Leistungskapazität für die beiden Knoten im HA-Paar. Wenn die kombinierte Leistungskapazität der beiden Knoten länger als 12 Stunden 200 % übersteigt, wirkt sich ein Controller-Failover auf die Arbeitslastlatenzen aus. Dies ist eine Informationsveranstaltung.

- **Knoten-Festplattenfragmentierung**

Identifiziert Situationen, in denen eine oder mehrere Festplatten in einem Aggregat fragmentiert sind, wodurch wichtige Systemdienste verlangsamt werden und möglicherweise die Arbeitslastlatenzen auf einem Knoten beeinträchtigt werden.

Dies geschieht durch die Betrachtung bestimmter Lese- und Schreibvorgangsverhältnisse über alle Aggregate auf einem Knoten hinweg. Diese Richtlinie kann auch während der SyncMirror Neusynchronisierung ausgelöst werden oder wenn bei Festplattenbereinigungsvorgängen Fehler gefunden werden. Dies ist ein Warnereignis.

Die Richtlinie „Knoten-Festplattenfragmentierung“ analysiert nur HDD-Aggregate; Flash Pool-, SSD- und FabricPool -Aggregate werden nicht analysiert.

Richtlinien für aggregierte Schwellenwerte

Die systemdefinierte Richtlinie für aggregierte Leistungsschwellenwerte wird standardmäßig jedem Aggregat in den von Unified Manager überwachten Clustern zugewiesen:

- **Aggregate-Festplatten überlastet**

  Identifiziert Situationen, in denen ein Aggregat über den Grenzen seiner Betriebseffizienz arbeitet und dadurch möglicherweise die Arbeitslastlatenzen beeinträchtigt. Diese Situationen werden dadurch identifiziert, dass nach Aggregaten gesucht wird, bei denen die Festplatten im Aggregat länger als 30 Minuten zu mehr als 95 % ausgelastet sind. Diese Multicondition-Richtlinie führt dann die folgende Analyse durch, um die Ursache des Problems zu ermitteln:

  - Wird auf einer Festplatte im Aggregat derzeit im Hintergrund eine Wartungsaktivität ausgeführt?

    Zu den im Hintergrund ausgeführten Wartungsaktivitäten einer Festplatte zählen unter anderem die Festplattenrekonstruktion, die Festplattenbereinigung, die SyncMirror Neusynchronisierung und die Reparatur.

  - Gibt es einen Kommunikationsengpass bei der Fibre-Channel-Verbindung des Festplattenregals?
  - 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 Leistungsereignis wird nicht ausgelöst, wenn nur die Festplatten im Aggregat zu mehr als 95 % ausgelastet sind.

Die Richtlinie „Aggregate disks over-utilized“ analysiert reine HDD-Aggregate und Flash Pool-Aggregate (Hybrid); SSD- und FabricPool -Aggregate werden nicht analysiert.

Richtlinien für Workload-Latenzschwellenwerte

Die systemdefinierten Richtlinien für die Schwellenwerte für die Arbeitslastlatenz werden jeder Arbeitslast zugewiesen, für die eine konfigurierte Leistungsservicelevelrichtlinie mit einem definierten Wert für die „erwartete Latenz“ vorliegt:

- **Workload-Volumen/LUN-Latenzschwelle überschritten, wie durch Leistungs-Servicelevel definiert**

  Identifiziert Volumes (Dateifreigaben) und LUNs, die ihr Limit für die „erwartete Latenz“ überschritten haben und die die Workload-Leistung beeinträchtigen. Dies ist ein Warnereignis.

  Dies geschieht durch die Suche nach Arbeitslasten, die in der letzten Stunde 30 % der Zeit den erwarteten Latenzwert überschritten haben.

QoS-Schwellenwertrichtlinien

Die systemdefinierten QoS-Leistungsschwellenwertrichtlinien 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 Workload-Durchsatzwert 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 MB/s-Durchsatzlimit überschritten haben und die die Arbeitslastlatenz beeinträchtigen. Dies ist ein Warnereignis.

  Wenn einer Richtliniengruppe eine einzelne Arbeitslast zugewiesen wird, wird nach Arbeitslasten gesucht, die den in der zugewiesenen QoS-Richtliniengruppe definierten maximalen Durchsatzschwellenwert während jedes Erfassungszeitraums der vorherigen Stunde überschritten haben.

  Wenn mehrere Workloads eine einzige QoS-Richtlinie gemeinsam nutzen, geschieht dies, indem die IOPS oder MB/s aller Workloads in der Richtlinie addiert und diese Summe mit dem Schwellenwert verglichen wird.

- **QoS Peak IOPS/TB oder IOPS/TB mit Blockgrößenschwelle**

  Identifiziert Volumes, die ihr adaptives QoS-Spitzen-IOPS/TB-Durchsatzlimit (oder IOPS/TB mit Blockgrößenlimit) überschritten haben und die die Arbeitslastlatenz beeinträchtigen. Dies ist ein Warnereignis.

  Dies geschieht durch die Umwandlung des in der adaptiven QoS-Richtlinie definierten IOPS/TB-Spitzenschwellenwerts in einen QoS-Maximal-IOPS-Wert basierend auf der Größe jedes Volumes. Anschließend wird nach Volumes gesucht, die den QoS-Maximal-IOPS-Wert während jedes Leistungserfassungszeitraums der vorherigen Stunde überschritten haben.

  > Diese Richtlinie wird nur auf Volumes angewendet, wenn der Cluster mit ONTAP 9.3 oder einer späteren Software installiert ist.

  Wenn das Element „Blockgröße“ in der adaptiven QoS-Richtlinie definiert wurde, wird der Schwellenwert basierend auf der Größe jedes Volumes in einen maximalen QoS-MB/s-Wert umgewandelt. Anschließend wird nach Volumes gesucht, die während jedes Leistungserfassungszeitraums der vorherigen Stunde den QoS-Maximum-MB/s-Wert überschritten haben.

  > Diese Richtlinie wird nur auf Volumes angewendet, wenn der Cluster mit ONTAP 9.5 oder einer späteren Software installiert ist.

Analyse und Benachrichtigung von Leistungsereignissen

Leistungsereignisse benachrichtigen Sie über E/A-Leistungsprobleme bei einer Arbeitslast, die durch Konflikte bei einer Clusterkomponente verursacht werden. Unified Manager analysiert das Ereignis, um alle beteiligten Workloads und die umstrittene Komponente zu identifizieren und festzustellen, ob das Ereignis immer noch ein Problem darstellt, das Sie möglicherweise lösen müssen.

Unified Manager überwacht die E/A-Latenz (Reaktionszeit) und IOPS (Operationen) für Volumes in einem Cluster. Wenn beispielsweise andere Workloads eine Clusterkomponente übermäßig beanspruchen, ist die

Komponente überlastet und kann die optimale Leistung nicht erbringen, um die Workload-Anforderungen zu erfüllen. Die Leistung anderer Workloads, die dieselbe Komponente verwenden, kann beeinträchtigt werden, was zu einer Erhöhung ihrer Latenzen führt. Wenn die Latenz den dynamischen Leistungsschwellenwert überschreitet, löst Unified Manager ein Leistungsereignis aus, um Sie zu benachrichtigen.

Ereignisanalyse

Unified Manager führt die folgenden Analysen durch und verwendet dabei die Leistungsstatistiken der letzten 15 Tage, um die Opfer-Workloads, die Bully-Workloads und die an einem Ereignis beteiligte Clusterkomponente zu identifizieren:

- Identifiziert betroffene Workloads, deren Latenz den dynamischen Leistungsschwellenwert überschritten hat, der die Obergrenze der Latenzprognose darstellt:
  - Bei Volumes auf HDD- oder Flash Pool-Hybridaggregaten (lokale Ebene) werden Ereignisse nur ausgelöst, wenn die Latenz größer als 5 Millisekunden (ms) ist und die IOPS mehr als 10 Vorgänge pro Sekunde (Ops/Sek.) betragen.
  - Bei Volumes auf reinen SSD-Aggregaten oder FabricPool Aggregaten (Cloud-Ebene) werden Ereignisse nur ausgelöst, wenn die Latenz größer als 1 ms und die IOPS über 100 Ops/Sek. liegen.
- Identifiziert die konkurrierende Clusterkomponente.

  Wenn die Latenz der Opfer-Workloads an der Cluster-Verbindung größer als 1 ms ist, behandelt Unified Manager dies als signifikant und löst ein Ereignis für die Cluster-Verbindung aus.

- Identifiziert die Bully-Workloads, die die Clusterkomponente überbeanspruchen und zu Konflikten führen.
- Ordnet die beteiligten Arbeitslasten anhand ihrer Abweichung bei der Nutzung oder Aktivität einer Clusterkomponente ein, um zu ermitteln, bei welchen Tätern die größten Änderungen bei der Nutzung der Clusterkomponente auftreten und welche Opfer am stärksten betroffen sind.

Ein Ereignis kann nur für einen kurzen Moment auftreten und sich dann selbst korrigieren, nachdem die verwendete Komponente nicht mehr im Konflikt steht. Ein kontinuierliches Ereignis ist ein Ereignis, das für dieselbe Clusterkomponente innerhalb eines Fünf-Minuten-Intervalls erneut auftritt und im aktiven Zustand bleibt. Bei kontinuierlichen Ereignissen löst Unified Manager einen Alarm aus, nachdem das gleiche Ereignis während zwei aufeinanderfolgender Analyseintervalle erkannt wurde.

Wenn ein Ereignis behoben ist, bleibt es im Unified Manager als Teil der Aufzeichnung früherer Leistungsprobleme für ein Volume verfügbar. Jedes Ereignis verfügt über eine eindeutige ID, die den Ereignistyp und die beteiligten Volumes, Cluster und Clusterkomponenten identifiziert.

Ein einzelnes Volume kann gleichzeitig an mehreren Ereignissen beteiligt sein.

Ereignisstatus

Ereignisse können sich in einem der folgenden Zustände befinden:

- **Aktiv**

  Zeigt an, dass das Leistungsereignis derzeit aktiv ist (neu oder bestätigt). Das Problem, das das Ereignis verursacht hat, hat sich nicht von selbst behoben oder wurde nicht gelöst. Der Leistungsindikator für das Speicherobjekt bleibt über dem Leistungsschwellenwert.

- **Veraltet**

Zeigt an, dass das Ereignis nicht mehr aktiv ist. Das Problem, das das Ereignis verursacht hat, hat sich von selbst behoben oder wurde gelöst. Der Leistungsindikator für das Speicherobjekt liegt nicht mehr über dem Leistungsschwellenwert.

Ereignisbenachrichtigung

Die Ereignisse werden auf der Dashboard-Seite und auf vielen anderen Seiten der Benutzeroberfläche angezeigt und Benachrichtigungen zu diesen Ereignissen werden an angegebene E-Mail-Adressen gesendet. Auf der Seite „Ereignisdetails“ und auf der Seite „Arbeitslastanalyse“ können Sie detaillierte Analyseinformationen zu einem Ereignis anzeigen und Vorschläge zur Lösung des Ereignisses erhalten.

Ereignisinteraktion

Auf der Seite „Ereignisdetails“ und auf der Seite „Arbeitslastanalyse“ können Sie auf folgende Weise mit Ereignissen interagieren:

- Wenn Sie die Maus über ein Ereignis bewegen, wird eine Meldung mit Datum und Uhrzeit der Ereigniserkennung angezeigt.

  Wenn für denselben Zeitraum mehrere Ereignisse vorliegen, zeigt die Meldung die Anzahl der Ereignisse an.

- Wenn Sie auf ein einzelnes Ereignis klicken, wird ein Dialogfeld mit ausführlicheren Informationen zu dem Ereignis angezeigt, einschließlich der beteiligten Clusterkomponenten.

  Die umstrittene Komponente ist eingekreist und rot hervorgehoben. Sie können auf **Vollständige Analyse anzeigen** klicken, um die vollständige Analyse auf der Seite mit den Ereignisdetails anzuzeigen. Wenn für denselben Zeitraum mehrere Ereignisse vorliegen, werden im Dialogfeld Details zu den drei aktuellsten Ereignissen angezeigt. Sie können auf ein Ereignis klicken, um die Ereignisanalyse auf der Seite „Ereignisdetails“ anzuzeigen.

So ermittelt Unified Manager die Leistungsauswirkungen eines Ereignisses

Unified Manager verwendet die Abweichung bei Aktivität, Auslastung, Schreibdurchsatz, Clusterkomponentennutzung oder E/A-Latenz (Reaktionszeit) für eine Arbeitslast, um das Ausmaß der Auswirkungen auf die Arbeitslastleistung zu bestimmen. Diese Informationen bestimmen die Rolle der einzelnen Arbeitslasten im Ereignis und ihre Rangfolge auf der Seite mit den Ereignisdetails.

Unified Manager vergleicht die zuletzt analysierten Werte für eine Arbeitslast mit dem erwarteten Wertebereich (Latenzprognose). Die Differenz zwischen den zuletzt analysierten Werten und dem erwarteten Wertebereich identifiziert die Workloads, deren Leistung durch das Ereignis am stärksten beeinträchtigt wurde.

Angenommen, ein Cluster enthält zwei Workloads: Workload A und Workload B. Die Latenzprognose für Workload A beträgt 5–10 Millisekunden pro Vorgang (ms/Operation) und die tatsächliche Latenz liegt normalerweise bei etwa 7 ms/Operation. Die Latenzprognose für Workload B beträgt 10–20 ms/Operation und die tatsächliche Latenz liegt normalerweise bei etwa 15 ms/Operation. Beide Workloads liegen deutlich innerhalb ihrer Latenzprognose. Aufgrund von Konflikten im Cluster erhöht sich die Latenz beider Workloads auf 40 ms/Operation, wodurch der dynamische Leistungsschwellenwert, der die Obergrenze der Latenzprognose darstellt, überschritten wird und Ereignisse ausgelöst werden. Die Abweichung der Latenz von den erwarteten Werten zu den Werten über dem Leistungsschwellenwert beträgt für Workload A etwa 33 ms/Op, und die Abweichung für Workload B beträgt etwa 25 ms/Op. Die Latenz beider Workloads steigt auf 40

ms/op, Workload A hatte jedoch die größeren Auswirkungen auf die Leistung, da sie mit 33 ms/op die höhere Latenzabweichung aufwies.

Auf der Seite „Ereignisdetails“ im Abschnitt „Systemdiagnose“ können Sie Workloads nach ihrer Abweichung bei Aktivität, Auslastung oder Durchsatz für eine Clusterkomponente sortieren. Sie können Workloads auch nach Latenz sortieren. 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 Arbeitslast zu bestimmen. Für die Latenz stehen die roten Punkte (🔴) weisen auf das Überschreiten einer Leistungsschwelle durch eine betroffene Arbeitslast und die daraus resultierenden Auswirkungen auf die Latenz hin. Jeder rote Punkt zeigt eine höhere Abweichung bei der Latenz an, wodurch Sie die betroffenen Workloads identifizieren können, deren Latenz durch ein Ereignis am stärksten beeinträchtigt wurde.

Clusterkomponenten und warum sie kontrovers diskutiert werden können

Sie können Leistungsprobleme im Cluster erkennen, wenn eine Clusterkomponente in einen Konflikt gerät. Die Leistung von Workloads, die die Komponente verwenden, verlangsamt sich und ihre Antwortzeit (Latenz) für Clientanforderungen erhöht sich, was ein Ereignis in Unified Manager auslöst.

Eine Komponente, die im Streit liegt, kann nicht die optimale Leistung erbringen. Seine Leistung hat nachgelassen und die Leistung anderer Clusterkomponenten und Workloads, sogenannter *Opfer*, hat möglicherweise die Latenz erhöht. Um eine Komponente aus dem Wettbewerb zu nehmen, müssen Sie ihre Arbeitslast reduzieren oder ihre Fähigkeit erhöhen, mehr Arbeit zu bewältigen, damit die Leistung wieder auf ein normales Niveau zurückkehren kann. Da Unified Manager die Workload-Leistung in Fünf-Minuten-Intervallen erfasst und analysiert, erkennt er nur, wenn eine Clusterkomponente dauerhaft überbeansprucht wird. Vorübergehende Überlastungsspitzen, die innerhalb des Fünf-Minuten-Intervalls nur von kurzer Dauer sind, werden nicht erkannt.

Beispielsweise kann es zu einem Konflikt um ein Speicheraggregat kommen, weil eine oder mehrere Workloads darauf um die Erfüllung ihrer E/A-Anforderungen konkurrieren. Andere Arbeitslasten im Aggregat können beeinträchtigt werden, was zu einer Leistungsminderung führt. Um die Aktivität auf dem Aggregat zu reduzieren, können Sie verschiedene Schritte unternehmen, z. B. eine oder mehrere Arbeitslasten auf ein weniger ausgelastetes Aggregat oder einen weniger ausgelasteten Knoten verschieben, um die Gesamtarbeitslastanforderung an das aktuelle Aggregat zu verringern. Für eine QoS-Richtliniengruppe können Sie die Durchsatzgrenze anpassen oder Workloads in eine andere Richtliniengruppe verschieben, sodass die Workloads nicht mehr gedrosselt werden.

Unified Manager überwacht die folgenden Clusterkomponenten, um Sie zu warnen, wenn es zu Konflikten kommt:

- **Netzwerk**

  Stellt die Wartezeit von E/A-Anfragen durch die externen Netzwerkprotokolle im Cluster dar. Die Wartezeit ist die Zeit, die darauf gewartet wird, dass die „Transfer Ready“-Transaktionen abgeschlossen werden, bevor der Cluster auf eine E/A-Anforderung antworten kann. Wenn es zu Konflikten mit der Netzwerkkomponente kommt, bedeutet dies, dass eine hohe Wartezeit auf der Protokollebene die Latenz einer 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 durchführt, hat sich möglicherweise seit der Erkennung des Ereignisses geändert. Wenn es bei der

Netzwerkverarbeitungskomponente zu Konflikten kommt, bedeutet dies, dass eine hohe Auslastung des Netzwerkverarbeitungsknotens die Latenz einer oder mehrerer Arbeitslasten beeinträchtigt.

Wenn Sie einen All-SAN-Array-Cluster in einer Aktiv-Aktiv-Konfiguration verwenden, wird der Latenzwert der Netzwerkverarbeitung für beide Knoten angezeigt, sodass Sie überprüfen können, ob die Knoten die Last gleichmäßig teilen.

- **QoS-Limit Max**

  Stellt die maximale Durchsatzeinstellung (Spitzenwert) der der Arbeitslast zugewiesenen Speicher-QoS-Richtliniengruppe (Quality of Service) dar. Wenn die Richtliniengruppenkomponente im Konflikt steht, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch die festgelegte Durchsatzgrenze gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- **Mindest-QoS-Limit**

  Stellt die Latenz einer Arbeitslast dar, die durch die anderen Arbeitslasten zugewiesene Einstellung für den minimalen (erwarteten) QoS-Durchsatz verursacht wird. Wenn das für bestimmte Workloads festgelegte QoS-Minimum den Großteil der Bandbreite nutzt, um den versprochenen Durchsatz zu garantieren, werden andere Workloads gedrosselt und weisen eine höhere Latenz auf.

- **Cluster-Verbindung**

  Stellt die Kabel und Adapter dar, mit denen Clusterknoten physisch verbunden sind. Wenn es bei der Cluster-Interconnect-Komponente zu Konflikten kommt, bedeutet dies, dass die lange Wartezeit für E/A-Anfragen bei der Cluster-Interconnect-Komponente die Latenz einer oder mehrerer Workloads beeinträchtigt.

- * Data Processing*

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen dem Cluster und dem Speicheraggregat beteiligt ist, das die Arbeitslast enthält. Der Knoten, der die Datenverarbeitung durchführt, hat sich möglicherweise seit der Erkennung des Ereignisses geändert. Wenn es bei der Datenverarbeitungskomponente zu Konflikten kommt, bedeutet dies, dass eine hohe Auslastung des Datenverarbeitungsknotens die Latenz einer oder mehrerer Arbeitslasten beeinträchtigt.

- **Lautstärkeaktivierung**

  Stellt den Prozess dar, der die Nutzung aller aktiven Volumes verfolgt. In großen Umgebungen mit mehr als 1.000 aktiven Volumes verfolgt dieser Prozess, wie viele kritische Volumes gleichzeitig über den Knoten auf Ressourcen zugreifen müssen. Wenn die Anzahl gleichzeitig aktiver Volumes den empfohlenen Höchstschwellenwert überschreitet, kommt es bei einigen der nicht kritischen Volumes zu Latenzen, wie hier angegeben.

- * 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 die MetroCluster Komponente im Konflikt steht, bedeutet dies, dass ein hoher Schreibdurchsatz von Workloads auf dem lokalen Cluster oder ein Link-Health-Problem die Latenz einer oder mehrerer Workloads auf dem lokalen Cluster beeinträchtigt. Wenn sich der Cluster nicht in einer MetroCluster -Konfiguration befindet, wird dieses Symbol nicht angezeigt.

- **Aggregate- oder SSD-Aggregate-Operationen**

  Stellt das Speicheraggregat dar, auf dem die Workloads ausgeführt werden. Wenn es zu Konflikten bei der

Aggregatkomponente kommt, bedeutet dies, dass eine hohe Auslastung des Aggregats die Latenz einer oder mehrerer Workloads beeinträchtigt. Ein Aggregat besteht aus allen HDDs oder einer Mischung aus HDDs und SSDs (ein Flash Pool-Aggregat) oder einer Mischung aus HDDs und einer Cloud-Ebene (ein FabricPool -Aggregat). Ein „SSD-Aggregat“ besteht aus allen SSDs (einem All-Flash-Aggregat) oder einer Mischung aus SSDs und einer Cloud-Ebene (einem FabricPool -Aggregat).

- **Cloud-Latenz**

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen dem Cluster und der Cloud-Ebene beteiligt ist, auf der Benutzerdaten gespeichert sind. Wenn die Cloud-Latenzkomponente in Konflikt steht, bedeutet dies, dass eine große Anzahl von Lesevorgängen von Volumes, die auf der Cloud-Ebene gehostet werden, die Latenz einer oder mehrerer Workloads beeinträchtigt.

- * SnapMirror synchronisieren*

  Stellt die Softwarekomponente im Cluster dar, die in einer synchronen SnapMirror -Beziehung an der Replikation von Benutzerdaten vom primären Volume auf das sekundäre Volume beteiligt ist. Wenn es bei der Synchronisierungskomponente von SnapMirror zu Konflikten kommt, bedeutet dies, dass die Aktivität der synchronen SnapMirror -Vorgänge die Latenz einer oder mehrerer Arbeitslasten beeinträchtigt.

Rollen der an einem Leistungsereignis beteiligten Workloads

Unified Manager verwendet Rollen, um die Beteiligung einer Arbeitslast an einem Leistungsereignis zu identifizieren. Zu den Rollen gehören Opfer, Tyrannen und Haie. Eine benutzerdefinierte Arbeitslast kann gleichzeitig Opfer, Tyrann und Hai sein.

Rolle	Beschreibung
Opfer	Eine benutzerdefinierte Arbeitslast, deren Leistung aufgrund anderer Arbeitslasten, sogenannter „Bullies“, die eine Clusterkomponente übermäßig beanspruchen, abgenommen hat. Als Opfer werden nur benutzerdefinierte Workloads identifiziert. Unified Manager identifiziert die Arbeitslast der Opfer anhand ihrer Latenzabweichung, wobei die tatsächliche Latenz während eines Ereignisses im Vergleich zur Latenzprognose (erwarteter Bereich) stark angestiegen ist.
Schikanieren	Eine benutzerdefinierte oder systemdefinierte Arbeitslast, deren übermäßige Nutzung einer Clusterkomponente zu einer Leistungsminderung anderer Arbeitslasten, sogenannter Opfer, geführt hat. Unified Manager identifiziert problematische Workloads anhand ihrer Abweichung bei der Nutzung einer Clusterkomponente, wobei die tatsächliche Nutzung während eines Ereignisses stark über den erwarteten Nutzungsbereich hinausgeht.

Rolle	Beschreibung
Hai	Eine benutzerdefinierte Arbeitslast mit der höchsten Nutzung einer Clusterkomponente im Vergleich zu allen an einem Ereignis beteiligten Arbeitslasten. Unified Manager identifiziert Shark-Workloads basierend auf ihrer Nutzung einer Clusterkomponente während eines Ereignisses.

Workloads auf einem Cluster können viele Clusterkomponenten gemeinsam nutzen, beispielsweise Aggregate und die CPU für die Netzwerk- und Datenverarbeitung. Wenn eine Arbeitslast, beispielsweise ein Volume, die Nutzung einer Clusterkomponente so weit erhöht, dass die Komponente die Arbeitslastanforderungen nicht mehr effizient erfüllen kann, liegt ein Konflikt mit der Komponente vor. Die Arbeitslast, die eine Clusterkomponente überbeansprucht, ist ein Tyrann. Die anderen Workloads, die diese Komponenten gemeinsam nutzen und deren Leistung durch den Mobber beeinträchtigt wird, sind die Opfer. Auch Aktivitäten von systemdefinierten Workloads, wie etwa Deduplizierung oder Snapshot-Kopien, können zu „Mobbing“ eskalieren.

Wenn Unified Manager ein Ereignis erkennt, identifiziert es alle beteiligten Workloads und Clusterkomponenten, einschließlich der Bully-Workloads, die das Ereignis verursacht haben, der Clusterkomponente, um die es geht, und der Opfer-Workloads, deren Leistung aufgrund der erhöhten Aktivität der Bully-Workloads abgenommen hat.

Wenn Unified Manager die schädlichen Workloads nicht identifizieren kann, gibt er nur Warnmeldungen zu den betroffenen Workloads und der betroffenen Clusterkomponente aus.

Unified Manager kann Arbeitslasten identifizieren, die Opfer von Mobbing-Arbeitslasten sind, und auch erkennen, wann diese Arbeitslasten zu Mobbing-Arbeitslasten werden. Eine Arbeitsbelastung kann sich selbst zum Tyrannen machen. Beispielsweise führt eine Hochleistungs-Workload, die durch eine Richtliniengruppenbeschränkung gedrosselt wird, dazu, dass alle Workloads in der Richtliniengruppe gedrosselt werden, einschließlich der eigenen Workloads. Eine Arbeitsbelastung, die in einem laufenden Leistungsereignis als Tyrann oder Opfer auftritt, kann ihre Rolle ändern oder nicht länger an dem Ereignis teilnehmen.

Leistungsschwellenwerte verwalten

Mithilfe von Richtlinien für Leistungsschwellenwerte können Sie den Zeitpunkt bestimmen, an dem Unified Manager ein Ereignis generiert, um Systemadministratoren über Probleme zu informieren, die die Workload-Leistung beeinträchtigen könnten. Diese Schwellenwertrichtlinien werden als *benutzerdefinierte* Leistungsschwellenwerte bezeichnet.

Diese Version unterstützt benutzerdefinierte, systemdefinierte und dynamische Leistungsschwellenwerte. Mit dynamischen und systemdefinierten Leistungsschwellenwerten analysiert Unified Manager die Arbeitslastaktivität, um den entsprechenden Schwellenwert zu bestimmen. Mit benutzerdefinierten Schwellenwerten können Sie die oberen Leistungsgrenzen für viele Leistungsindikatoren und viele Speicherobjekte definieren.

Systemdefinierte Leistungsschwellenwerte und dynamische Leistungsschwellenwerte werden von Unified Manager festgelegt und sind nicht konfigurierbar. Wenn Sie unnötige Ereignisse von systemdefinierten Leistungsschwellenwertrichtlinien erhalten, können Sie einzelne Richtlinien auf der Seite „Ereigniseinrichtung“ deaktivieren.

Funktionsweise benutzerdefinierter Leistungsschwellenwertrichtlinien

Sie legen Richtlinien für Leistungsschwellenwerte für Speicherobjekte fest (z. B. für Aggregate und Volumes), sodass ein Ereignis an den Speicheradministrator gesendet werden kann, um ihn darüber zu informieren, dass im Cluster ein Leistungsproblem vorliegt.

Sie erstellen eine Leistungsschwellenwertrichtlinie für ein Speicherobjekt, indem Sie:

- Auswählen eines Speicherobjekts
- Auswählen eines mit diesem Objekt verknüpften Leistungsindikators
- Festlegen von Werten, die die oberen Grenzwerte des Leistungsindikators definieren, die als Warn- und kritische Situationen gelten
- Angabe einer Zeitspanne, die definiert, wie lange der Zähler die Obergrenze überschreiten muss

Sie können beispielsweise eine Richtlinie für Leistungsschwellenwerte auf einem Volume festlegen, sodass Sie eine Benachrichtigung über ein kritisches Ereignis erhalten, wenn die IOPS für dieses Volume 10 Minuten lang 750 Vorgänge pro Sekunde überschreiten. Mit derselben Schwellenwertrichtlinie kann auch festgelegt werden, dass ein Warnereignis gesendet wird, wenn die IOPS 10 Minuten lang 500 Vorgänge pro Sekunde überschreiten.

Die aktuelle Version bietet Schwellenwerte, die Ereignisse senden, wenn ein Zählerwert die Schwellenwerteinstellung überschreitet. Sie können keine Schwellenwerte festlegen, die Ereignisse senden, wenn ein Zählerwert unter eine Schwellenwerteinstellung fällt.

Hier sehen Sie ein Beispiel für ein Zählerdiagramm, das angibt, dass um 1:00 Uhr ein Warnschwellenwert (gelbes Symbol) und um 12:10, 12:30 und 1:10 Uhr ein kritischer Schwellenwert (rotes Symbol) überschritten wurde:

Eine Grenzwertüberschreitung muss für die angegebene Dauer ununterbrochen auftreten. Wird der Grenzwert aus irgendeinem Grund unterschritten, gilt eine erneute Überschreitung als Beginn einer neuen Laufzeit.

Bei einigen Clusterobjekten und Leistungsindikatoren können Sie eine kombinierte Schwellenwertrichtlinie erstellen, die erfordert, dass zwei Leistungsindikatoren ihre Höchstgrenzen überschreiten, bevor ein Ereignis generiert wird. Sie können beispielsweise eine Schwellenwertrichtlinie anhand der folgenden Kriterien erstellen:

Clusterobjekt	Leistungsindikator	Warnschwelle	Kritischer Schwellenwert	Dauer
Volumen	Latenz	10 Millisekunden	20 Millisekunden	15 Minuten
Aggregat	Verwendung	65 %	85 %	

Schwellenwertrichtlinien, die zwei Clusterobjekte verwenden, führen dazu, dass nur dann ein Ereignis generiert wird, wenn beide Bedingungen verletzt werden. Beispielsweise mithilfe der in der Tabelle definierten Schwellenwertrichtlinie:

Wenn die Lautstärkelatenz durchschnittlich ist …	Und die Gesamtdatenträgerauslastung beträgt …	Dann…
15 Millisekunden	50 %	Es wird kein Ereignis gemeldet.
15 Millisekunden	75 %	Es wird ein Warnereignis gemeldet.
25 Millisekunden	75 %	Es wird ein Warnereignis gemeldet.
25 Millisekunden	90 %	Es wird ein kritisches Ereignis gemeldet.

Was passiert, wenn eine Leistungsschwellenrichtlinie verletzt wird?

Wenn ein Zählerwert seinen definierten Leistungsschwellenwert für die in der Dauer angegebene Zeit überschreitet, wird der Schwellenwert überschritten und ein Ereignis gemeldet.

Das Ereignis führt dazu, dass folgende Aktionen eingeleitet werden:

- Das Ereignis wird im Dashboard, auf der Seite „Leistungsclusterübersicht“, auf der Seite „Ereignisse“ und auf der objektspezifischen Seite „Leistungsinventar“ angezeigt.
- (optional) Eine E-Mail-Benachrichtigung über das Ereignis kann an einen oder mehrere E-Mail-Empfänger gesendet werden, und ein SNMP-Trap kann an einen Trap-Empfänger gesendet werden.
- (optional) Ein Skript kann ausgeführt werden, um Speicherobjekte automatisch zu ändern oder zu aktualisieren.

Es wird immer die erste Aktion ausgeführt. Sie konfigurieren auf der Seite „Alarm-Setup“, ob die optionalen Aktionen ausgeführt werden. Sie können eindeutige Aktionen definieren, je nachdem, ob eine Warn- oder eine kritische Schwellenwertrichtlinie verletzt wird.

Nachdem bei einem Speicherobjekt ein Verstoß gegen die Richtlinie zum Leistungsschwellenwert aufgetreten ist, werden für diese Richtlinie keine weiteren Ereignisse generiert, bis der Zählerwert unter den Schwellenwert fällt. An diesem Punkt wird die Dauer für diesen Grenzwert zurückgesetzt. Während der Schwellenwert weiterhin überschritten wird, wird die Endzeit des Ereignisses kontinuierlich aktualisiert, um anzuzeigen, dass dieses Ereignis andauert.

Ein Schwellenwertereignis erfasst oder friert die Informationen zum Schweregrad und zur Richtliniendefinition ein, sodass eindeutige Schwellenwertinformationen mit dem Ereignis angezeigt werden, auch wenn die Schwellenwertrichtlinie in der Zukunft geändert wird.

Welche Leistungsindikatoren können mithilfe von Schwellenwerten verfolgt werden?

Für einige gängige Leistungsindikatoren, wie etwa IOPS und MB/s, können

Schwellenwerte für alle Speicherobjekte festgelegt werden. Es gibt andere Zähler, bei denen Schwellenwerte nur für bestimmte Speicherobjekte festgelegt werden können.

Verfügbare Leistungsindikatoren

Speicherobjekt	Leistungsindikator	Beschreibung
Cluster	IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabevorgänge, die der Cluster pro Sekunde verarbeitet.
MB/s	Durchschnittliche Anzahl an Megabyte an Daten, die pro Sekunde zu und von diesem Cluster übertragen werden.	Node
IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabevorgänge, die der Knoten pro Sekunde verarbeitet.	MB/s
Durchschnittliche Anzahl Megabyte an Daten, die pro Sekunde zu und von diesem Knoten übertragen werden.	Latenz	Durchschnittliche Anzahl von Millisekunden, die der Knoten benötigt, um auf Anwendungsanforderungen zu antworten.
Verwendung	Durchschnittlicher Prozentsatz der CPU- und RAM-Nutzung des Knotens.	Ausgenutzte Leistungsfähigkeit
Durchschnittlicher Prozentsatz der Leistungskapazität, die vom Knoten verbraucht wird.	Ausgelastete Leistungsfähigkeit - Übernahme	Durchschnittlicher Prozentsatz der Leistungskapazität, die vom Knoten verbraucht wird, zuzüglich der Leistungskapazität seines Partnerknotens.
Aggregat	IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabevorgänge, die das Aggregat pro Sekunde verarbeitet.
MB/s	Durchschnittliche Anzahl an Megabyte an Daten, die pro Sekunde zu und von diesem Aggregat übertragen werden.	Latenz

Speicherobjekt	Leistungsindikator	Beschreibung
Durchschnittliche Anzahl von Millisekunden, die das Aggregat benötigt, um auf Anwendungsanforderungen zu antworten.	Verwendung	Durchschnittlicher Prozentsatz der verwendeten Festplatten des Aggregats.
Ausgenutzte Leistungsfähigkeit	Durchschnittlicher Prozentsatz der Leistungskapazität, die vom Aggregat verbraucht wird.	Speicher-VM
IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabevorgänge, die der SVM pro Sekunde verarbeitet.	MB/s
Durchschnittliche Anzahl Megabyte an Daten, die pro Sekunde zu und von diesem SVM übertragen werden.	Latenz	Durchschnittliche Anzahl von Millisekunden, die die SVM benötigt, um auf Anwendungsanforderungen zu antworten.
Volumen	IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabevorgänge, die das Volume pro Sekunde verarbeitet.
MB/s	Durchschnittliche Anzahl an Megabyte an Daten, die pro Sekunde von und zu diesem Datenträger übertragen werden.	Latenz
Durchschnittliche Anzahl von Millisekunden, die das Volume benötigt, um auf Anwendungsanforderungen zu reagieren.	Cache-Fehlerquote	Durchschnittlicher Prozentsatz der Leseanforderungen von Clientanwendungen, die vom Volume und nicht vom Cache zurückgegeben werden.
LUN	IOPS	Durchschnittliche Anzahl der Eingabe-/Ausgabevorgänge, die die LUN pro Sekunde verarbeitet.
MB/s	Durchschnittliche Anzahl an Megabyte an Daten, die pro Sekunde zu und von dieser LUN übertragen werden.	Latenz

Speicherobjekt	Leistungsindikator	Beschreibung
Durchschnittliche Anzahl von Millisekunden, die die LUN benötigt, um auf Anwendungsanforderungen zu antworten.	Namensraum	IOPS
Durchschnittliche Anzahl der Eingabe-/Ausgabevorgänge, die der Namespace pro Sekunde verarbeitet.	MB/s	Durchschnittliche Anzahl an Megabyte an Daten, die pro Sekunde zu und von diesem Namespace übertragen werden.
Latenz	Durchschnittliche Anzahl von Millisekunden, die der Namespace benötigt, um auf Anwendungsanforderungen zu antworten.	Hafen
Bandbreitenauslastung	Durchschnittlicher Prozentsatz der verfügbaren Bandbreite des Ports, der verwendet wird.	MB/s
Durchschnittliche Anzahl Megabyte an Daten, die pro Sekunde von und zu diesem Port übertragen werden.	Netzwerkschnittstelle (LIF)	MB/s

Welche Objekte und Zähler können in Kombinationsschwellenwertrichtlinien verwendet werden?

Nur einige Leistungsindikatoren können zusammen in Kombinationsrichtlinien verwendet werden. Wenn primäre und sekundäre Leistungsindikatoren angegeben werden, müssen beide Leistungsindikatoren ihre Höchstgrenzen überschreiten, bevor ein Ereignis generiert wird.

Primäres Speicherobjekt und Zähler	Sekundäres Speicherobjekt und Zähler
Lautstärkelatenz	Datenträger-IOPS
Volumen MB/s	Gesamtnutzung
Verwendete Gesamtleistungskapazität	Knotenauslastung
Verwendete Knotenleistungskapazität	Verwendete Knotenleistungskapazität – Übernahme
LUN-Latenz	LUN-IOPS
LUN MB/s	Gesamtnutzung

Primäres Speicherobjekt und Zähler	Sekundäres Speicherobjekt und Zähler
Verwendete Gesamtleistungskapazität	Knotenauslastung
Verwendete Knotenleistungskapazität	Verwendete Knotenleistungskapazität – Übernahme

Wenn eine Volume-Kombinationsrichtlinie auf ein FlexGroup Volume und nicht 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, die diesen Fall beschreibt. Dies liegt daran, dass FlexGroup Volumes auf mehr als einem Knoten oder Aggregat vorhanden sein können.

Erstellen Sie benutzerdefinierte Richtlinien für Leistungsschwellenwerte

Sie erstellen Leistungsschwellenwertrichtlinien für Speicherobjekte, sodass Benachrichtigungen gesendet werden, wenn ein Leistungsindikator einen bestimmten Wert überschreitet. Die Ereignisbenachrichtigung weist darauf hin, dass im Cluster ein Leistungsproblem vorliegt.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Sie erstellen Richtlinien für Leistungsschwellenwerte, indem Sie die Schwellenwerte auf der Seite „Richtlinie für Leistungsschwellenwerte erstellen“ eingeben. Sie können neue Richtlinien erstellen, indem Sie alle Richtlinienwerte auf dieser Seite definieren, oder Sie können eine Kopie einer vorhandenen Richtlinie erstellen und die Werte in der Kopie ändern (dies wird als *Klonen* bezeichnet).

Gültige Schwellenwerte sind 0,001 bis 10.000.000 für Zahlen, 0,001–100 für Prozentsätze und 0,001–200 für Prozentsätze der genutzten Leistungskapazität.

Die aktuelle Version bietet Schwellenwerte, die Ereignisse senden, wenn ein Zählerwert die Schwellenwerteinstellung überschreitet. Sie können keine Schwellenwerte festlegen, die Ereignisse senden, wenn ein Zählerwert unter eine Schwellenwerteinstellung fällt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ereignisschwellenwerte** > **Leistung** aus.

   Die Seite „Leistungsschwellenwerte“ wird angezeigt.

2. Klicken Sie auf die entsprechende Schaltfläche, je nachdem, ob Sie eine neue Richtlinie erstellen oder eine ähnliche Richtlinie klonen und die geklonte Version ändern möchten.

Zu…	Klicken…
Erstellen einer neuen Richtlinie	**Erstellen**
Klonen einer vorhandenen Richtlinie	Wählen Sie eine vorhandene Richtlinie aus und klicken Sie auf **Klonen**

Die Seite „Richtlinie für Leistungsschwellenwerte erstellen“ oder „Richtlinie für Leistungsschwellenwerte klonen“ wird angezeigt.

3. Definieren Sie die Schwellenwertrichtlinie, indem Sie die Schwellenwerte für den Leistungsindikator angeben, die Sie für bestimmte Speicherobjekte festlegen möchten:

   a. Wählen Sie den Speicherobjekttyp aus und geben Sie einen Namen und eine Beschreibung für die Richtlinie an.

   b. Wählen Sie den zu verfolgenden Leistungsindikator aus und geben Sie die Grenzwerte an, die Warn- und kritische Ereignisse definieren.

      Sie müssen mindestens eine Warnung oder einen kritischen Grenzwert definieren. Sie müssen nicht beide Arten von Grenzwerten definieren.

   c. Wählen Sie bei Bedarf einen sekundären Leistungsindikator aus und legen Sie die Grenzwerte für Warn- und kritische Ereignisse fest.

      Die Einbeziehung eines sekundären Zählers erfordert, dass beide Zähler die Grenzwerte überschreiten, bevor der Schwellenwert überschritten und ein Ereignis gemeldet wird. Mithilfe einer Kombinationsrichtlinie können nur bestimmte Objekte und Zähler konfiguriert werden.

   d. Wählen Sie die Zeitdauer aus, für die die Grenzwerte überschritten werden müssen, damit ein Ereignis gesendet wird.

   Wenn Sie eine vorhandene Richtlinie klonen, müssen Sie einen neuen Namen für die Richtlinie eingeben.

4. Klicken Sie auf **Speichern**, um die Richtlinie zu speichern.

   Sie werden zur Seite „Leistungsschwellenwerte“ zurückgeleitet. Eine Erfolgsmeldung oben auf der Seite bestätigt, dass die Schwellenwertrichtlinie erstellt wurde, und bietet einen Link zur Inventarseite für diesen Objekttyp, sodass Sie die neue Richtlinie sofort auf Speicherobjekte anwenden können.

Wenn Sie die neue Schwellenwertrichtlinie jetzt auf Speicherobjekte anwenden möchten, können Sie auf den Link **Jetzt zu Objekttyp wechseln** klicken, um zur Inventarseite zu gelangen.

Zuweisen von Leistungsschwellenwertrichtlinien zu Speicherobjekten

Sie weisen einem Speicherobjekt eine benutzerdefinierte Leistungsschwellenwertrichtlinie zu, sodass Unified Manager ein Ereignis meldet, wenn der Wert des Leistungsindikators die Richtlinieneinstellung überschreitet.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Die Leistungsschwellenwertrichtlinie(n), die Sie auf das Objekt anwenden möchten, muss/müssen vorhanden sein.

Sie können jeweils nur eine Leistungsrichtlinie auf ein Objekt oder eine Gruppe von Objekten anwenden.

Sie können jedem Speicherobjekt maximal drei Schwellenwertrichtlinien zuweisen. Wenn beim Zuweisen von Richtlinien zu mehreren Objekten einem der Objekte bereits die maximale Anzahl an Richtlinien zugewiesen ist, führt Unified Manager die folgenden Aktionen aus:

- Wendet die Richtlinie auf alle ausgewählten Objekte an, die ihr Maximum noch nicht erreicht haben.
- Ignoriert die Objekte, die die maximale Anzahl an Richtlinien erreicht haben
- Zeigt eine Meldung an, dass die Richtlinie nicht allen Objekten zugewiesen wurde

Schritte

1. Wählen Sie auf der Seite „Leistungsinventar“ eines beliebigen Speicherobjekts das Objekt bzw. die Objekte aus, denen Sie eine Schwellenwertrichtlinie zuweisen möchten:

So weisen Sie Schwellenwerte zu:	Klicken…
Ein einzelnes Objekt	Das Kontrollkästchen links neben diesem Objekt.
Mehrere Objekte	Das Kontrollkästchen links neben jedem Objekt.
Alle Objekte auf der Seite	Der Dropdown-Feld und wählen Sie **Alle Objekte auf dieser Seite auswählen**.
Alle Objekte des gleichen Typs	Der Dropdown-Feld und wählen Sie **Alle Objekte auswählen**.

   Sie können die Sortier- und Filterfunktion verwenden, um die Liste der Objekte auf der Inventarseite zu verfeinern und so die Anwendung von Schwellenwertrichtlinien auf viele Objekte zu vereinfachen.

2. Treffen Sie Ihre Auswahl und klicken Sie dann auf **Richtlinie für Leistungsschwellenwerte zuweisen**.

   Die Seite „Richtlinie für Leistungsschwellenwerte zuweisen“ wird angezeigt und enthält eine Liste der Schwellenwertrichtlinien, die für diesen bestimmten Speicherobjekttyp vorhanden sind.

3. Klicken Sie auf die einzelnen Richtlinien, um die Details der Leistungsschwellenwerteinstellungen anzuzeigen und zu überprüfen, ob Sie die richtige Schwellenwertrichtlinie ausgewählt haben.
4. Nachdem Sie die entsprechende Schwellenwertrichtlinie ausgewählt haben, klicken Sie auf **Richtlinie zuweisen**.

   Eine Erfolgsmeldung oben auf der Seite bestätigt, dass die Schwellenwertrichtlinie dem oder den Objekten zugewiesen wurde, und bietet einen Link zur Seite „Warnmeldungen“, damit Sie die Warnmeldungseinstellungen für dieses Objekt und diese Richtlinie konfigurieren können.

Wenn Sie Warnmeldungen per E-Mail oder als SNMP-Trap erhalten möchten, um Sie darüber zu informieren, dass ein bestimmtes Leistungsereignis generiert wurde, müssen Sie die Warnmeldungseinstellungen auf der Seite „Warnmeldungseinrichtung“ konfigurieren.

Richtlinien für Leistungsschwellenwerte anzeigen

Sie können alle derzeit definierten Richtlinien für Leistungsschwellenwerte auf der Seite „Leistungsschwellenwerte“ anzeigen.

Die Liste der Schwellenwertrichtlinien ist alphabetisch nach Richtliniennamen sortiert und enthält Richtlinien für alle Arten von Speicherobjekten. Sie können auf eine Spaltenüberschrift klicken, um die Richtlinien nach dieser Spalte zu sortieren. Wenn Sie nach einer bestimmten Richtlinie suchen, verwenden Sie die Filter- und Suchmechanismen, um die Liste der Schwellenwertrichtlinien zu verfeinern, die in der Inventarliste angezeigt

werden.

Sie können den Cursor über den Richtliniennamen und den Bedingungsnamen bewegen, um die Konfigurationsdetails der Richtlinie anzuzeigen. Darüber hinaus können Sie die bereitgestellten Schaltflächen verwenden, um benutzerdefinierte Schwellenwertrichtlinien zu erstellen, zu klonen, zu bearbeiten und zu löschen.

Schritt

1. Wählen Sie im linken Navigationsbereich **Ereignisschwellenwerte** > **Leistung** aus.

   Die Seite „Leistungsschwellenwerte“ wird angezeigt.

Bearbeiten benutzerdefinierter Richtlinien für Leistungsschwellenwerte

Sie können die Schwellenwerteinstellungen für vorhandene Leistungsschwellenwertrichtlinien bearbeiten. Dies kann nützlich sein, wenn Sie feststellen, dass Sie für bestimmte Schwellenwertbedingungen zu viele oder zu wenige Warnungen erhalten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Sie können den Richtliniennamen oder den Typ des Speicherobjekts, das für vorhandene Schwellenwertrichtlinien überwacht wird, nicht ändern.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ereignisschwellenwerte** > **Leistung** aus.

   Die Seite „Leistungsschwellenwerte“ wird angezeigt.

2. Wählen Sie die Schwellenwertrichtlinie aus, die Sie ändern möchten, und klicken Sie auf **Bearbeiten**.

   Die Seite „Richtlinie für Leistungsschwellenwerte bearbeiten“ wird angezeigt.

3. Nehmen Sie Ihre Änderungen an der Schwellenwertrichtlinie vor und klicken Sie auf **Speichern**.

   Sie werden zur Seite „Leistungsschwellenwerte“ zurückgeleitet.

Nach dem Speichern werden Änderungen sofort auf allen Speicherobjekten aktualisiert, die die Richtlinie verwenden.

Abhängig von der Art der Änderungen, die Sie an der Richtlinie vorgenommen haben, möchten Sie möglicherweise die Warneinstellungen überprüfen, die für die Objekte konfiguriert sind, die die Richtlinie auf der Seite „Warnungseinrichtung“ verwenden.

Entfernen Sie Leistungsschwellenwertrichtlinien aus Speicherobjekten

Sie können eine benutzerdefinierte Leistungsschwellenwertrichtlinie aus einem Speicherobjekt entfernen, wenn Unified Manager den Wert des Leistungsindikators nicht mehr überwachen soll.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Sie können jeweils nur eine Richtlinie von einem ausgewählten Objekt entfernen.

Sie können eine Schwellenwertrichtlinie von mehreren Speicherobjekten entfernen, indem Sie mehr als ein Objekt in der Liste auswählen.

Schritte

1. Wählen Sie auf der **Inventar**-Seite eines beliebigen Speicherobjekts ein oder mehrere Objekte aus, auf die mindestens eine Leistungsschwellenwertrichtlinie angewendet wurde.

Um Schwellenwerte zu löschen von…	Machen Sie Folgendes…
Ein einzelnes Objekt	Aktivieren Sie das Kontrollkästchen links neben diesem Objekt.
Mehrere Objekte	Aktivieren Sie das Kontrollkästchen links neben jedem Objekt.
Alle Objekte auf der Seite	Klicken ☐▾ in der Spaltenüberschrift.

2. Klicken Sie auf **Richtlinie für Leistungsschwellenwerte löschen**.

   Die Seite „Schwellenwertrichtlinie löschen“ wird angezeigt und enthält eine Liste der Schwellenwertrichtlinien, die den Speicherobjekten derzeit zugewiesen sind.

3. Wählen Sie die Schwellenwertrichtlinie aus, die Sie aus den Objekten entfernen möchten, und klicken Sie auf **Richtlinie löschen**.

   Wenn Sie eine Schwellenwertrichtlinie auswählen, werden die Details der Richtlinie angezeigt, sodass Sie bestätigen können, dass Sie die richtige Richtlinie ausgewählt haben.

Was passiert, wenn eine Leistungsschwellenwertrichtlinie geändert wird?

Wenn Sie den Zählerwert oder die Dauer einer vorhandenen Leistungsschwellenwertrichtlinie anpassen, wird die Richtlinienänderung auf alle Speicherobjekte angewendet, die die Richtlinie verwenden. Die neue Einstellung wird sofort wirksam und Unified Manager beginnt, die Leistungsindikatorwerte mit den neuen Schwellenwerteinstellungen für alle neu erfassten Leistungsdaten zu vergleichen.

Wenn aktive Ereignisse für Objekte vorhanden sind, die die geänderte Schwellenwertrichtlinie verwenden, werden die Ereignisse als veraltet markiert und die Schwellenwertrichtlinie beginnt mit der Überwachung des Zählers als neu definierte Schwellenwertrichtlinie.

Wenn Sie den Zähler, auf den der Schwellenwert angewendet wurde, in der Detailansicht der Zählerdiagramme anzeigen, spiegeln die kritischen und Warnschwellenwertlinien die aktuellen Schwellenwerteinstellungen wider. Die ursprünglichen Schwellenwerteinstellungen werden auf dieser Seite nicht angezeigt, auch wenn Sie historische Daten anzeigen, als die alte Schwellenwerteinstellung wirksam war.

Da ältere Schwellenwerteinstellungen nicht in der Detailansicht der Zählerdiagramme angezeigt werden, werden möglicherweise historische Ereignisse angezeigt, die unterhalb der aktuellen Schwellenwertlinien liegen.

Was passiert mit Leistungsschwellenwertrichtlinien, wenn ein Objekt verschoben wird?

Da den Speicherobjekten Leistungsschwellenwertrichtlinien zugewiesen sind, bleiben beim Verschieben eines Objekts alle zugewiesenen Schwellenwertrichtlinien auch nach Abschluss der Verschiebung mit dem Objekt verknüpft. Wenn Sie beispielsweise ein Volume oder eine LUN in ein anderes Aggregat verschieben, sind 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), z. B. wenn einem Aggregat oder einem Knoten eine zusätzliche Bedingung zugewiesen ist, wird die sekundäre Zählerbedingung auf das neue Aggregat oder den neuen Knoten angewendet, auf das bzw. den das Volume oder die LUN verschoben wurde.

Wenn neue aktive Ereignisse für Objekte vorhanden sind, die die geänderte Schwellenwertrichtlinie verwenden, werden die Ereignisse als veraltet markiert und die Schwellenwertrichtlinie beginnt mit der Überwachung des Zählers als neu definierte Schwellenwertrichtlinie.

Ein Volume-Verschiebevorgang veranlasst ONTAP , ein Informationsänderungsereignis zu senden. In der Ereigniszeitleiste auf der Seite „Performance Explorer“ und der Seite „Workload-Analyse“ wird ein Symbol für ein Änderungsereignis angezeigt, um den Zeitpunkt anzuzeigen, zu dem der Verschiebungsvorgang abgeschlossen wurde.

Wenn Sie ein Objekt in einen anderen Cluster verschieben, wird die benutzerdefinierte Schwellenwertrichtlinie aus dem Objekt entfernt. Falls erforderlich, müssen Sie dem Objekt nach Abschluss des Verschiebevorgangs eine Schwellenwertrichtlinie zuweisen. Dynamische und systemdefinierte Schwellenwertrichtlinien werden jedoch automatisch auf ein Objekt angewendet, nachdem es in einen neuen Cluster verschoben wurde.

Schwellenwertrichtlinienfunktionalität während der HA-Übernahme und -Rückgabe

Wenn in einer Hochverfügbarkeitskonfiguration (HA) ein Übernahme- oder Rückgabevorgang stattfindet, behalten Objekte, die von einem Knoten zum anderen verschoben werden, ihre Schwellenwertrichtlinien auf dieselbe Weise bei wie bei manuellen Verschiebungsvorgängen. Da Unified Manager alle 15 Minuten nach Änderungen an der Clusterkonfiguration sucht, werden die Auswirkungen der Umstellung auf den neuen Knoten erst bei der nächsten Abfrage der Clusterkonfiguration erkannt.

Wenn innerhalb des 15-minütigen Erfassungszeitraums für Konfigurationsänderungen sowohl ein Übernahme- als auch ein Rückgabevorgang stattfinden, werden die Leistungsstatistiken möglicherweise nicht von einem Knoten zum anderen verschoben.

Schwellenwertrichtlinienfunktionalität während der Aggregatverlagerung

Wenn Sie ein Aggregat von einem Knoten zu einem anderen Knoten verschieben, indem Sie `aggregate relocation start` Befehl werden sowohl einzelne als auch kombinierte Schwellenwertrichtlinien für alle Objekte beibehalten und der Knotenteil der Schwellenwertrichtlinie wird auf den neuen Knoten angewendet.

Schwellenwertrichtlinienfunktionalität während der MetroCluster -Umschaltung

Objekte, die in einer MetroCluster -Konfiguration von einem Cluster zu einem anderen Cluster verschoben werden, behalten ihre benutzerdefinierten Schwellenwertrichtlinieneinstellungen nicht bei. Bei Bedarf können Sie Schwellenwertrichtlinien auf die Volumes und LUNs anwenden, die in den Partnercluster verschoben wurden. Nachdem ein Objekt wieder in seinen ursprünglichen Cluster verschoben wurde, wird die benutzerdefinierte Schwellenwertrichtlinie automatisch erneut angewendet.

Weitere Informationen finden Sie unter"Lautstärkeverhalten beim Umschalten und Zurückschalten" .

Analysieren von Leistungsereignissen

Sie können Leistungsereignisse analysieren, um festzustellen, wann sie erkannt wurden, ob sie aktiv (neu oder bestätigt) oder veraltet sind, welche Arbeitslasten und Clusterkomponenten beteiligt sind und welche Optionen Sie zum Beheben der Ereignisse selbst haben.

Informationen zu Leistungsereignissen anzeigen

Auf der Inventarseite der Ereignisverwaltung können Sie eine Liste aller Leistungsereignisse auf den Clustern anzeigen, die von Unified Manager überwacht werden. Durch Anzeigen dieser Informationen können Sie die kritischsten Ereignisse ermitteln und dann detaillierte Informationen abrufen, um die Ursache des Ereignisses zu ermitteln.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die Liste der Ereignisse ist nach der Erkennungszeit sortiert, wobei die aktuellsten Ereignisse zuerst aufgeführt werden. Sie können auf eine Spaltenüberschrift klicken, um die Ereignisse basierend auf dieser Spalte zu sortieren. Sie können beispielsweise 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 Suchmechanismen verwenden, um die Liste der in der Liste angezeigten Ereignisse zu verfeinern.

Auf dieser Seite werden Ereignisse aus allen Quellen angezeigt:

- Benutzerdefinierte Richtlinie für Leistungsschwellenwerte
- Systemdefinierte Richtlinie für Leistungsschwellenwerte
- Dynamische Leistungsschwelle

In der Spalte „Ereignistyp“ wird die Quelle des Ereignisses aufgeführt. Sie können ein Ereignis auswählen, um auf der Seite mit den Ereignisdetails Details zum Ereignis anzuzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.
2. Wählen Sie im Menü „Ansicht“ die Option „Aktive Leistungsereignisse“ aus.

   Auf der Seite werden alle neuen und bestätigten Leistungsereignisse angezeigt, die in den letzten 7 Tagen generiert wurden.

3. Suchen Sie ein Ereignis, das Sie analysieren möchten, und klicken Sie auf den Ereignisnamen.

   Die Detailseite für das Ereignis wird angezeigt.

   Sie können die Detailseite für ein Ereignis auch anzeigen, indem Sie auf der Performance Explorer-Seite und in einer Warn-E-Mail auf den Link zum Ereignisnamen klicken.

Analysieren Sie Ereignisse anhand benutzerdefinierter Leistungsschwellenwerte

Aus benutzerdefinierten Schwellenwerten generierte Ereignisse zeigen an, dass ein Leistungsindikator für ein bestimmtes Speicherobjekt, beispielsweise ein Aggregat oder Volume, den in der Richtlinie definierten Schwellenwert überschritten hat. Dies weist darauf hin, dass beim Clusterobjekt ein Leistungsproblem vorliegt.

Auf der Seite „Ereignisdetails“ können Sie das Leistungsereignis analysieren und gegebenenfalls Korrekturmaßnahmen ergreifen, um die Leistung wieder auf den Normalwert zu bringen.

Reagieren Sie auf benutzerdefinierte Leistungsschwellenwertereignisse

Mit Unified Manager können Sie Leistungsereignisse untersuchen, die dadurch verursacht werden, dass ein Leistungsindikator eine benutzerdefinierte Warnung oder einen kritischen Schwellenwert überschreitet. Sie können Unified Manager auch verwenden, um den Zustand der Clusterkomponente zu überprüfen und festzustellen, ob kürzlich auf der Komponente erkannte Zustandsereignisse zum Leistungsereignis beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es müssen neue oder veraltete Leistungsereignisse vorliegen.

Schritte

1. Zeigen Sie die Seite **Ereignisdetails** an, um Informationen zum Ereignis anzuzeigen.
2. Überprüfen Sie die **Beschreibung**, in der die Schwellenwertüberschreitung beschrieben wird, die das Ereignis verursacht hat.

   Beispielsweise zeigt die Meldung „Latenzwert von 456 ms/op hat basierend auf der Schwellenwerteinstellung von 400 ms/op ein WARNUNG-Ereignis ausgelöst“ an, dass für das Objekt ein Latenz-Warnereignis aufgetreten ist.

3. Bewegen Sie den Cursor über den Richtliniennamen, um Details zur Schwellenwertrichtlinie anzuzeigen, die das Ereignis ausgelöst hat.

   Hierzu gehören der Richtlinienname, der auszuwertende Leistungsindikator, der Indikatorwert, der überschritten werden muss, damit dies als kritisches Ereignis oder Warnereignis gilt, und die Dauer, um die der Indikator den Wert überschreiten muss.

4. Notieren Sie sich die **Ereignisauslösezeit**, damit Sie untersuchen können, ob möglicherweise gleichzeitig andere Ereignisse aufgetreten sind, die zu diesem Ereignis beigetragen haben könnten.
5. Führen Sie eine der folgenden Optionen aus, um das Ereignis genauer zu untersuchen und festzustellen,

ob Sie Maßnahmen zur Behebung des Leistungsproblems ergreifen müssen:

Option	Mögliche Untersuchungsmaßnahmen
Klicken Sie auf den Namen des Quellobjekts, um die Explorer-Seite für dieses Objekt anzuzeigen.	Auf dieser Seite können Sie die Objektdetails anzeigen und dieses Objekt mit anderen ähnlichen Speicherobjekten vergleichen, um festzustellen, ob bei anderen Speicherobjekten etwa zur gleichen Zeit ein Leistungsproblem auftritt. Beispielsweise um festzustellen, ob bei anderen Volumes auf demselben Aggregat ebenfalls ein Leistungsproblem vorliegt.
Klicken Sie auf den Clusternamen, um die Seite „Clusterübersicht“ anzuzeigen.	Auf dieser Seite können Sie die Details für den Cluster anzeigen, auf dem sich dieses Objekt befindet, um festzustellen, ob etwa zur gleichen Zeit andere Leistungsprobleme aufgetreten sind.

Analysieren Sie Ereignisse anhand systemdefinierter Leistungsschwellenwerte

Aus systemdefinierten Leistungsschwellenwerten generierte Ereignisse weisen darauf hin, dass ein Leistungsindikator oder eine Reihe von Leistungsindikatoren für ein bestimmtes Speicherobjekt den Schwellenwert einer systemdefinierten Richtlinie überschritten hat. Dies weist darauf hin, dass beim Speicherobjekt, beispielsweise einem Aggregat oder Knoten, ein Leistungsproblem vorliegt.

Auf der Seite „Ereignisdetails“ können Sie das Leistungsereignis analysieren und gegebenenfalls Korrekturmaßnahmen ergreifen, um die Leistung wieder auf den Normalwert zu bringen.

Systemdefinierte Schwellenwertrichtlinien sind auf Cloud Volumes ONTAP, ONTAP Edge- oder ONTAP Select Systemen nicht aktiviert.

Reagieren auf systemdefinierte Leistungsschwellenereignisse

Sie können Unified Manager verwenden, um Leistungsereignisse zu untersuchen, die dadurch verursacht werden, dass ein Leistungsindikator einen systemdefinierten Warnschwellenwert überschreitet. Sie können Unified Manager auch verwenden, um den Zustand der Clusterkomponente zu überprüfen und festzustellen, ob kürzlich auf der Komponente erkannte Ereignisse zum Leistungsereignis beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es müssen neue oder veraltete Leistungsereignisse vorliegen.

Schritte

1. Zeigen Sie die Seite **Ereignisdetails** an, um Informationen zum Ereignis anzuzeigen.
2. Überprüfen Sie die **Beschreibung**, in der die Schwellenwertüberschreitung beschrieben wird, die das Ereignis verursacht hat.

Beispielsweise zeigt die Meldung „Ein Knotenauslastungswert von 90 % hat ein WARNUNG-Ereignis basierend auf einer Schwellenwerteinstellung von 85 % ausgelöst“ an, dass für das Clusterobjekt ein Warnereignis zur Knotenauslastung aufgetreten ist.

3. Notieren Sie sich die **Ereignisauslösezeit**, damit Sie untersuchen können, ob möglicherweise gleichzeitig andere Ereignisse aufgetreten sind, die zu diesem Ereignis beigetragen haben könnten.
4. Lesen Sie unter **Systemdiagnose** die kurze Beschreibung der Art der Analyse, die die systemdefinierte Richtlinie für das Clusterobjekt durchführt.

   Bei einigen Ereignissen wird neben der Diagnose ein grünes oder rotes Symbol angezeigt, um anzugeben, ob bei dieser bestimmten Diagnose ein Problem gefunden wurde. Für andere Arten systemdefinierter Ereignisse zeigen Zählerdiagramme die Leistung für das Objekt an.

5. Klicken Sie unter **Vorgeschlagene Aktionen** auf den Link **Helfen Sie mir dabei**, um die vorgeschlagenen Aktionen anzuzeigen, die Sie ausführen können, um zu versuchen, das Leistungsproblem selbst zu beheben.

Reagieren auf Leistungsereignisse der QoS-Richtliniengruppe

Unified Manager generiert QoS-Richtlinienwarnungsereignisse, wenn der Workload-Durchsatz (IOPS, IOPS/TB oder MBps) die definierte ONTAP QoS-Richtlinieneinstellung überschritten hat und die Workload-Latenz beeinträchtigt wird. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Leistungsprobleme zu beheben, bevor viele Workloads von der Latenz betroffen sind.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Leistungsereignisse vorliegen.

Unified Manager generiert Warnereignisse für Verstöße gegen die QoS-Richtlinie, wenn der Workload-Durchsatz während jedes Leistungserfassungszeitraums der vorherigen Stunde die definierte QoS-Richtlinieneinstellung überschritten hat. Der Workload-Durchsatz kann den QoS-Schwellenwert während jedes Erfassungszeitraums nur für einen kurzen Zeitraum überschreiten, Unified Manager zeigt im Diagramm jedoch nur den „durchschnittlichen“ Durchsatz während des Erfassungszeitraums an. Aus diesem Grund erhalten Sie möglicherweise QoS-Ereignisse, obwohl der Durchsatz für eine Arbeitslast den im Diagramm angezeigten Richtlinienschwellenwert möglicherweise nicht überschritten hat.

Sie können System Manager oder die ONTAP -Befehle verwenden, um Richtliniengruppen zu verwalten, einschließlich der folgenden Aufgaben:

- Erstellen einer neuen Richtliniengruppe für die Arbeitslast
- Hinzufügen oder Entfernen von Workloads in einer Richtliniengruppe
- Verschieben einer Arbeitslast zwischen Richtliniengruppen
- Ändern des Durchsatzlimits einer Richtliniengruppe
- Verschieben einer Arbeitslast auf ein anderes Aggregat oder einen anderen Knoten

Schritte

1. Zeigen Sie die Seite **Ereignisdetails** an, um Informationen zum Ereignis anzuzeigen.
2. Überprüfen Sie die **Beschreibung**, in der die Schwellenwertüberschreitung beschrieben wird, die das Ereignis verursacht hat.

Beispielsweise weist die Meldung „IOPS-Wert von 1.352 IOPS auf vol1_NFS1 hat ein WARNUNG-Ereignis ausgelöst, um potenzielle Leistungsprobleme für die Arbeitslast zu ermitteln“ darauf hin, dass auf dem Volume vol1_NFS1 ein QoS Max IOPS-Ereignis aufgetreten ist.

3. Weitere Einzelheiten dazu, wann das Ereignis stattgefunden hat und wie lange es aktiv war, finden Sie im Abschnitt **Ereignisinformationen**.

   Darüber hinaus können Sie für Volumes oder LUNs, die den Durchsatz einer QoS-Richtlinie gemeinsam nutzen, die Namen der drei Workloads mit dem höchsten IOPS- oder MBps-Verbrauch sehen.

4. Sehen Sie sich im Abschnitt **Systemdiagnose** die beiden Diagramme an: eines für die durchschnittlichen IOPS oder MBps (je nach Ereignis) und eines für die Latenz. Bei dieser Anordnung können Sie sehen, welche Clusterkomponenten die Latenz am stärksten beeinflussen, wenn sich die Arbeitslast dem QoS-Maximum-Limit nähert.

   Bei einem gemeinsamen QoS-Richtlinienereignis werden die drei höchsten Arbeitslasten im Durchsatzdiagramm angezeigt. Wenn mehr als drei Workloads die QoS-Richtlinie gemeinsam nutzen, werden zusätzliche Workloads in einer Kategorie „Andere Workloads“ zusammengefasst. Darüber hinaus zeigt das Latenzdiagramm die durchschnittliche Latenz aller Workloads, die Teil der QoS-Richtlinie sind.

   Beachten Sie, 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 konvertiert hat.

5. Überprüfen Sie die Vorschläge im Abschnitt **Vorgeschlagene Maßnahmen** und legen Sie fest, welche Maßnahmen Sie durchführen sollten, um eine Erhöhung der Latenz für die Arbeitslast zu vermeiden.

   Klicken Sie bei Bedarf auf die Schaltfläche **Hilfe**, um weitere Details zu den vorgeschlagenen Aktionen anzuzeigen, die Sie ausführen können, um das Leistungsproblem zu beheben.

Verstehen Sie Ereignisse aus adaptiven QoS-Richtlinien mit einer definierten Blockgröße

Adaptive QoS-Richtliniengruppen skalieren automatisch eine Durchsatzober- oder -untergrenze basierend auf der Volumegröße und behalten das Verhältnis von IOPS zu TB bei, wenn sich die Volumegröße ändert. Ab ONTAP 9.5 können Sie die Blockgröße in der QoS-Richtlinie angeben, um gleichzeitig effektiv einen MB/s-Schwellenwert anzuwenden.

Durch die Zuweisung eines IOPS-Schwellenwerts in einer adaptiven QoS-Richtlinie wird nur die Anzahl der Vorgänge begrenzt, die in jeder Arbeitslast auftreten. Abhängig von der Blockgröße, die auf dem Client festgelegt ist, der die Arbeitslasten generiert, umfassen einige IOPS viel mehr Daten und stellen daher eine viel größere Belastung für die Knoten dar, die die Vorgänge verarbeiten.

Der MB/s-Wert für eine Arbeitslast wird mithilfe der folgenden Formel generiert:

```
MB/s = (IOPS * Block Size) / 1000
```

Wenn eine Arbeitslast durchschnittlich 3.000 IOPS beträgt und die Blockgröße auf dem Client auf 32 KB eingestellt ist, beträgt der effektive Wert für diese Arbeitslast 96 MB/s. Wenn diese gleiche Arbeitslast durchschnittlich 3.000 IOPS beträgt und die Blockgröße auf dem Client auf 48 KB eingestellt ist, beträgt der effektive MB/s-Wert für diese Arbeitslast 144. Sie können sehen, dass der Knoten 50 % mehr Daten verarbeitet, wenn die Blockgröße größer ist.

Sehen wir uns die folgende adaptive QoS-Richtlinie mit einer definierten Blockgröße an und wie Ereignisse basierend auf der auf dem Client festgelegten Blockgröße ausgelöst werden.

Erstellen Sie eine Richtlinie und legen Sie den Spitzendurchsatz auf 2.500 IOPS/TB mit einer Blockgröße von 32 KB fest. Dadurch wird der MB/s-Schwellenwert für ein Volume mit 1 TB genutzter Kapazität effektiv auf 80 MB/s ((2500 IOPS * 32 KB) / 1000) festgelegt. Beachten Sie, dass Unified Manager ein Warnereignis generiert, wenn der Durchsatzwert 10 % unter dem definierten Schwellenwert liegt. Ereignisse werden in den folgenden Situationen generiert:

Verwendete Kapazität	**Das Ereignis wird generiert, wenn der Durchsatz diese Anzahl von … 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 nutzt, die IOPS 4.000 betragen und die QoS-Blockgröße auf dem Client auf 32 KB eingestellt ist, beträgt der MB/ps-Durchsatz 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 verwendet.

Wenn das Volume 2 TB des verfügbaren Speicherplatzes nutzt, die IOPS 4.000 betragen und die QoS-Blockgröße auf dem Client auf 64 KB eingestellt ist, beträgt der MB/s-Durchsatz 256 MB/s ((4.000 IOPS * 64 KB) / 1.000). In diesem Fall erzeugen die 4.000 IOPS kein Ereignis, aber der MB/s-Wert von 256 MB/s liegt über dem Schwellenwert von 144 MB/s und es wird ein Ereignis erzeugt.

Aus diesem Grund wird im Abschnitt „Systemdiagnose“ der Seite „Ereignisdetails“ ein MB/s-Diagramm angezeigt, wenn ein Ereignis aufgrund einer MB/s-Verletzung für eine adaptive QoS-Richtlinie ausgelöst wird, die die Blockgröße enthält. Wenn das Ereignis aufgrund einer IOPS-Verletzung für die adaptive QoS-Richtlinie ausgelöst wird, wird im Abschnitt „Systemdiagnose“ ein IOPS-Diagramm angezeigt. Wenn sowohl bei IOPS als auch bei MB/s ein Verstoß auftritt, erhalten Sie zwei Ereignisse.

Weitere Informationen zum Anpassen der QoS-Einstellungen finden Sie unter "Übersicht zum Leistungsmanagement" .

Reagieren Sie auf Leistungsereignisse bei überlasteten Knotenressourcen

Unified Manager generiert Warnereignisse zur Überauslastung von Knotenressourcen, wenn ein einzelner Knoten über die Grenzen seiner Betriebseffizienz hinaus betrieben wird und sich daher möglicherweise auf die Arbeitslastlatenzen auswirkt. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Leistungsprobleme zu beheben, bevor viele Workloads von der Latenz betroffen sind.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es müssen neue oder veraltete Leistungsereignisse vorliegen.

Unified Manager generiert Warnereignisse für Richtlinienverstöße bei überlasteten Knotenressourcen, indem

er nach Knoten sucht, die länger als 30 Minuten mehr als 100 % ihrer Leistungskapazität nutzen.

Sie können System Manager oder die ONTAP -Befehle verwenden, um diese Art von Leistungsproblemen zu beheben, einschließlich der folgenden Aufgaben:

- Erstellen und Anwenden einer QoS-Richtlinie auf alle Volumes oder LUNs, die Systemressourcen übermäßig nutzen
- Reduzieren des maximalen QoS-Durchsatzlimits einer Richtliniengruppe, auf die Workloads angewendet wurden
- Verschieben einer Arbeitslast auf ein anderes Aggregat oder einen anderen Knoten
- Erhöhen Sie die Kapazität durch Hinzufügen von Festplatten zum Knoten oder durch ein Upgrade auf einen Knoten mit einer schnelleren CPU und mehr RAM

Schritte

1. Zeigen Sie die Seite **Ereignisdetails** an, um Informationen zum Ereignis anzuzeigen.
2. Überprüfen Sie die **Beschreibung**, in der die Schwellenwertüberschreitung beschrieben wird, die das Ereignis verursacht hat.

   Beispielsweise wird die Meldung „`Perf. Der Wert „Kapazitätsnutzung“ von 139 % auf simplicity-02 hat ein WARNUNG-Ereignis ausgelöst, um potenzielle Leistungsprobleme in der Datenverarbeitungseinheit zu identifizieren. „“ zeigt an, dass die Leistungskapazität auf Knoten simplicity-02 überbeansprucht ist und die Knotenleistung beeinträchtigt.

3. Überprüfen Sie im Abschnitt **Systemdiagnose** die drei Diagramme: eines für die auf dem Knoten verwendete Leistungskapazität, eines für die durchschnittlichen Speicher-IOPS, die von den wichtigsten Workloads verwendet werden, und eines für die Latenz bei den wichtigsten Workloads. Bei dieser Anordnung können Sie erkennen, welche Workloads die Ursache für die Latenz auf dem Knoten sind.

   Sie können anzeigen, auf welche Workloads QoS-Richtlinien angewendet werden und auf welche nicht, indem Sie den Cursor über das IOPS-Diagramm bewegen.

4. Überprüfen Sie die Vorschläge im Abschnitt **Vorgeschlagene Maßnahmen** und legen Sie fest, welche Maßnahmen Sie durchführen sollten, um eine Erhöhung der Latenz für die Arbeitslast zu vermeiden.

   Klicken Sie bei Bedarf auf die Schaltfläche **Hilfe**, um weitere Details zu den vorgeschlagenen Aktionen anzuzeigen, die Sie ausführen können, um das Leistungsproblem zu beheben.

Reagieren auf Leistungsereignisse aufgrund von Clusterungleichgewichten

Unified Manager generiert Warnereignisse zu Cluster-Ungleichgewichten, wenn ein Knoten in einem Cluster mit einer viel höheren Last als andere Knoten arbeitet und daher möglicherweise die Arbeitslastlatenzen beeinträchtigt. Diese systemdefinierten Ereignisse bieten die Möglichkeit, potenzielle Leistungsprobleme zu beheben, bevor viele Workloads von der Latenz betroffen sind.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Unified Manager generiert Warnereignisse bei Verstößen gegen die Schwellenwertrichtlinie für Clusterungleichgewichte, indem er den Wert der genutzten Leistungskapazität für alle Knoten im Cluster vergleicht, um festzustellen, ob zwischen den Knoten ein Lastunterschied von 30 % besteht.

Mithilfe dieser Schritte können Sie die folgenden Ressourcen identifizieren, sodass Sie leistungsstarke Workloads auf einen Knoten mit geringerer Auslastung verschieben können:

- Die Knoten im selben Cluster, die weniger genutzt werden
- Die Aggregate auf dem neuen Knoten, die am wenigsten genutzt werden
- Die leistungsstärksten Volumes auf dem aktuellen Knoten

Schritte

1. Zeigen Sie die Detailseite **Ereignis** an, um Informationen zum Ereignis anzuzeigen.
2. Überprüfen Sie die **Beschreibung**, in der die Schwellenwertüberschreitung beschrieben wird, die das Ereignis verursacht hat.

   Beispielsweise weist die Meldung „Der Zähler für die genutzte Leistungskapazität weist auf einen Lastunterschied von 62 % zwischen den Knoten im Cluster Dallas-1-8 hin und hat basierend auf dem Systemschwellenwert von 30 % ein WARNUNG-Ereignis ausgelöst“ darauf hin, dass die Leistungskapazität auf einem der Knoten überbeansprucht ist und die Knotenleistung beeinträchtigt.

3. Lesen Sie den Text in den **Vorgeschlagenen Aktionen**, um ein Volume mit hoher Leistung vom Knoten mit dem höchsten Wert für die genutzte Leistungskapazität auf einen Knoten mit dem niedrigsten Wert für die genutzte Leistungskapazität zu verschieben.
4. Identifizieren Sie die Knoten mit dem höchsten und niedrigsten Wert für die genutzte Leistungskapazität:
   a. Klicken Sie im Abschnitt **Ereignisinformationen** auf den Namen des Quellclusters.
   b. Klicken Sie auf der Seite **Cluster-/Leistungsübersicht** im Bereich **Verwaltete Objekte** auf **Knoten**.
   c. Sortieren Sie auf der Inventarseite **Knoten** die Knoten nach der Spalte **Verwendete Leistungskapazität**.
   d. Identifizieren Sie die Knoten mit dem höchsten und niedrigsten Wert für die genutzte Leistungskapazität und notieren Sie sich die Namen.
5. Identifizieren Sie das Volume mit den meisten IOPS auf dem Knoten mit dem höchsten Wert für die genutzte Leistungskapazität:
   a. Klicken Sie auf den Knoten mit dem höchsten Wert für die genutzte Leistungskapazität.
   b. Wählen Sie auf der Seite **Knoten-/Leistungs-Explorer** im Menü **Anzeigen und Vergleichen** die Option **Aggregate auf diesem Knoten** aus.
   c. Klicken Sie auf das Aggregat mit dem höchsten Wert für die genutzte Leistungskapazität.
   d. Wählen Sie auf der Seite **Aggregate/Performance Explorer** im Menü **Anzeigen und Vergleichen** die Option **Volumes auf diesem Aggregat** aus.
   e. Sortieren Sie die Volumes nach der Spalte **IOPS** und notieren Sie den Namen des Volumes mit den meisten IOPS sowie den Namen des Aggregats, in dem sich das Volume befindet.
6. Identifizieren Sie das Aggregat mit der niedrigsten Auslastung auf dem Knoten, der den niedrigsten Wert für die genutzte Leistungskapazität aufweist:
   a. Klicken Sie auf **Speicher** > **Aggregate**, um die Inventarseite **Aggregate** anzuzeigen.
   b. Wählen Sie die Ansicht **Leistung: Alle Aggregate**.
   c. Klicken Sie auf die Schaltfläche **Filter** und fügen Sie einen Filter hinzu, bei dem „Knoten“ dem Namen des Knotens mit dem niedrigsten Wert für die genutzte Leistungskapazität entspricht, den Sie in Schritt 4 notiert haben.
   d. Notieren Sie den Namen des Aggregats mit dem niedrigsten Wert für die genutzte Leistungskapazität.

7. Verschieben Sie das Volume vom überlasteten Knoten auf das Aggregat, das Sie als gering ausgelastet auf dem neuen Knoten identifiziert haben.

   Sie können den Verschiebevorgang mithilfe von ONTAP System Manager, OnCommand Workflow Automation, ONTAP -Befehlen oder einer Kombination dieser Tools durchführen.

Überprüfen Sie nach einigen Tagen, ob Sie von diesem Cluster dasselbe Cluster-Ungleichgewichtsereignis erhalten.

Analysieren Sie Ereignisse anhand dynamischer Leistungsschwellenwerte

Aus dynamischen Schwellenwerten generierte Ereignisse weisen darauf hin, dass die tatsächliche Antwortzeit (Latenz) für eine Arbeitslast im Vergleich zum erwarteten Antwortzeitbereich zu hoch oder zu niedrig ist. Auf der Seite „Ereignisdetails“ können Sie das Leistungsereignis analysieren und gegebenenfalls Korrekturmaßnahmen ergreifen, um die Leistung wieder auf den Normalwert zu bringen.

Dynamische Leistungsschwellenwerte sind auf Cloud Volumes ONTAP, ONTAP Edge- oder ONTAP Select Systemen nicht aktiviert.

Identifizieren Sie die Arbeitslasten der Opfer, die an einem dynamischen Leistungsereignis beteiligt sind

In Unified Manager können Sie ermitteln, welche Volume-Workloads die höchste Abweichung in der Antwortzeit (Latenz) aufweisen, die durch eine konkurrierende Speicherkomponente verursacht wird. Durch die Identifizierung dieser Workloads können Sie besser verstehen, warum die Clientanwendungen, die auf sie zugreifen, langsamer als gewöhnlich arbeiten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es müssen neue, bestätigte oder veraltete dynamische Leistungsereignisse vorliegen.

Auf der Seite „Ereignisdetails“ wird eine Liste der benutzerdefinierten und systemdefinierten Workloads angezeigt, sortiert nach der größten Abweichung bei der Aktivität oder Nutzung der Komponente oder der am stärksten vom Ereignis betroffenen Komponente. Die Werte basieren auf den Spitzen, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Zeigen Sie die Seite **Ereignisdetails** an, um Informationen zum Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen „Workload-Latenz“ und „Workload-Aktivität“ die Option „Opfer-Workloads“ aus.
3. Bewegen Sie den Cursor über die Diagramme, um die wichtigsten benutzerdefinierten Workloads anzuzeigen, die sich auf die Komponente auswirken, sowie den Namen des betroffenen Workloads.

Identifizieren Sie die Arbeitsbelastung, die bei einem dynamischen Leistungsereignis auftritt.

In Unified Manager können Sie ermitteln, welche Workloads die höchste Abweichung bei der Nutzung einer konkurrierenden Clusterkomponente aufweisen. Durch die

Identifizierung dieser Workloads können Sie besser verstehen, warum bestimmte Volumes im Cluster langsame Reaktionszeiten (Latenz) aufweisen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es müssen neue, bestätigte oder veraltete dynamische Leistungsereignisse vorliegen.

Auf der Seite „Ereignisdetails“ wird eine Liste der benutzerdefinierten und systemdefinierten Arbeitslasten angezeigt, sortiert nach der höchsten Nutzung der Komponente oder der stärksten Auswirkung des Ereignisses. Die Werte basieren auf den Spitzen, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Zeigen Sie die Seite mit den Ereignisdetails an, um Informationen zum Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen „Workload-Latenz“ und „Workload-Aktivität“ **Bully Workloads** aus.
3. Bewegen Sie den Cursor über die Diagramme, um die wichtigsten benutzerdefinierten Bully-Arbeitslasten anzuzeigen, die sich auf die Komponente auswirken.

Identifizieren Sie die an einem dynamischen Leistungsereignis beteiligten Shark-Workloads

In Unified Manager können Sie ermitteln, welche Workloads die größte Abweichung bei der Nutzung einer umstrittenen Speicherkomponente aufweisen. Durch die Identifizierung dieser Workloads können Sie feststellen, ob diese Workloads in einen weniger ausgelasteten Cluster verschoben werden sollten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es gibt neue, anerkannte oder veraltete leistungsdynamische Ereignisse.

Auf der Seite „Ereignisdetails“ wird eine Liste der benutzerdefinierten und systemdefinierten Arbeitslasten angezeigt, sortiert nach der höchsten Nutzung der Komponente oder der stärksten Auswirkung des Ereignisses. Die Werte basieren auf den Spitzen, die Unified Manager bei der Erkennung und letzten Analyse des Ereignisses ermittelt hat.

Schritte

1. Zeigen Sie die Seite **Ereignisdetails** an, um Informationen zum Ereignis anzuzeigen.
2. Wählen Sie in den Diagrammen „Workload-Latenz“ und „Workload-Aktivität“ **Shark Workloads** aus.
3. Bewegen Sie den Cursor über die Diagramme, um die wichtigsten benutzerdefinierten Workloads anzuzeigen, die sich auf die Komponente auswirken, sowie den Namen des Shark-Workloads.

Leistungsereignisanalyse für eine MetroCluster -Konfiguration

Sie können Unified Manager verwenden, um ein Leistungsereignis für eine MetroCluster -Konfiguration zu analysieren. Sie können die mit dem Ereignis verbundenen Arbeitslasten ermitteln und die vorgeschlagenen Maßnahmen zur Lösung des Problems prüfen.

Leistungsereignisse bei MetroCluster können auf übermäßige Arbeitslasten zurückzuführen sein, die die Interswitch-Links (ISLs) zwischen den Clustern überbeanspruchen, oder auf Probleme mit der

Verbindungsintegrität. Unified Manager überwacht jeden Cluster in einer MetroCluster -Konfiguration unabhängig, ohne Leistungsereignisse auf einem Partnercluster zu berücksichtigen.

Leistungsereignisse aus beiden Clustern in der MetroCluster -Konfiguration werden auch auf der Dashboard-Seite des Unified Managers angezeigt. Sie können auch die Integritätsseiten von Unified Manager anzeigen, um die Integrität jedes Clusters zu überprüfen und ihre Beziehung anzuzeigen.

Analysieren Sie ein dynamisches Leistungsereignis auf einem Cluster in einer MetroCluster -Konfiguration

Sie können Unified Manager verwenden, um den Cluster in einer MetroCluster -Konfiguration zu analysieren, in der ein Leistungsereignis erkannt wurde. Sie können den Clusternamen, die Ereigniserkennungszeit und die beteiligten *Bully*- und *Opfer* -Workloads identifizieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Für eine MetroCluster Konfiguration müssen neue, bestätigte oder veraltete Leistungsereignisse vorliegen.
- Beide Cluster in der MetroCluster -Konfiguration müssen von derselben Instanz von Unified Manager überwacht werden.

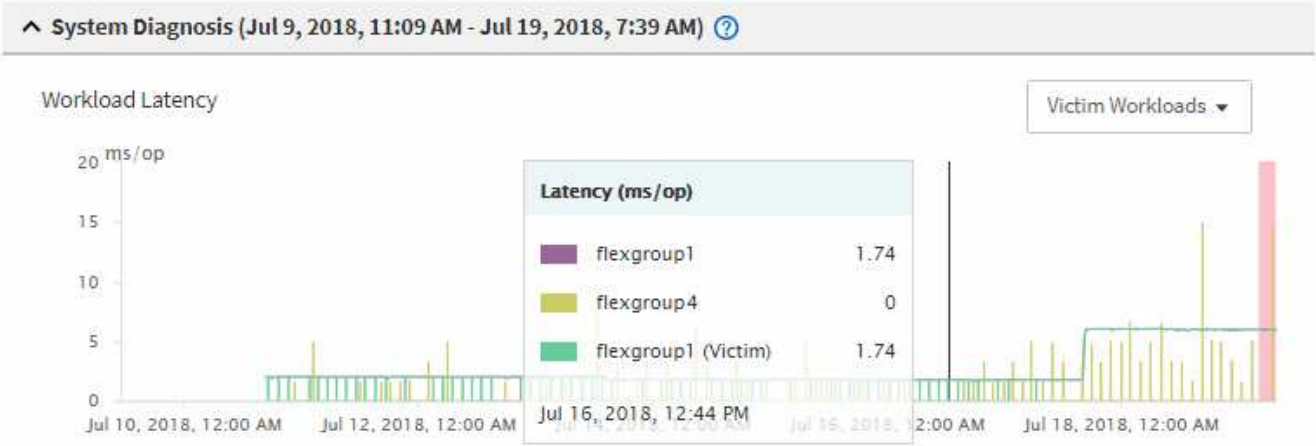
Schritte

1. Zeigen Sie die Seite **Ereignisdetails** an, um Informationen zum Ereignis anzuzeigen.
2. Überprüfen Sie die Ereignisbeschreibung, um die Namen und die Anzahl der beteiligten Workloads anzuzeigen.

   In diesem Beispiel ist das Symbol „MetroCluster -Ressourcen“ rot, was darauf hinweist, dass es um die MetroCluster -Ressourcen geht. Sie positionieren Ihren Cursor über dem Symbol, um eine Beschreibung des Symbols anzuzeigen.

3. Notieren Sie sich den Clusternamen und die Ereigniserkennungszeit, die Sie zur Analyse von Leistungsereignissen auf dem Partnercluster verwenden können.
4. Überprüfen Sie in den Diagrammen die Arbeitslasten der Opfer, um sicherzustellen, dass ihre Reaktionszeiten über dem Leistungsschwellenwert liegen.

   In diesem Beispiel wird die Arbeitsbelastung des Opfers im Hover-Text angezeigt. Die Latenzdiagramme zeigen auf hoher Ebene ein konsistentes Latenzmuster für die beteiligten Arbeitslasten der Opfer. Auch wenn die anormale Latenz der betroffenen Workloads das Ereignis ausgelöst hat, kann ein konsistentes Latenzmuster darauf hinweisen, dass die Workloads innerhalb des erwarteten Bereichs arbeiten, aber dass eine Spitze bei den E/A-Vorgängen die Latenz erhöht und das Ereignis ausgelöst hat.



Wenn Sie vor Kurzem eine Anwendung auf einem Client installiert haben, der auf diese Volumen-Workloads zugreift, und diese Anwendung eine große Menge an E/A an sie sendet, können Sie mit einer Erhöhung der Latenzen 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 bleibt, können Sie das Ereignis wahrscheinlich ignorieren. Wenn das Ereignis andauert und im neuen Zustand verbleibt, können Sie es weiter untersuchen, um festzustellen, ob andere Probleme die Ursache des Ereignisses waren.

5. Wählen Sie im Diagramm „Workload-Durchsatz“ **Bully-Workloads** aus, um die Bully-Workloads anzuzeigen.

   Das Vorhandensein von Bully-Workloads weist darauf hin, dass das Ereignis möglicherweise durch eine oder mehrere Workloads auf dem lokalen Cluster verursacht wurde, die die MetroCluster Ressourcen überbeansprucht haben. Die Bully-Workloads weisen eine hohe Abweichung beim Schreibdurchsatz (MB/s) auf.

   Dieses Diagramm zeigt auf hoher Ebene das Schreibdurchsatzmuster (MB/s) für die Workloads. Sie können das MB/s-Schreibmuster überprüfen, um einen abnormalen Durchsatz zu ermitteln, der darauf hinweisen könnte, dass eine Arbeitslast die MetroCluster -Ressourcen übermäßig nutzt.

   Wenn keine Bully-Workloads an dem Ereignis beteiligt sind, wurde das Ereignis möglicherweise durch ein Integritätsproblem mit der Verbindung zwischen den Clustern oder ein Leistungsproblem auf dem Partnercluster verursacht. Sie können Unified Manager verwenden, um den Zustand beider Cluster in einer MetroCluster -Konfiguration zu überprüfen. Sie können Unified Manager auch verwenden, um Leistungsereignisse im Partnercluster zu prüfen und zu analysieren.

Analysieren Sie ein dynamisches Leistungsereignis für einen Remote-Cluster in einer MetroCluster -Konfiguration

Sie können Unified Manager verwenden, um dynamische Leistungsereignisse auf einem Remote-Cluster in einer MetroCluster -Konfiguration zu analysieren. Mithilfe der Analyse können Sie feststellen, ob ein Ereignis auf dem Remote-Cluster ein Ereignis auf seinem Partner-Cluster verursacht hat.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen ein Leistungsereignis auf einem lokalen Cluster in einer MetroCluster -Konfiguration analysiert und die Ereigniserkennungszeit ermittelt haben.
- Sie müssen den Zustand des lokalen Clusters und seines Partnerclusters, der am Leistungsereignis

beteiligt war, überprüft und den Namen des Partnerclusters abgerufen haben.

Schritte

1. Melden Sie sich bei der Unified Manager-Instanz an, die den Partnercluster überwacht.
2. Klicken Sie im linken Navigationsbereich auf **Ereignisse**, um die Ereignisliste anzuzeigen.
3. Wählen Sie im Auswahlfeld **Zeitbereich** die Option **Letzte Stunde** aus und klicken Sie dann auf **Bereich anwenden**.
4. Wählen Sie im Auswahlfeld **Filtern** im linken Dropdown-Menü **Cluster** aus, geben Sie den Namen des Partnerclusters in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.

   Wenn für den ausgewählten Cluster in der letzten Stunde keine Ereignisse aufgetreten sind, bedeutet dies, dass für den Cluster während der Zeit, in der das Ereignis auf seinem Partner erkannt wurde, keine Leistungsprobleme aufgetreten sind.

5. Wenn im ausgewählten Cluster in der letzten Stunde Ereignisse erkannt wurden, vergleichen Sie die Ereigniserkennungszeit mit der Ereigniserkennungszeit für das Ereignis im lokalen Cluster.

   Wenn es sich bei diesen Ereignissen um Bully-Workloads handelt, die zu Konflikten bei der Datenverarbeitungskomponente führen, kann es sein, dass einer oder mehrere dieser Bullys das Ereignis im lokalen Cluster verursacht haben. Sie können auf das Ereignis klicken, um es zu analysieren und die vorgeschlagenen Maßnahmen zur Lösung des Problems auf der Seite „Ereignisdetails“ zu überprüfen.

   Wenn diese Ereignisse keine übermäßigen Arbeitslasten beinhalten, haben sie das Leistungsereignis auf dem lokalen Cluster nicht verursacht.

Reagieren Sie auf ein dynamisches Leistungsereignis, das durch die Drosselung der QoS-Richtliniengruppe verursacht wird

Sie können Unified Manager verwenden, um ein Leistungsereignis zu untersuchen, das durch eine Quality of Service (QoS)-Richtliniengruppe verursacht wird, die den Arbeitslastdurchsatz (MB/s) drosselt. Durch die Drosselung erhöhten sich die Reaktionszeiten (Latenz) der Volumen-Workloads in der Richtliniengruppe. Anhand der Ereignisinformationen können Sie feststellen, ob neue Grenzwerte für die Richtliniengruppen erforderlich sind, um die Drosselung zu beenden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Leistungsereignisse vorliegen.

Schritte

1. Zeigen Sie die Seite **Ereignisdetails** an, um Informationen zum Ereignis anzuzeigen.
2. Lesen Sie die **Beschreibung**, in der die Namen der von der Drosselung betroffenen Workloads angezeigt werden.

   Die Beschreibung kann für Opfer und Täter die gleiche Arbeitsbelastung anzeigen, da die Arbeitsbelastung durch die Drosselung selbst zum Opfer wird.

3. Notieren Sie den Namen des Datenträgers mithilfe einer Anwendung wie beispielsweise einem Texteditor.

   Sie können nach dem Datenträgernamen suchen, um ihn später zu finden.

4. Wählen Sie in den Diagrammen „Workload-Latenz“ und „Workload-Auslastung“ **Bully Workloads** aus.
5. Bewegen Sie den Cursor über die Diagramme, um die wichtigsten benutzerdefinierten Arbeitslasten anzuzeigen, die sich auf die Richtliniengruppe auswirken.

   Die Arbeitslast am Anfang der Liste weist die größte Abweichung auf und hat zur Drosselung geführt. Die Aktivität ist der Prozentsatz des Richtliniengruppenlimits, der von jeder Arbeitslast verwendet wird.

6. Klicken Sie im Bereich **Vorgeschlagene Aktionen** auf die Schaltfläche **Arbeitslast analysieren** für die höchste Arbeitslast.
7. Legen Sie auf der Seite „Arbeitslastanalyse“ das Latenzdiagramm so fest, dass alle Clusterkomponenten angezeigt werden, und das Durchsatzdiagramm, um die Aufschlüsselung anzuzeigen.

   Die Aufschlüsselungsdiagramme werden unter dem Latenzdiagramm und dem IOPS-Diagramm angezeigt.

8. Vergleichen Sie die QoS-Grenzwerte im Diagramm **Latenz**, um zu sehen, welcher Drosselungsgrad die Latenz zum Zeitpunkt des Ereignisses beeinflusst hat.

   Die QoS-Richtliniengruppe verfügt über einen maximalen Durchsatz von 1.000 Operationen pro Sekunde (op/sec), der von den darin enthaltenen Arbeitslasten insgesamt nicht überschritten werden kann. Zum Zeitpunkt des Ereignisses hatten die Workloads in der Richtliniengruppe einen kombinierten Durchsatz von über 1.200 Operationen/Sek., was dazu führte, dass die Richtliniengruppe ihre Aktivität auf 1.000 Operationen/Sek. drosselte.

9. Vergleichen Sie die Werte für die **Lese-/Schreiblatenz** mit den Werten für **Lese-/Schreibvorgänge/Sonstiges**.

   Beide Diagramme zeigen eine hohe Anzahl von Leseanforderungen mit hoher Latenz, aber die Anzahl der Anforderungen und die Latenzzeit für Schreibanforderungen sind gering. Mithilfe dieser Werte können Sie feststellen, ob ein hoher Durchsatz oder eine hohe Anzahl von Vorgängen die Latenz erhöht hat. Sie können diese Werte verwenden, wenn Sie sich entscheiden, eine Richtliniengruppenbeschränkung für den Durchsatz oder die Vorgänge festzulegen.

10. Verwenden Sie ONTAP System Manager, um das aktuelle Limit der Richtliniengruppe auf 1.300 Operationen/Sek. zu erhöhen.
11. Kehren Sie nach einem Tag zu Unified Manager zurück und geben Sie die Arbeitslast, die Sie in Schritt 3 aufgezeichnet haben, auf der Seite **Arbeitslastanalyse** ein.
12. Wählen Sie das Diagramm „Durchsatzaufschlüsselung“ aus.

    Das Diagramm „Lesen/Schreiben/Sonstiges“ wird angezeigt.

13. Zeigen Sie oben auf der Seite mit dem Cursor auf das Symbol „Ereignis ändern“ ( ) für die Änderung des Richtliniengruppenlimits.
14. Vergleichen Sie das Diagramm **Lesen/Schreiben/Sonstiges** mit dem Diagramm **Latenz**.

    Die Lese- und Schreibanforderungen sind dieselben, aber die Drosselung wurde gestoppt und die Latenz hat abgenommen.

Reagieren auf ein dynamisches Leistungsereignis, das durch einen Datenträgerfehler verursacht wurde

Sie können Unified Manager verwenden, um ein Leistungsereignis zu untersuchen, das durch Arbeitslasten verursacht wird, die ein Aggregat überbeanspruchen. Sie können

Unified Manager auch verwenden, um den Zustand des Aggregats zu überprüfen und festzustellen, ob kürzlich auf dem Aggregat erkannte Zustandsereignisse zum Leistungsereignis beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Leistungsereignisse vorliegen.

Schritte

1. Zeigen Sie die Seite **Ereignisdetails** an, um Informationen zum Ereignis anzuzeigen.
2. Lesen Sie die **Beschreibung**, in der die am Ereignis beteiligten Arbeitslasten und die betroffene Clusterkomponente beschrieben werden.

   Es gibt mehrere Opfervolumes, deren Latenz durch die konkurrierende Clusterkomponente beeinträchtigt wurde. Das Aggregat, das sich mitten in einer RAID-Rekonstruktion befindet, um die ausgefallene Festplatte durch eine Ersatzfestplatte zu ersetzen, ist die umstrittene Clusterkomponente. Unter „Konkurrierende Komponente“ wird das Aggregatsymbol rot hervorgehoben und der Name des Aggregats in Klammern angezeigt.
3. Wählen Sie im Diagramm „Workload-Auslastung“ **Bully Workloads** aus.
4. Bewegen Sie den Cursor über das Diagramm, um die Arbeitsbelastungen anzuzeigen, die die Komponente am stärksten beeinträchtigen.

   Die Top-Workloads mit der höchsten Spitzenauslastung seit der Erkennung des Ereignisses werden oben im Diagramm angezeigt. Eine der wichtigsten Arbeitslasten ist die systemdefinierte Arbeitslast „Datenträgerintegrität“, die auf eine RAID-Rekonstruktion hinweist. Eine Rekonstruktion ist der interne Prozess, der mit dem Wiederaufbau des Aggregats mit der Ersatzfestplatte verbunden ist. Die Disk Health-Arbeitslast sowie andere Arbeitslasten auf dem Aggregat haben wahrscheinlich den Konflikt auf dem Aggregat und das damit verbundene Ereignis verursacht.
5. Nachdem Sie bestätigt haben, dass die Aktivität der Disk Health-Workload das Ereignis verursacht hat, warten Sie etwa 30 Minuten, bis die Rekonstruktion abgeschlossen ist und Unified Manager das Ereignis analysiert und ermittelt hat, ob das Aggregat noch immer im Konflikt steht.
6. Aktualisieren Sie die **Ereignisdetails**.

   Überprüfen Sie nach Abschluss der RAID-Rekonstruktion, ob der Status veraltet ist, was darauf hinweist, dass das Ereignis behoben ist.
7. Wählen Sie im Diagramm „Workload-Auslastung“ **Bully-Workloads** aus, um die Workloads insgesamt nach Spitzenauslastung anzuzeigen.
8. Klicken Sie im Bereich **Vorgeschlagene Aktionen** auf die Schaltfläche **Arbeitslast analysieren** für die höchste Arbeitslast.
9. Legen Sie auf der Seite „Workload-Analyse“ den Zeitraum so fest, dass die Daten der letzten 24 Stunden (1 Tag) für das ausgewählte Volume angezeigt werden.

   In der Ereigniszeitleiste wird ein roter Punkt (🛑) gibt an, wann das Festplattenfehlerereignis aufgetreten ist.
10. Blenden Sie im Diagramm „Knoten- und Gesamtauslastung“ die Zeile für die Knotenstatistik aus, sodass nur die Gesamtzeile übrig bleibt.
11. Vergleichen Sie die Daten in diesem Diagramm mit den Daten zum Zeitpunkt des Ereignisses im

Diagramm **Latenz**.

Zum Zeitpunkt des Ereignisses zeigt die Gesamtauslastung eine hohe Lese- und Schreibaktivität, die durch die RAID-Rekonstruktionsprozesse verursacht wurde und die Latenz des ausgewählten Volumes erhöhte. Einige Stunden nach dem Ereignis haben sich sowohl die Lese- und Schreibvorgänge als auch die Latenz verringert, was bestätigt, dass das Aggregat nicht mehr im Konflikt steht.

Reagieren Sie auf ein dynamisches Leistungsereignis, das durch die HA-Übernahme verursacht wurde

Sie können Unified Manager verwenden, um ein Leistungsereignis zu untersuchen, das durch eine hohe Datenverarbeitung auf einem Clusterknoten verursacht wird, der sich in einem Hochverfügbarkeitspaar (HA) befindet. Sie können Unified Manager auch verwenden, um den Zustand der Knoten zu überprüfen und festzustellen, ob kürzlich auf den Knoten erkannte Zustandsereignisse zum Leistungsereignis beigetragen haben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Es müssen neue, anerkannte oder veraltete Leistungsereignisse vorliegen.

Schritte

1. Zeigen Sie die Seite **Ereignisdetails** an, um Informationen zum Ereignis anzuzeigen.
2. Lesen Sie die **Beschreibung**, in der die am Ereignis beteiligten Arbeitslasten und die betroffene Clusterkomponente beschrieben werden.

   Es gibt ein Opfervolume, dessen Latenz durch die konkurrierende Clusterkomponente beeinträchtigt wurde. Der Datenverarbeitungsknoten, der alle Arbeitslasten von seinem Partnerknoten übernommen hat, ist die umstrittene Clusterkomponente. Unter „Komponente im Konflikt“ wird das Symbol „Data Processing“ rot hervorgehoben und der Name des Knotens, der zum Zeitpunkt des Ereignisses die Datenverarbeitung durchführte, wird in Klammern angezeigt.

3. Klicken Sie in der **Beschreibung** auf den Namen des Datenträgers.

   Die Seite „Volume Performance Explorer“ wird angezeigt. Oben auf der Seite, in der Zeitleiste „Ereignisse“, wird ein Symbol zum Ändern von Ereignissen ( ) gibt den Zeitpunkt an, zu dem Unified Manager den Beginn der HA-Übernahme erkannt hat.

4. Zeigen Sie mit dem Cursor auf das Änderungsereignissymbol für die HA-Übernahme. Details zur HA-Übernahme werden im 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 Leistungsschwellenwert überschritten hat.

5. Klicken Sie auf **Zoom-Ansicht**, um das Latenzdiagramm auf einer neuen Seite anzuzeigen.
6. Wählen Sie im Menü „Ansicht“ die Option „Clusterkomponenten“ aus, um die Gesamtlatenz nach Clusterkomponente anzuzeigen.
7. Bewegen Sie den Mauszeiger auf das Änderungsereignissymbol für den Beginn der HA-Übernahme und vergleichen Sie die Latenz für die Datenverarbeitung mit der Gesamtlatenz.

   Zum Zeitpunkt der HA-Übernahme kam es aufgrund der erhöhten Arbeitslast auf dem Datenverarbeitungsknoten zu einem Anstieg der Datenverarbeitung. Die erhöhte CPU-Auslastung erhöhte die Latenz und löste das Ereignis aus.

8. Nachdem Sie den ausgefallenen Knoten repariert haben, führen Sie mit ONTAP System Manager ein HA-Giveback durch, bei dem die Workloads vom Partnerknoten auf den reparierten Knoten verschoben werden.
9. Nachdem die HA-Rückgabe abgeschlossen ist, suchen Sie nach der nächsten Konfigurationserkennung in Unified Manager (ca. 15 Minuten) auf der Inventarseite **Event Management** nach dem Ereignis und der Arbeitslast, die durch die HA-Übernahme ausgelöst wurden.

   Das durch die HA-Übernahme ausgelöste Ereignis hat jetzt den Status „Veraltet“, was darauf hinweist, dass das Ereignis aufgelöst ist. Die Latenzzeit bei der Datenverarbeitungskomponente hat sich verringert, wodurch sich die Gesamtlatenzzeit verringert hat. Der Knoten, den das ausgewählte Volume jetzt zur Datenverarbeitung verwendet, hat das Ereignis aufgelöst.

Beheben von Leistungsereignissen

Sie können die vorgeschlagenen Maßnahmen nutzen, um zu versuchen, Leistungsprobleme selbst zu beheben. Die ersten drei Vorschläge werden immer angezeigt und die Aktionen unter dem vierten Vorschlag sind spezifisch für den angezeigten Ereignistyp.

Die Links **Helfen Sie mir dabei** bieten zusätzliche Informationen zu jeder vorgeschlagenen Aktion, einschließlich Anweisungen zum Ausführen 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 beinhalten.

Bestätigen Sie, dass die Latenz im erwarteten Bereich liegt

Wenn eine Clusterkomponente im Konflikt steht, kann die Reaktionszeit (Latenz) der Volume-Workloads, die sie verwenden, verkürzt sein. Sie können die Latenz der einzelnen Opfer-Workloads auf der betroffenen Komponente überprüfen, um zu bestätigen, dass die tatsächliche Latenz im erwarteten Bereich liegt. Sie können auch auf einen Volumenamen klicken, um die historischen Daten für das Volume anzuzeigen.

Wenn sich das Leistungsereignis im veralteten Zustand befindet, ist die Latenz jedes am Ereignis beteiligten Opfers möglicherweise wieder in den erwarteten Bereich zurückgekehrt.

Überprüfen Sie die Auswirkungen von Konfigurationsänderungen auf die Workload-Leistung

Konfigurationsänderungen am Cluster, wie etwa ein Festplattenfehler, ein HA-Failover oder ein verschobenes Volume, können sich negativ auf die Volume-Leistung auswirken und zu einer erhöhten Latenz führen.

In Unified Manager können Sie auf der Seite „Workload-Analyse“ nachsehen, wann kürzlich eine Konfigurationsänderung stattgefunden hat, und diese mit den Vorgängen und der Latenz (Reaktionszeit) vergleichen, um festzustellen, ob es für die ausgewählte Volume-Workload eine Änderung der Aktivität gab.

Die Leistungsseiten von Unified Manager können nur eine begrenzte Anzahl von Änderungsereignissen erkennen. Die Integritätsseiten bieten Warnungen für andere Ereignisse, die durch Konfigurationsänderungen verursacht werden. Sie können im Unified Manager nach dem Volume suchen, um den Ereignisverlauf anzuzeigen.

Optionen zur Verbesserung der Workload-Leistung auf der Clientseite

Sie können Ihre Client-Workloads (z. B. Anwendungen oder Datenbanken) überprüfen, die E/A-Daten an Volumes senden, die an einem Leistungsereignis beteiligt sind, um festzustellen, ob das Ereignis durch eine clientseitige Änderung behoben werden kann.

Wenn die mit Volumes in einem Cluster verbundenen Clients ihre E/A-Anforderungen erhöhen, muss der Cluster mehr arbeiten, um die Nachfrage zu erfüllen. Wenn Sie wissen, welche Clients eine hohe Anzahl von E/A-Anfragen an ein bestimmtes Volume im Cluster haben, können Sie die Clusterleistung verbessern, indem Sie die Anzahl der Clients anpassen, die auf das Volume zugreifen, oder die E/A-Menge für das Volume verringern. Sie können auch ein Limit auf die QoS-Richtliniengruppe anwenden oder erhöhen, deren Mitglied das Volume ist.

Sie können Clients und ihre Anwendungen untersuchen, um festzustellen, ob die Clients mehr E/A als üblich senden, was zu Konflikten bei einer Clusterkomponente führen könnte. Auf der Seite „Ereignisdetails“ werden im Abschnitt „Systemdiagnose“ die größten Volume-Workloads angezeigt, die die umstrittene Komponente verwenden. Wenn Sie wissen, welcher Client auf ein bestimmtes Volume zugreift, können Sie zum Client gehen, um festzustellen, ob die Client-Hardware oder eine Anwendung nicht wie erwartet funktioniert oder mehr Arbeit als üblich leistet.

In einer MetroCluster -Konfiguration werden Schreibanforderungen an ein Volume auf einem lokalen Cluster auf ein Volume auf dem Remote-Cluster gespiegelt. Wenn das Quellvolume auf dem lokalen Cluster mit dem Zielvolume auf dem Remotecluster synchron gehalten wird, kann dies auch die Nachfrage beider Cluster in der MetroCluster Konfiguration erhöhen. Durch die Reduzierung der Schreibanforderungen an diese gespiegelten Volumes können die Cluster weniger Synchronisierungsvorgänge durchführen, wodurch die Auswirkungen auf die Leistung anderer Workloads reduziert werden.

Suchen Sie nach Client- oder Netzwerkproblemen

Wenn die E/A-Anforderungen der mit Volumes in einem Cluster verbundenen Clients steigen, muss der Cluster mehr arbeiten, um die Nachfrage zu erfüllen. Die erhöhte Nachfrage nach dem Cluster kann zu Konflikten zwischen einer Komponente und deren Nutzung führen, die Latenz der Workloads erhöhen und ein Ereignis im Unified Manager auslösen.

Auf der Seite „Ereignisdetails“ werden im Abschnitt „Systemdiagnose“ die größten Volume-Workloads angezeigt, die die umstrittene Komponente verwenden. Wenn Sie wissen, welcher Client auf ein bestimmtes Volume zugreift, können Sie zum Client gehen, um festzustellen, ob die Client-Hardware oder eine Anwendung nicht wie erwartet funktioniert oder mehr Arbeit als üblich leistet. Möglicherweise müssen Sie sich an Ihren Clientadministrator oder Anwendungsanbieter wenden, um Hilfe zu erhalten.

Sie können Ihre Netzwerkinfrastruktur überprüfen, um festzustellen, ob Hardwareprobleme, Engpässe oder konkurrierende Arbeitslasten vorliegen, die möglicherweise dazu geführt haben, dass E/A-Anfragen zwischen dem Cluster und den verbundenen Clients langsamer als erwartet ausgeführt werden. Möglicherweise müssen Sie sich an Ihren Netzwerkadministrator wenden, um Hilfe zu erhalten.

Überprüfen Sie, ob andere Volumes in der QoS-Richtliniengruppe ungewöhnlich hohe Aktivität aufweisen

Sie können die Workloads in der Quality of Service (QoS)-Richtliniengruppe mit der größten Aktivitätsänderung überprüfen, um festzustellen, ob mehr als eine Workload das Ereignis verursacht hat. Sie können auch sehen, ob andere Workloads weiterhin das

festgelegte Durchsatzlimit überschreiten oder ob sie wieder innerhalb ihres erwarteten Aktivitätsbereichs liegen.

Auf der Seite „Ereignisdetails“ im Abschnitt „Systemdiagnose“ können Sie die Workloads nach der höchsten Aktivitätsabweichung sortieren, um die Workloads mit der größten Aktivitätsänderung oben in der Tabelle anzuzeigen. Bei diesen Arbeitslasten kann es sich möglicherweise um die „Bullys“ handeln, deren Aktivität den festgelegten Grenzwert überschritten hat und die möglicherweise das Ereignis verursacht haben.

Sie können für jede Volume-Arbeitslast zur Seite „Arbeitslastanalyse“ navigieren, um deren IOPS-Aktivität zu überprüfen. Wenn die Arbeitsbelastung in Zeiten mit sehr hoher Betriebsaktivität auftritt, könnte dies zu dem Ereignis beigetragen haben. Sie können die Richtliniengruppeneinstellungen für die Arbeitslast ändern oder die Arbeitslast in eine andere Richtliniengruppe verschieben.

Sie können den ONTAP System Manager oder die ONTAP CLI-Befehle wie folgt verwenden, um Richtliniengruppen zu verwalten:

- Erstellen Sie eine Richtliniengruppe.
- Fügen Sie Workloads einer Richtliniengruppe hinzu oder entfernen Sie sie.
- Verschieben Sie eine Arbeitslast zwischen Richtliniengruppen.
- Ändern Sie die Durchsatzgrenze einer Richtliniengruppe.

Logische Schnittstellen (LIFs) verschieben

Das Verschieben logischer Schnittstellen (LIFs) auf einen weniger ausgelasteten Port kann zur Verbesserung des Lastenausgleichs beitragen, Wartungsvorgänge und Leistungsoptimierungen unterstützen und den indirekten Zugriff reduzieren.

Indirekter Zugriff kann die Systemleistung verringern. Dies tritt auf, wenn eine große Arbeitslast verschiedene Knoten für die Netzwerkverarbeitung und die Datenverarbeitung verwendet. Um den indirekten Zugriff zu reduzieren, können Sie LIFs neu anordnen. Dazu müssen LIFs verschoben werden, um denselben Knoten für die Netzwerkverarbeitung und die Datenverarbeitung zu verwenden. Sie können den Lastenausgleich so konfigurieren, dass ONTAP ausgelastete LIFs automatisch an einen anderen Port verschiebt, oder Sie können ein LIF manuell verschieben.

Vorteile	Überlegungen
• Verbessern Sie den Lastenausgleich. • Reduzieren Sie den indirekten Zugriff.	Beim Verschieben eines mit CIFS-Freigaben verbundenen LIF wird die Verbindung der Clients, die auf die CIFS-Freigaben zugreifen, getrennt. Alle Lese- oder Schreibanforderungen an die CIFS-Freigaben werden unterbrochen.

Sie verwenden die ONTAP -Befehle, um den Lastenausgleich zu konfigurieren. Weitere Informationen finden Sie in der ONTAP Netzwerkdokumentation.

Sie verwenden ONTAP System Manager und die ONTAP CLI-Befehle, um LIFs manuell zu verschieben.

Führen Sie Speichereffizienzvorgänge in weniger ausgelasteten Zeiten durch

Sie können die Richtlinie oder den Zeitplan für Speichereffizienzvorgänge so ändern, dass sie ausgeführt werden, wenn die betroffenen Volume-Workloads weniger ausgelastet sind.

Speichereffizienzvorgänge können einen großen Teil der CPU-Ressourcen des Clusters beanspruchen und die Volumes, auf denen die Vorgänge ausgeführt werden, stark belasten. Wenn die betroffenen Volumes gleichzeitig mit der Ausführung der Speichereffizienzvorgänge eine hohe Aktivität aufweisen, kann sich ihre Latenz erhöhen und ein Ereignis auslösen.

Auf der Seite „Ereignisdetails“ werden im Abschnitt „Systemdiagnose“ die Arbeitslasten in der QoS-Richtliniengruppe nach Spitzenabweichung der Aktivität angezeigt, um die problematischsten Arbeitslasten zu identifizieren. Wenn oben in der Tabelle „Speichereffizienz“ angezeigt wird, belasten diese Vorgänge die Arbeitslast der Opfer. Indem Sie die Effizienzrichtlinie oder den Zeitplan so ändern, dass die Ausführung zu Zeiten erfolgt, in denen diese Workloads weniger ausgelastet sind, können Sie verhindern, dass die Speichereffizienzvorgänge zu Konflikten in einem Cluster führen.

Sie können ONTAP System Manager zum Verwalten von Effizienzrichtlinien verwenden. Sie können die ONTAP -Befehle verwenden, um Effizienzrichtlinien und Zeitpläne zu verwalten.

Was ist Speichereffizienz?

Durch Speichereffizienz können Sie die maximale Datenmenge zu den niedrigsten Kosten speichern und schnelles Datenwachstum bewältigen, während Sie weniger Speicherplatz verbrauchen. Die NetApp Strategie für Speichereffizienz basiert auf der integrierten Grundlage der Speichervirtualisierung und des einheitlichen Speichers, die durch das zentrale ONTAP Betriebssystem und das Write Anywhere File Layout (WAFL)-Dateisystem bereitgestellt werden.

Zur Speichereffizienz gehört der Einsatz von Technologien wie Thin Provisioning, Snapshot Copy, Deduplizierung, Datenkomprimierung, FlexClone, Thin Replication mit SnapVault und Volume SnapMirror, RAID-DP, Flash Cache, Flash Pool Aggregate und FabricPool-fähige Aggregate, die dazu beitragen, die Speicherauslastung zu erhöhen und die Speicherkosten zu senken.

Die einheitliche Speicherarchitektur ermöglicht Ihnen die effiziente Konsolidierung eines Storage Area Network (SAN), eines Network Attached Storage (NAS) und eines Sekundärspeichers auf einer einzigen Plattform.

Festplattenlaufwerke mit hoher Dichte, wie z. B. SATA-Laufwerke (Serial Advanced Technology Attachment), die innerhalb eines Flash Pool-Aggregats oder mit Flash Cache- und RAID-DP-Technologie konfiguriert sind, steigern die Effizienz, ohne die Leistung und Ausfallsicherheit zu beeinträchtigen.

Ein FabricPool-fähiges Aggregat umfasst ein reines SSD-Aggregat oder HDD-Aggregat (ab ONTAP 9.8) als lokale Leistungsebene und einen Objektspeicher, den Sie als Cloud-Ebene angeben. Durch die Konfiguration von FabricPool können Sie verwalten, auf welcher Speicherebene (der lokalen Ebene oder der Cloud-Ebene) Daten gespeichert werden sollen, je nachdem, ob häufig auf die Daten zugegriffen wird.

Technologien wie Thin Provisioning, Snapshot Copy, Deduplizierung, Datenkomprimierung, Thin Replication mit SnapVault und Volume SnapMirror sowie FlexClone bieten größere Einsparungen. Sie können diese Technologien einzeln oder zusammen verwenden, um maximale Speichereffizienz zu erreichen.

Hinzufügen von Datenträgern und Neuzuweisung von Daten

Sie können einem Aggregat Festplatten hinzufügen, um die Speicherkapazität und die Leistung dieses Aggregats zu erhöhen. Nach dem Hinzufügen der Datenträger werden Sie eine Verbesserung der Leseleistung erst feststellen, wenn Sie die Daten auf die hinzugefügten Datenträger neu verteilen.

Sie können diese Anweisungen verwenden, wenn Unified Manager aggregierte Ereignisse empfangen hat, die durch dynamische Schwellenwerte oder systemdefinierte Leistungsschwellenwerte ausgelöst wurden:

- Wenn Sie ein dynamisches Schwellenwertereignis erhalten haben, wird auf der Seite „Ereignisdetails“ das Clusterkomponentensymbol, das das konkurrierende Aggregat darstellt, rot hervorgehoben.

  Unter dem Symbol steht in Klammern der Name des Aggregats, der das Aggregat identifiziert, zu dem Sie Festplatten hinzufügen können.

- Wenn Sie ein systemdefiniertes Schwellenwertereignis erhalten haben, wird auf der Seite „Ereignisdetails“ im Ereignisbeschreibungstext der Name des Aggregats aufgeführt, bei dem das Problem auftritt.

  Sie können Festplatten hinzufügen und Daten auf diesem Aggregat neu zuweisen.

Die Festplatten, die Sie dem Aggregat hinzufügen, müssen bereits im Cluster vorhanden sein. Wenn für den Cluster keine zusätzlichen Festplatten verfügbar sind, müssen Sie sich möglicherweise an Ihren Administrator wenden oder weitere Festplatten kaufen. Sie können ONTAP System Manager oder die ONTAP -Befehle verwenden, um einem Aggregat Festplatten hinzuzufügen.

Sie sollten Daten nur neu zuweisen, wenn Sie HDD- und Flash Pool-Aggregate verwenden. Weisen Sie Daten auf SSD- oder FabricPool -Aggregaten nicht neu zu.

So kann die Aktivierung von Flash Cache auf einem Knoten die Workload-Leistung verbessern

Sie können die Workload-Leistung verbessern, indem Sie das intelligente Daten-Caching von Flash Cache™ auf jedem Knoten im Cluster aktivieren.

Ein Flash-Cache-Modul oder ein PCIe-basiertes Speichermodul mit Performance Acceleration Module optimiert die Leistung von Workloads mit vielen zufälligen Lesevorgängen, indem es als intelligenter externer Lese-Cache fungiert. Diese Hardware arbeitet mit der WAFL External Cache-Softwarekomponente von ONTAP zusammen.

In Unified Manager wird auf der Seite „Ereignisdetails“ das Clusterkomponentensymbol, das das konkurrierende Aggregat darstellt, rot hervorgehoben. Unter dem Symbol steht in Klammern der Name des Aggregats, der das Aggregat identifiziert. Sie können Flash Cache auf dem Knoten aktivieren, auf dem sich das Aggregat befindet.

Sie können den ONTAP System Manager oder die ONTAP -Befehle verwenden, um zu sehen, ob Flash Cache installiert oder aktiviert ist, und um ihn zu aktivieren, falls er noch nicht aktiviert ist. Der folgende Befehl gibt 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 dessen Verwendung finden Sie im folgenden technischen Bericht:

"Technischer Bericht 3832: Leitfaden zu Best Practices für Flash Cache"

So kann die Aktivierung von Flash Pool auf einem Speicheraggregat die Workload-Leistung verbessern

Sie können die Workload-Leistung 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 als primärer Speicher verwendet und die SSDs bieten einen leistungsstarken Lese- und Schreibcache, um die Gesamtleistung zu steigern.

In Unified Manager wird auf der Seite „Ereignisdetails“ der Name des umstrittenen Aggregats angezeigt. Sie können ONTAP System Manager oder die ONTAP -Befehle verwenden, um zu sehen, ob Flash Pool für ein Aggregat aktiviert ist. Wenn Sie SSDs installiert haben, können Sie diese über die Befehlszeilenschnittstelle aktivieren. Wenn Sie SSDs installiert haben, können Sie den folgenden Befehl auf dem Aggregat ausführen, um zu sehen, ob Flash Pool aktiviert ist: **`cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled`**

In diesem Befehl *`aggr_name`* ist der Name des Aggregats, beispielsweise des Aggregats im Streit.

Weitere Informationen zu Flash Pool und den Anforderungen für dessen Verwendung finden Sie im *Clustered Data ONTAP Physical Storage Management Guide*.

Integritätsprüfung der MetroCluster -Konfiguration

Sie können Unified Manager verwenden, um den Zustand der Cluster in einer MetroCluster -Konfiguration über IP oder FC zu überprüfen. Anhand des Integritätsstatus und der Ereignisse können Sie feststellen, ob Hardware- oder Softwareprobleme vorliegen, die die Leistung Ihrer Workloads beeinträchtigen könnten.

Wenn Sie Unified Manager zum Senden von E-Mail-Benachrichtigungen konfigurieren, können Sie Ihre E-Mails auf etwaige Integritätsprobleme im lokalen oder Remote-Cluster überprüfen, die möglicherweise zu einem Leistungsereignis beigetragen haben. In der Unified Manager-GUI können Sie **Ereignisverwaltung** auswählen, um eine Liste aktueller Ereignisse anzuzeigen, und dann die Filter verwenden, um nur MetroCluster Konfigurationsereignisse anzuzeigen.

Weitere Informationen finden Sie unter"Überprüfen der Integrität von Clustern in einer MetroCluster -Konfiguration"

Überprüfung der MetroCluster -Konfiguration

Sie können Leistungsprobleme bei gespiegelten Workloads in einem MetroCluster über FC- und IP-Konfigurationen verhindern, indem Sie sicherstellen, dass die MetroCluster Konfiguration richtig eingerichtet ist. Sie können die Workload-Leistung auch verbessern, indem Sie die Konfiguration ändern oder Software- oder Hardwarekomponenten aktualisieren.

Siehe "MetroCluster Dokumentation" Anweisungen zum Einrichten der Cluster in der MetroCluster -Konfiguration, einschließlich der Fibre Channel (FC)-Switches, Kabel und Inter-Switch-Links (ISLs). Es hilft Ihnen auch dabei, die MetroCluster -Software so zu konfigurieren, dass die lokalen und Remote-Cluster mit Spiegelvolumendaten kommunizieren können. Spezifische Informationen zu Ihrem MetroCluster over IP-Setup finden Sie unter "Installieren einer MetroCluster IP-Konfiguration" .

Sie können Ihre MetroCluster Konfiguration mit den Anforderungen in vergleichen "MetroCluster Dokumentation" um festzustellen, ob das Ändern oder Aktualisieren von Komponenten in Ihrer MetroCluster -Konfiguration die Workload-Leistung verbessern könnte. Dieser Vergleich kann Ihnen bei der Beantwortung der folgenden Fragen helfen:

- Sind die Controller für Ihre Arbeitslasten geeignet?
- Müssen Sie Ihre ISL-Pakete auf eine größere Bandbreite aktualisieren, um einen höheren Durchsatz zu bewältigen?
- Können Sie die Buffer-to-Buffer-Credits (BBC) auf Ihren Switches anpassen, um die Bandbreite zu erhöhen?
- Wenn Ihre Workloads einen hohen Schreibdurchsatz auf Solid-State-Drive-Speicher (SSD) aufweisen, müssen Sie Ihre FC-zu-SAS-Brücken aktualisieren, um den Durchsatz zu bewältigen?

Verwandte Informationen

- Informationen zum Ersetzen oder Aktualisieren von MetroCluster Komponenten finden Sie im "MetroCluster Dokumentation" .
- Informationen zum Upgrade von Controllern finden Sie unter "Aktualisieren von Controllern in einer MetroCluster FC-Konfiguration mithilfe von Switchover und Switchback" Und "Aktualisieren von Controllern in einer MetroCluster -IP-Konfiguration mithilfe von Switchover und Switchback"

Verschieben von Workloads in ein anderes Aggregat

Sie können Unified Manager verwenden, um ein Aggregat zu identifizieren, das weniger ausgelastet ist als das Aggregat, in dem sich Ihre Workloads derzeit befinden. Anschließend können Sie ausgewählte Volumes oder LUNs in dieses Aggregat verschieben. Durch die Verschiebung leistungsstarker Workloads auf ein weniger ausgelastetes Aggregat oder ein Aggregat mit aktiviertem Flash-Speicher kann die Workload effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen den Namen des Aggregats aufgezeichnet haben, bei dem derzeit ein Leistungsproblem auftritt.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu der das Aggregat das Ereignis empfangen hat.
- Unified Manager muss mindestens einen Monat lang Leistungsdaten gesammelt und analysiert haben.

Mithilfe dieser Schritte können Sie die folgenden Ressourcen identifizieren, sodass Sie leistungsstarke Workloads auf ein weniger ausgelastetes Aggregat verschieben können:

- Die Aggregate auf demselben Cluster, die weniger genutzt werden
- Die leistungsstärksten Volumina auf der aktuellen Gesamtsumme

Schritte

1. Identifizieren Sie das Aggregat im Cluster, das am wenigsten genutzt wird:
   a. Klicken Sie auf der Detailseite **Ereignis** auf den Namen des Clusters, auf dem sich das Aggregat befindet.

Die Clusterdetails werden auf der Leistungs-/Cluster-Startseite angezeigt.

b. Klicken Sie auf der Seite **Zusammenfassung** im Bereich **Verwaltete Objekte** auf **Aggregate**.

Die Liste der Aggregate in diesem Cluster wird angezeigt.

c. Klicken Sie auf die Spalte **Auslastung**, um die Aggregate nach der geringsten Auslastung zu sortieren.

Sie können auch die Aggregate identifizieren, die die größte **freie Kapazität** haben. Dadurch wird eine Liste potenzieller Aggregate bereitgestellt, auf die Sie möglicherweise Arbeitslasten verschieben möchten.

d. Notieren Sie den Namen des Aggregats, in das Sie die Workloads verschieben möchten.

2. Identifizieren Sie die leistungsstarken Volumes aus dem Aggregat, die das Ereignis empfangen haben:
   a. Klicken Sie auf das Aggregat, bei dem das Leistungsproblem auftritt.

   Die aggregierten Details werden auf der Seite „Performance/Aggregate Explorer“ angezeigt.

   b. Wählen Sie im Auswahlfeld **Zeitbereich** die Option **Letzte 30 Tage** aus und klicken Sie dann auf **Bereich anwenden**.

   Dadurch können Sie einen längeren Leistungsverlaufszeitraum als die standardmäßigen 72 Stunden anzeigen. Sie möchten ein Volume verschieben, das regelmäßig viele Ressourcen nutzt, nicht nur in den letzten 72 Stunden.

   c. Wählen Sie im Steuerelement **Anzeigen und Vergleichen** die Option **Volumes auf diesem Aggregat** aus.

   Es wird eine Liste der FlexVol Volumes und FlexGroup Bestandteilvolumes in diesem Aggregat angezeigt.

   d. Sortieren Sie die Volumes nach den höchsten MB/s und dann nach den höchsten IOPS, um die Volumes mit der höchsten Leistung anzuzeigen.
   e. Notieren Sie die Namen der Volumes, die Sie in ein anderes Aggregat verschieben möchten.
3. Verschieben Sie die Volumes mit hoher Leistung in das Aggregat, das Sie als Volume mit geringer Auslastung identifiziert haben.

   Sie können den Verschiebevorgang mithilfe von ONTAP System Manager, OnCommand Workflow Automation, ONTAP -Befehlen oder einer Kombination dieser Tools durchführen.

Überprüfen Sie nach einigen Tagen, ob Sie von diesem Knoten oder Aggregat denselben Ereignistyp erhalten.

Verschieben von Workloads auf einen anderen Knoten

Sie können Unified Manager verwenden, um ein Aggregat auf einem anderen Knoten zu identifizieren, der weniger ausgelastet ist als der Knoten, auf dem Ihre Workloads derzeit ausgeführt werden. Anschließend können Sie ausgewählte Volumes in dieses Aggregat verschieben. 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 müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen den Namen des Knotens aufgezeichnet haben, bei dem derzeit ein Leistungsproblem auftritt.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu der der Knoten das Leistungsereignis empfangen hat.
- Unified Manager muss mindestens einen Monat lang Leistungsdaten gesammelt und analysiert haben.

Mit diesem Verfahren können Sie die folgenden Ressourcen identifizieren, sodass Sie leistungsstarke Workloads auf einen weniger ausgelasteten Knoten verschieben können:

- Die Knoten im selben Cluster, die über die größte freie Leistungskapazität verfügen
- Die Aggregate auf dem neuen Knoten, die die größte freie Leistungskapazität haben
- Die leistungsstärksten Volumes auf dem aktuellen Knoten

Schritte

1. Identifizieren Sie einen Knoten im Cluster, der über die größte freie Leistungskapazität verfügt:
   a. Klicken Sie auf der Seite **Ereignisdetails** auf den Namen des Clusters, auf dem sich der Knoten befindet.

      Die Clusterdetails werden auf der Leistungs-/Cluster-Startseite angezeigt.

   b. Klicken Sie auf der Registerkarte **Zusammenfassung** im Bereich **Verwaltete Objekte** auf **Knoten**.

      Die Liste der Knoten in diesem Cluster wird angezeigt.

   c. Klicken Sie auf die Spalte **Verwendete Leistungskapazität**, um die Knoten nach dem geringsten Prozentsatz der Nutzung zu sortieren.

      Dadurch wird eine Liste potenzieller Knoten bereitgestellt, auf die Sie möglicherweise Arbeitslasten verschieben möchten.

   d. Notieren Sie den Namen des Knotens, auf den Sie die Workloads verschieben möchten.
2. Identifizieren Sie ein Aggregat auf dem neuen Knoten, das am wenigsten genutzt wird:
   a. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate** und wählen Sie im Menü „Ansicht“ die Option **Leistung** > **Alle Aggregate** aus.

      Die Ansicht „Leistung: Alle Aggregate“ wird angezeigt.

   b. Klicken Sie auf **Filtern**, wählen Sie **Knoten** aus dem linken Dropdown-Menü, geben Sie den Namen des Knotens in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.

      Die Ansicht „Leistung: Alle Aggregate“ wird erneut mit der Liste der auf diesem Knoten verfügbaren Aggregate angezeigt.

   c. Klicken Sie auf die Spalte **Genutzte Leistungskapazität**, um die Aggregate nach der am wenigsten genutzten zu sortieren.

      Dadurch wird eine Liste potenzieller Aggregate bereitgestellt, auf die Sie möglicherweise Arbeitslasten verschieben möchten.

   d. Notieren Sie den Namen des Aggregats, in das Sie die Workloads verschieben möchten.
3. Identifizieren Sie die leistungsstarken Workloads des Knotens, der das Ereignis empfangen hat:

a. Kehren Sie zur Seite **Ereignisdetails** für das Ereignis zurück.
b. Klicken Sie im Feld **Betroffene Volumes** auf den Link für die Anzahl der Volumes.

   Die Ansicht „Leistung: Alle Volumes“ wird mit einer gefilterten Liste der Volumes auf diesem Knoten angezeigt.

c. Klicken Sie auf die Spalte **Gesamtkapazität**, um die Volumes nach dem größten zugewiesenen Speicherplatz zu sortieren.

   Dadurch wird eine Liste potenzieller Datenträger bereitgestellt, die Sie möglicherweise verschieben möchten.

d. Notieren Sie die Namen der Volumes, die Sie verschieben möchten, und die Namen der aktuellen Aggregate, auf denen sie sich befinden.

4. Verschieben Sie die Volumes auf die Aggregate, die Ihrer Meinung nach die größte freie Leistungskapazität auf dem neuen Knoten aufweisen.

   Sie können den Verschiebevorgang mithilfe von ONTAP System Manager, OnCommand Workflow Automation, ONTAP -Befehlen oder einer Kombination dieser Tools durchführen.

Nach einigen Tagen können Sie überprüfen, ob Sie von diesem Knoten oder Aggregat den gleichen Ereignistyp erhalten.

Verschieben von Workloads in ein Aggregat auf einem anderen Knoten

Sie können Unified Manager verwenden, um ein Aggregat auf einem anderen Knoten zu identifizieren, der weniger ausgelastet ist als der Knoten, auf dem Ihre Workloads derzeit ausgeführt werden. Anschließend können Sie ausgewählte Volumes in dieses Aggregat verschieben. Durch die Verschiebung leistungsstarker Workloads auf ein Aggregat auf einem weniger ausgelasteten Knoten können die Workloads auf beiden Knoten effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen den Namen des Knotens aufgezeichnet haben, bei dem derzeit ein Leistungsproblem auftritt.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu der der Knoten das Leistungsereignis empfangen hat.
- Unified Manager muss mindestens einen Monat lang Leistungsdaten gesammelt und analysiert haben.

Mithilfe dieser Schritte können Sie die folgenden Ressourcen identifizieren, sodass Sie leistungsstarke Workloads auf einen Knoten mit geringerer Auslastung verschieben können:

- Die Knoten im selben Cluster, die weniger genutzt werden
- Die Aggregate auf dem neuen Knoten, die am wenigsten genutzt werden
- Die leistungsstärksten Volumes auf dem aktuellen Knoten

Schritte

1. Identifizieren Sie einen Knoten im Cluster, der am wenigsten genutzt wird:

a. Klicken Sie auf der Detailseite **Ereignis** auf den Namen des Clusters, auf dem sich der Knoten befindet.

   Die Clusterdetails werden auf der Leistungs-/Cluster-Startseite angezeigt.

b. Klicken Sie auf der Seite **Zusammenfassung** im Bereich **Verwaltete Objekte** auf **Knoten**.

   Die Liste der Knoten in diesem Cluster wird angezeigt.

c. Klicken Sie auf die Spalte **Auslastung**, um die Knoten nach der geringsten Auslastung zu sortieren.

   Sie können auch die Knoten identifizieren, die über die größte **freie Kapazität** verfügen. Dadurch wird eine Liste potenzieller Knoten bereitgestellt, auf die Sie möglicherweise Arbeitslasten verschieben möchten.

d. Notieren Sie den Namen des Knotens, auf den Sie die Workloads verschieben möchten.

2. Identifizieren Sie ein Aggregat auf dem neuen Knoten, das am wenigsten genutzt wird:
   a. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate** und wählen Sie im Menü „Ansicht“ die Option **Leistung** > **Alle Aggregate** aus.

      Die Ansicht „Leistung: Alle Aggregate“ wird angezeigt.

   b. Klicken Sie auf **Filtern**, wählen Sie **Knoten** aus dem linken Dropdown-Menü, geben Sie den Namen des Knotens in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.

      Die Ansicht „Leistung: Alle Aggregate“ wird erneut mit der Liste der auf diesem Knoten verfügbaren Aggregate angezeigt.

   c. Klicken Sie auf die Spalte **Auslastung**, um die Aggregate nach der geringsten Auslastung zu sortieren.

      Sie können auch die Aggregate identifizieren, die die größte **freie Kapazität** haben. Dadurch wird eine Liste potenzieller Aggregate bereitgestellt, auf die Sie möglicherweise Arbeitslasten verschieben möchten.

   d. Notieren Sie den Namen des Aggregats, in das Sie die Workloads verschieben möchten.

3. Identifizieren Sie die leistungsstarken Workloads des Knotens, der das Ereignis empfangen hat:
   a. Kehren Sie zur Detailseite **Event** für das Event zurück.
   b. Klicken Sie im Feld **Betroffene Volumes** auf den Link für die Anzahl der Volumes.

      Die Ansicht „Leistung: Alle Volumes“ wird mit einer gefilterten Liste der Volumes auf diesem Knoten angezeigt.

   c. Klicken Sie auf die Spalte **Gesamtkapazität**, um die Volumes nach dem größten zugewiesenen Speicherplatz zu sortieren.

      Dadurch wird eine Liste potenzieller Datenträger bereitgestellt, die Sie möglicherweise verschieben möchten.

   d. Notieren Sie die Namen der Volumes, die Sie verschieben möchten, und die Namen der aktuellen Aggregate, auf denen sie sich befinden.

4. Verschieben Sie die Volumes auf die Aggregate, die Ihrer Meinung nach auf dem neuen Knoten eine geringe Auslastung aufweisen.

Sie können den Verschiebevorgang mithilfe von ONTAP System Manager, OnCommand Workflow Automation, ONTAP -Befehlen oder einer Kombination dieser Tools durchführen.

Überprüfen Sie nach einigen Tagen, ob Sie von diesem Knoten oder Aggregat denselben Ereignistyp erhalten.

Verschieben Sie Workloads auf einen Knoten in einem anderen HA-Paar

Sie können Unified Manager verwenden, um ein Aggregat auf einem Knoten in einem anderen Hochverfügbarkeitspaar (HA) zu identifizieren, das über mehr freie Leistungskapazität verfügt als das HA-Paar, auf dem Ihre Workloads derzeit ausgeführt werden. Anschließend können Sie ausgewählte Volumes in Aggregate auf dem neuen HA-Paar verschieben.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Ihr Cluster muss aus mindestens zwei HA-Paaren bestehen

  Sie können diesen Behebungsprozess nicht verwenden, wenn Ihr Cluster nur über ein HA-Paar verfügt.

- Sie müssen die Namen der beiden Knoten im HA-Paar aufgezeichnet haben, bei denen derzeit ein Leistungsproblem auftritt.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu der die Knoten das Leistungsereignis empfangen haben.
- Unified Manager muss mindestens einen Monat lang Leistungsdaten gesammelt und analysiert haben.

Durch das Verschieben leistungsstarker Workloads auf ein Aggregat auf einem Knoten mit mehr freier Leistungskapazität können Workloads auf beiden Knoten effizienter ausgeführt werden. Mit diesem Verfahren können Sie die folgenden Ressourcen identifizieren, sodass Sie leistungsstarke Workloads auf einen Knoten verschieben können, der über mehr freie Leistungskapazität auf einem anderen HA-Paar verfügt:

- Die Knoten in einem anderen HA-Paar im selben Cluster, die über die größte freie Leistungskapazität verfügen
- Die Aggregate auf den neuen Knoten, die die größte freie Leistungskapazität haben
- Die leistungsstärksten Volumes auf den aktuellen Knoten

Schritte

1. Identifizieren Sie die Knoten, die Teil eines anderen HA-Paares im selben Cluster sind:
   a. Klicken Sie auf der Seite **Ereignisdetails** auf den Namen des Clusters, auf dem sich die Knoten befinden.

      Die Clusterdetails werden auf der Leistungs-/Cluster-Startseite angezeigt.

   b. Klicken Sie auf der Seite **Zusammenfassung** im Bereich **Verwaltete Objekte** auf **Knoten**.

      Die Liste der Knoten in diesem Cluster wird in der Ansicht „Leistung: Alle Knoten“ angezeigt.

   c. Notieren Sie die Namen der Knoten, die sich in anderen HA-Paaren befinden als das HA-Paar, bei dem derzeit ein Leistungsproblem auftritt.
2. Identifizieren Sie einen Knoten im neuen HA-Paar, der über die größte freie Leistungskapazität verfügt:

a. Klicken Sie in der Ansicht **Leistung: Alle Knoten** auf die Spalte **Genutzte Leistungskapazität**, um die Knoten nach dem geringsten Prozentsatz der Nutzung zu sortieren.

   Dadurch wird eine Liste potenzieller Knoten bereitgestellt, auf die Sie möglicherweise Arbeitslasten verschieben möchten.

b. Notieren Sie den Namen des Knotens auf einem anderen HA-Paar, auf den Sie die Workloads verschieben möchten.

3. Identifizieren Sie ein Aggregat auf dem neuen Knoten, das über die größte freie Leistungskapazität verfügt:
   a. Klicken Sie in der Ansicht **Leistung: Alle Knoten** auf den Knoten.

      Die Knotendetails werden auf der Seite „Leistung/Knoten-Explorer“ angezeigt.

   b. Wählen Sie im Menü **Anzeigen und Vergleichen** die Option **Aggregate auf diesem Knoten** aus.

      Die Aggregate auf diesem Knoten werden im Raster angezeigt.

   c. Klicken Sie auf die Spalte **Genutzte Leistungskapazität**, um die Aggregate nach der am wenigsten genutzten zu sortieren.

      Dadurch wird eine Liste potenzieller Aggregate bereitgestellt, auf die Sie möglicherweise Arbeitslasten verschieben möchten.

   d. Notieren Sie den Namen des Aggregats, in das Sie die Workloads verschieben möchten.
4. Identifizieren Sie die leistungsstarken Workloads der Knoten, die das Ereignis empfangen haben:
   a. Kehren Sie zur Detailseite **Event** für das Event zurück.
   b. Klicken Sie im Feld **Betroffene Volumes** auf den Link für die Anzahl der Volumes für den ersten Knoten.

      Die Ansicht „Leistung: Alle Volumes“ wird mit einer gefilterten Liste der Volumes auf diesem Knoten angezeigt.

   c. Klicken Sie auf die Spalte **Gesamtkapazität**, um die Volumes nach dem größten zugewiesenen Speicherplatz zu sortieren.

      Dadurch wird eine Liste potenzieller Datenträger bereitgestellt, die Sie möglicherweise verschieben möchten.

   d. Notieren Sie die Namen der Volumes, die Sie verschieben möchten, und die Namen der aktuellen Aggregate, auf denen sie sich befinden.
   e. Führen Sie die Schritte 4c und 4d für den zweiten Knoten aus, der Teil dieses Ereignisses war, um mögliche Volumes zu identifizieren, die Sie ebenfalls von diesem Knoten verschieben möchten.
5. Verschieben Sie die Volumes auf die Aggregate, die Ihrer Meinung nach die größte freie Leistungskapazität auf dem neuen Knoten aufweisen.

   Sie können den Verschiebevorgang mithilfe von ONTAP System Manager, OnCommand Workflow Automation, ONTAP -Befehlen oder einer Kombination dieser Tools durchführen.

Nach einigen Tagen können Sie überprüfen, ob Sie von diesem Knoten oder Aggregat den gleichen Ereignistyp erhalten.

Verschieben Sie Workloads auf einen anderen Knoten in einem anderen HA-Paar

Sie können Unified Manager verwenden, um ein Aggregat auf einem Knoten in einem anderen HA-Paar zu identifizieren, das weniger ausgelastet ist als das HA-Paar, auf dem Ihre Workloads derzeit ausgeführt werden. Anschließend können Sie ausgewählte Volumes in Aggregate auf dem neuen HA-Paar verschieben. Durch die Verschiebung leistungsstarker Workloads auf ein Aggregat auf einem weniger ausgelasteten Knoten können die Workloads auf beiden Knoten effizienter ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Ihr Cluster muss aus mindestens zwei HA-Paaren bestehen. Sie können diesen Korrekturprozess nicht verwenden, wenn Ihr Cluster nur über ein HA-Paar verfügt.
- Sie müssen die Namen der beiden Knoten im HA-Paar aufgezeichnet haben, bei denen derzeit das Leistungsproblem auftritt.
- Sie müssen das Datum und die Uhrzeit aufgezeichnet haben, zu der die Knoten das Leistungsereignis empfangen haben.
- Unified Manager muss mindestens einen Monat lang Leistungsdaten gesammelt und analysiert haben.

Mithilfe dieser Schritte können Sie die folgenden Ressourcen identifizieren, sodass Sie leistungsstarke Workloads auf einen weniger ausgelasteten Knoten auf einem anderen HA-Paar verschieben können:

- Die Knoten in einem anderen HA-Paar im selben Cluster, die weniger genutzt werden
- Die Aggregate auf den neuen Knoten, die am wenigsten genutzt werden
- Die leistungsstärksten Volumes auf den aktuellen Knoten

Schritte

1. Identifizieren Sie die Knoten, die Teil eines anderen HA-Paares im selben Cluster sind:
   a. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Cluster** und wählen Sie im Menü „Ansicht“ die Option **Leistung** > **Alle Cluster** aus.

      Die Ansicht „Leistung: Alle Cluster“ wird angezeigt.

   b. Klicken Sie auf die Zahl im Feld **Knotenanzahl** für den aktuellen Cluster.

      Die Ansicht „Leistung: Alle Knoten“ wird angezeigt.

   c. Notieren Sie die Namen der Knoten, die sich in anderen HA-Paaren befinden als das HA-Paar, bei dem derzeit das Leistungsproblem auftritt.
2. Identifizieren Sie einen Knoten im neuen HA-Paar, der am wenigsten genutzt wird:
   a. Klicken Sie auf die Spalte **Auslastung**, um die Knoten nach der geringsten Auslastung zu sortieren.

      Sie können auch die Knoten identifizieren, die über die größte **freie Kapazität** verfügen. Dadurch wird eine Liste potenzieller Knoten bereitgestellt, auf die Sie möglicherweise Arbeitslasten verschieben möchten.

   b. Notieren Sie den Namen des Knotens, auf den Sie die Workloads verschieben möchten.
3. Identifizieren Sie ein Aggregat auf dem neuen Knoten, das am wenigsten genutzt wird:

a. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate** und wählen Sie im Menü „Ansicht“ die Option **Leistung** > **Alle Aggregate** aus.

   Die Ansicht „Leistung: Alle Aggregate“ wird angezeigt.

b. Klicken Sie auf **Filtern**, wählen Sie **Knoten** aus dem linken Dropdown-Menü, geben Sie den Namen des Knotens in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.

   Die Ansicht „Leistung: Alle Aggregate“ wird erneut mit der Liste der auf diesem Knoten verfügbaren Aggregate angezeigt.

c. Klicken Sie auf die Spalte **Auslastung**, um die Aggregate nach der geringsten Auslastung zu sortieren.

   Sie können auch die Aggregate identifizieren, die die größte **freie Kapazität** haben. Dadurch wird eine Liste potenzieller Aggregate bereitgestellt, auf die Sie möglicherweise Arbeitslasten verschieben möchten.

d. Notieren Sie den Namen des Aggregats, in das Sie die Workloads verschieben möchten.

4. Identifizieren Sie die leistungsstarken Workloads der Knoten, die das Ereignis empfangen haben:
   a. Kehren Sie zur Detailseite **Event** für das Event zurück.
   b. Klicken Sie im Feld **Betroffene Volumes** auf den Link für die Anzahl der Volumes für den ersten Knoten.

      Die Ansicht „Leistung: Alle Volumes“ wird mit einer gefilterten Liste der Volumes auf diesem Knoten angezeigt.

   c. Klicken Sie auf die Spalte **Gesamtkapazität**, um die Volumes nach dem größten zugewiesenen Speicherplatz zu sortieren.

      Dadurch wird eine Liste potenzieller Datenträger bereitgestellt, die Sie möglicherweise verschieben möchten.

   d. Notieren Sie die Namen der Volumes, die Sie verschieben möchten, und die Namen der aktuellen Aggregate, auf denen sie sich befinden.
   e. Führen Sie die Schritte 4c und 4d für den zweiten Knoten aus, der Teil dieses Ereignisses war, um mögliche Volumes zu identifizieren, die Sie ebenfalls von diesem Knoten verschieben möchten.
5. Verschieben Sie die Volumes auf die Aggregate, die Ihrer Meinung nach auf dem neuen Knoten eine geringe Auslastung aufweisen.

   Sie können den Verschiebevorgang mithilfe von ONTAP System Manager, OnCommand Workflow Automation, ONTAP -Befehlen oder einer Kombination dieser Tools durchführen.

Überprüfen Sie nach einigen Tagen, ob Sie von diesem Knoten oder Aggregat denselben Ereignistyp erhalten.

Verwenden Sie QoS-Richtlinieneinstellungen, um die Arbeit an diesem Knoten zu priorisieren

Sie können für eine QoS-Richtliniengruppe ein Limit festlegen, um die E/A-pro-Sekunde (IOPS) oder den MBps-Durchsatz für die darin enthaltenen Workloads zu steuern. Wenn sich Workloads in einer Richtliniengruppe ohne festgelegte Begrenzung befinden, beispielsweise in der Standardrichtliniengruppe, oder die festgelegte Begrenzung Ihren

Anforderungen nicht entspricht, können Sie die festgelegte Begrenzung erhöhen oder die Workloads in eine neue oder vorhandene Richtliniengruppe verschieben, die über die gewünschte Begrenzung verfügt.

Wenn ein Leistungsereignis auf einem Knoten durch Arbeitslasten verursacht wird, die die Knotenressourcen überbeanspruchen, wird in der Ereignisbeschreibung auf der Seite „Ereignisdetails“ ein Link zur Liste der betroffenen Volumes angezeigt. Auf der Seite „Leistung/Volumes“ können Sie die betroffenen Volumes nach IOPS und MBps sortieren, um zu sehen, welche Workloads die höchste Auslastung aufweisen, die möglicherweise zu dem Ereignis beigetragen hat.

Indem den Volumes, die die Knotenressourcen übermäßig nutzen, eine restriktivere Richtliniengruppeneinstellung zugewiesen wird, drosselt die Richtliniengruppe die Arbeitslasten, um ihre Aktivität einzuschränken, wodurch die Nutzung der Ressourcen auf diesem Knoten reduziert werden 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 Arbeitslast zwischen Richtliniengruppen
- Ändern des Durchsatzlimits einer Richtliniengruppe

Entfernen inaktiver Volumes und LUNs

Wenn der aggregierte freie Speicherplatz als Problem identifiziert wurde, können Sie nach nicht verwendeten Volumes und LUNs suchen und diese aus dem Aggregat löschen. Dies kann dazu beitragen, das Problem des geringen Speicherplatzes zu beheben.

Wenn ein Leistungsereignis auf einem Aggregat durch geringen Speicherplatz verursacht wird, gibt es einige Möglichkeiten, um festzustellen, welche Volumes und LUNs nicht mehr verwendet werden.

So identifizieren Sie nicht verwendete Volumes:

- Auf der Seite mit den Ereignisdetails enthält das Feld **Anzahl betroffener Objekte** einen Link, der die Liste der betroffenen Volumes anzeigt.

  Klicken Sie auf den Link, um die Volumes in der Ansicht „Leistung: Alle Volumes“ anzuzeigen. Von dort aus können Sie die betroffenen Volumes nach **IOPS** sortieren, um zu sehen, welche Volumes nicht aktiv waren.

So identifizieren Sie nicht verwendete LUNs:

1. Notieren Sie auf der Seite „Ereignisdetails“ den Namen des Aggregats, auf dem das Ereignis aufgetreten ist.
2. Klicken Sie im linken Navigationsbereich auf **Speicher** > **LUNs** und wählen Sie im Menü „Ansicht“ die Option **Leistung** > **Alle LUNs** aus.
3. Klicken Sie auf **Filtern**, wählen Sie **Aggregat** aus dem linken Dropdown-Menü aus, geben Sie den Namen des Aggregats in das Textfeld ein und klicken Sie dann auf **Filter anwenden**.
4. Sortieren Sie die resultierende Liste der betroffenen LUNs nach **IOPS**, um die LUNs anzuzeigen, die nicht aktiv sind.

Nachdem Sie die nicht verwendeten Volumes und LUNs identifiziert haben, können Sie diese Objekte mit dem ONTAP System Manager oder den ONTAP -Befehlen löschen.

Fügen Sie Datenträger hinzu und führen Sie eine Rekonstruktion des Gesamtlayouts durch

Sie können einem Aggregat Festplatten hinzufügen, um die Speicherkapazität und die Leistung dieses Aggregats zu erhöhen. Nach dem Hinzufügen der Festplatten sehen Sie erst nach dem Neuaufbau des Aggregats eine Leistungsverbesserung.

Wenn Sie auf der Seite „Ereignisdetails“ ein systemdefiniertes Schwellenwertereignis erhalten, wird im Ereignisbeschreibungstext der Name des Aggregats aufgeführt, bei dem das Problem auftritt. Sie können Datenträger hinzufügen und Daten auf diesem Aggregat rekonstruieren.

Die Festplatten, die Sie dem Aggregat hinzufügen, müssen bereits im Cluster vorhanden sein. Wenn für den Cluster keine zusätzlichen Festplatten verfügbar sind, müssen Sie sich möglicherweise an Ihren Administrator wenden oder weitere Festplatten kaufen. Sie können ONTAP System Manager oder die ONTAP -Befehle verwenden, um einem Aggregat Festplatten hinzuzufügen.

"Technischer Bericht 3838: Konfigurationshandbuch für Speichersubsysteme"

Einrichten einer Verbindung zwischen einem Unified Manager-Server und einem externen Datenanbieter

Über eine Verbindung zwischen einem Unified Manager-Server und einem externen Datenanbieter können Sie Cluster-Leistungsdaten an einen externen Server senden, sodass Speichermanager die Leistungsmetriken mithilfe von Drittanbietersoftware grafisch darstellen können.

Eine Verbindung zwischen einem Unified Manager-Server und einem externen Datenanbieter wird über die Menüoption „Externer Datenanbieter“ in der Wartungskonsole hergestellt.

Leistungsdaten, die an einen externen Server gesendet werden können

Unified Manager sammelt eine Vielzahl von Leistungsdaten von allen Clustern, die er überwacht. Sie können bestimmte Datengruppen an einen externen Server senden.

Abhängig von den Leistungsdaten, die Sie grafisch darstellen möchten, können Sie eine der folgenden Statistikgruppen senden:

Statistikgruppe	Daten enthalten	Details
Leistungsmonitor	Leistungsstatistiken auf hoher Ebene für die folgenden Objekte: • LUNs • Bände	Diese Gruppe bietet die gesamten IOPS oder Latenz für alle LUNs und Volumes in allen überwachten Clustern. Diese Gruppe bietet die geringste Anzahl an Statistiken.

Statistikgruppe	Daten enthalten	Details
Ressourcennutzung	Statistiken zur Ressourcennutzung für die folgenden Objekte: • Nodes • Aggregate	Diese Gruppe bietet Nutzungsstatistiken für den Knoten und aggregierte physische Ressourcen in allen überwachten Clustern. Es stellt auch die in der Leistungsmonitorgruppe gesammelten Statistiken bereit.
Drilldown	Low-Level-Lese-/Schreib- und Protokollstatistiken für alle verfolgten Objekte: • Nodes • Aggregate • LUNs • Bände • Festplatten • LIFs • Anschlüsse/Netzwerkkarten	Diese Gruppe bietet Lese-/Schreib- und Protokollaufschlüsselungen für alle sieben verfolgten Objekttypen in allen überwachten Clustern. Es stellt außerdem die in der Gruppe „Leistungsmonitor“ und in der Gruppe „Ressourcennutzung“ gesammelten Statistiken bereit. Diese Gruppe bietet die größte Anzahl an Statistiken.

Wenn der Name eines Clusters oder Clusterobjekts auf dem Speichersystem geändert wird, enthalten sowohl das alte als auch das neue Objekt Leistungsdaten auf dem externen Server (genannt „metric_path“). Die beiden Objekte werden nicht als dasselbe Objekt korreliert. Wenn Sie beispielsweise den Namen eines Volumes von „`volume1_acct`“ in „`acct_vol1`“ ändern, werden alte Leistungsdaten für das alte Volume und neue Leistungsdaten für das neue Volume angezeigt.

Eine Liste aller Leistungsindikatoren, die an einen externen Datenanbieter gesendet werden können, finden Sie im Knowledge Base-Artikel 30096.

"Unified Manager-Leistungsindikatoren, die an einen externen Datenanbieter exportiert werden können"

Richten Sie Graphite ein, um Leistungsdaten von Unified Manager zu erhalten

Graphite ist ein offenes Softwaretool zum Sammeln und grafischen Darstellen von Leistungsdaten von Computersystemen. Ihr Graphite-Server und Ihre Graphite-Software müssen richtig konfiguriert sein, um statistische Daten von Unified Manager zu empfangen.

NetApp testet oder überprüft keine bestimmten Versionen von Graphite oder anderen Tools von Drittanbietern.

Der Graphite-Server empfängt keine Leistungsdaten für Volumes vom Unified Manager.

Nachdem Sie Graphite gemäß den Installationsanweisungen installiert haben, müssen Sie die folgenden

Änderungen vornehmen, um die statistische Datenübertragung von Unified Manager zu unterstützen:

- Im `/opt/graphite/conf/carbon.conf` Datei, die maximale Anzahl der Dateien, die pro Minute auf dem Graphite-Server erstellt werden können, muss auf *200* eingestellt werden(**`MAX_CREATES_PER_MINUTE = 200`**).

  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 erstellt sind. Nachdem alle eindeutigen Metrikdateien erstellt wurden, ist dieser Parameter nicht mehr relevant.

- Wenn Sie Graphite auf einem Server ausführen, der mit einer IPv6-Adresse bereitgestellt wird, ist der Wert für LINE_RECEIVER_INTERFACE in der `/opt/graphite/conf/carbon.conf` Datei muss von "0.0.0.0" in "::" geändert werden(**`LINE_RECEIVER_INTERFACE = ::`**)
- Im `/opt/graphite/conf/storage-schemas.conf` Datei, die `retentions` Mit dem Parameter muss die Häufigkeit auf 5 Minuten und die Aufbewahrungsdauer auf die für Ihre Umgebung relevante Anzahl von Tagen eingestellt werden.

  Der Aufbewahrungszeitraum kann so lang sein, wie es Ihre Umgebung zulässt, der Frequenzwert muss jedoch für mindestens eine Aufbewahrungseinstellung auf 5 Minuten festgelegt werden. Im folgenden Beispiel wird ein Abschnitt für Unified Manager definiert, indem der `pattern` Parameter, 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-Anbieter-Tag von „netapp-performance“ in etwas anderes geändert wird, muss diese Änderung in der `pattern` Parameter ebenfalls.

Wenn der Graphite-Server nicht verfügbar ist, während der Unified Manager-Server versucht, Leistungsdaten zu senden, werden die Daten nicht gesendet und es entsteht eine Lücke in den erfassten Daten.

Konfigurieren einer Verbindung von einem Unified Manager-Server zu einem externen Datenanbieter

Unified Manager kann Cluster-Leistungsdaten an einen externen Server senden. Sie können den Typ der zu sendenden statistischen Daten und das Intervall angeben, in dem die Daten gesendet werden.

Bevor Sie beginnen

- Sie müssen über eine Benutzer-ID verfügen, die zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigt ist.
- Sie benötigen folgende Informationen zum externen Datenanbieter:
  - Servername oder IP-Adresse (IPv4 oder IPv6)
  - Standardport des Servers (wenn 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.

- Sie müssen wissen, welche Statistikgruppe Sie senden möchten:
  - PERFORMANCE_INDICATOR: Leistungsüberwachungsstatistiken
  - RESOURCE_UTILIZATION: Ressourcennutzung und Leistungsüberwachungsstatistiken
  - DRILL_DOWN: Alle Statistiken
- Sie müssen das Zeitintervall kennen, in dem Sie Statistiken übertragen möchten: 5, 10 oder 15 Minuten

  Standardmäßig sammelt Unified Manager Statistiken in 5-Minuten-Intervallen. Wenn Sie das Übertragungsintervall auf 10 (oder 15) Minuten einstellen, ist die Datenmenge, die bei jeder Übertragung gesendet wird, zwei- (oder dreimal) größer als bei Verwendung des Standardintervalls von 5 Minuten.

  Wenn Sie das Leistungserfassungsintervall des Unified Managers auf 10 oder 15 Minuten ändern, müssen Sie das Übertragungsintervall so ändern, dass es gleich oder größer als das Erfassungsintervall des Unified Managers ist.

Sie können eine Verbindung zwischen einem Unified Manager-Server und einem externen Datenanbieterserver konfigurieren.

Schritte

1. Melden Sie sich als Wartungsbenutzer bei der Wartungskonsole des Unified Manager-Servers an.

   Die Eingabeaufforderungen der Unified Manager-Wartungskonsole werden angezeigt.

2. Geben Sie in der Wartungskonsole die Nummer der Menüoption **Externer Datenanbieter** ein.

   Das Menü „Externe Serververbindung“ wird angezeigt.

3. Geben Sie die Nummer der Menüoption **Serververbindung hinzufügen/ändern** ein.

   Die aktuellen Serververbindungsinformationen werden angezeigt.

4. Wenn Sie dazu aufgefordert werden, geben Sie `y` , um fortzufahren.
5. Geben Sie bei entsprechender Aufforderung die IP-Adresse oder den Namen des Zielservers und die Server-Port-Informationen ein (falls diese vom Standardport 2003 abweichen).
6. Wenn Sie dazu aufgefordert werden, geben Sie `y` um zu überprüfen, ob die von Ihnen eingegebenen Informationen korrekt sind.
7. Drücken Sie eine beliebige Taste, um zum Menü „Externe Serververbindung“ zurückzukehren.
8. Geben Sie die Nummer der Menüoption **Serverkonfiguration ändern** ein.

   Die aktuellen Serverkonfigurationsinformationen werden angezeigt.

9. Wenn Sie dazu aufgefordert werden, geben Sie `y` , um fortzufahren.
10. Geben Sie bei der entsprechenden Aufforderung den Typ der zu sendenden Statistiken sowie das Zeitintervall ein, in dem die Statistiken gesendet werden, und ob Sie die Übertragung der Statistiken jetzt aktivieren möchten:

Für..	Eingeben…
Statistikgruppen-ID	**0**- PERFORMANCE_INDICATOR (Standard) **1**- RESSOURCENUTLIZATION **2**- DRILL_DOWN
Lieferanten-Tag	Ein beschreibender Name für den Ordner, in dem die Statistiken auf dem externen Server gespeichert werden. „`netapp-performance`“ ist der Standardname, Sie können jedoch einen anderen Wert eingeben. Durch die Verwendung der Punktnotation können Sie eine hierarchische Ordnerstruktur definieren. Zum Beispiel durch die Eingabe **`stats.performance.netapp`** Die Statistiken befinden sich unter **Statistiken** > **Leistung** > **NetApp**.
Sendeintervall	**5**(Standard), **10** , oder **15** Minuten
Aktivieren/Deaktivieren	**0**- Deaktivieren **1**- Aktivieren (Standard)

11. Wenn Sie dazu aufgefordert werden, geben Sie **y** um zu überprüfen, ob die von Ihnen eingegebenen Informationen korrekt sind.
12. Drücken Sie eine beliebige Taste, um zum Menü „Externe Serververbindung“ zurückzukehren.
13. Typ **x** , um die Wartungskonsole zu verlassen.

Nachdem Sie die Verbindung konfiguriert haben, werden die ausgewählten Leistungsdaten im von Ihnen angegebenen Zeitintervall an den Zielserver gesendet. Es dauert einige Minuten, bis die Messwerte im externen Tool angezeigt werden. Möglicherweise müssen Sie Ihren Browser aktualisieren, um die neuen Metriken in der Metrikhierarchie anzuzeigen.

Überwachen und Verwalten der Clusterintegrität

Einführung in die Integritätsüberwachung von Active IQ Unified Manager

Active IQ Unified Manager (früher OnCommand Unified Manager) hilft Ihnen, eine große Anzahl von Systemen mit ONTAP -Software über eine zentrale Benutzeroberfläche zu überwachen. Die Unified Manager-Serverinfrastruktur bietet Skalierbarkeit, Supportfähigkeit und erweiterte Überwachungs- und Benachrichtigungsfunktionen.

Zu den wichtigsten Funktionen von Unified Manager gehören Überwachung, Alarmierung, Verwaltung der Verfügbarkeit und Kapazität von Clustern, Verwaltung von Schutzfunktionen sowie Bündelung und Übermittlung von Diagnosedaten an den technischen Support.

Sie können Unified Manager zur Überwachung Ihrer Cluster verwenden. Wenn im Cluster Probleme auftreten, benachrichtigt Sie Unified Manager über die Details dieser Probleme durch Ereignisse. Bei einigen Ereignissen stehen Ihnen auch Abhilfemaßnahmen zur Verfügung, mit denen Sie die Probleme beheben können. Sie können Warnmeldungen für Ereignisse konfigurieren, sodass Sie beim Auftreten von Problemen per E-Mail und SNMP-Traps benachrichtigt werden.

Sie können Unified Manager verwenden, um Speicherobjekte in Ihrer Umgebung zu verwalten, indem Sie sie mit Anmerkungen verknüpfen. Sie können benutzerdefinierte Anmerkungen erstellen und Cluster, virtuelle Speichermaschinen (SVMs) und Volumes mithilfe von Regeln dynamisch mit den Anmerkungen verknüpfen.

Sie können den Speicherbedarf Ihrer Clusterobjekte auch anhand der in den Kapazitäts- und Integritätsdiagrammen für das jeweilige Clusterobjekt bereitgestellten Informationen planen.

Körperliche und logische Leistungsfähigkeit

Unified Manager nutzt die Konzepte des physischen und logischen Speicherplatzes, die für ONTAP Speicherobjekte verwendet werden.

- Physische Kapazität: Physischer Speicherplatz bezieht sich auf die im Datenträger verwendeten physischen Speicherblöcke. Die „physisch genutzte Kapazität“ ist aufgrund der Datenreduzierung durch Speichereffizienzfunktionen (wie Deduplizierung und Komprimierung) normalerweise kleiner als die logisch genutzte Kapazität.
- Logische Kapazität: Der logische Speicherplatz bezieht sich auf den nutzbaren Speicherplatz (die logischen Blöcke) in einem Volume. Der logische Speicherplatz bezieht sich darauf, wie der theoretische Speicherplatz genutzt werden kann, ohne die Ergebnisse der Deduplizierung oder Komprimierung zu berücksichtigen. Der „genutzte logische Speicherplatz“ ist der genutzte physische Speicherplatz zuzüglich der Einsparungen durch konfigurierte Speichereffizienzfunktionen (wie Deduplizierung und Komprimierung). Dieser Messwert erscheint häufig größer als die physisch genutzte Kapazität, da er die Datenkomprimierung und andere Reduzierungen des physischen Speicherplatzes nicht berücksichtigt. Daher kann die gesamte logische Kapazität höher sein als der bereitgestellte Speicherplatz.

Kapazitätsmesseinheiten

Unified Manager berechnet die Speicherkapazität basierend auf Binäreinheiten von 1024 (2^{10}) Bytes. In ONTAP 9.10.0 und früher wurden diese Einheiten als KB, MB, GB, TB und PB angezeigt. Ab ONTAP 9.10.1 werden sie im Unified Manager als KiB, MiB, GiB, TiB und PiB angezeigt.

Die für den Durchsatz verwendeten Einheiten sind für alle Versionen von ONTAP weiterhin Kilobyte pro Sekunde (Kbps), Megabyte pro Sekunde (Mbps), Gigabyte pro Sekunde (Gbps) oder Terabyte pro Sekunde (Tbps) usw.

Kapazitätseinheit, die im Unified Manager für ONTAP 9.10.0 und früher angezeigt wird	Kapazitätseinheit, die im Unified Manager für ONTAP 9.10.1 angezeigt wird	Berechnung	Wert in Bytes
KB	KiB	1024	1024 Byte
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

Unified Manager-Funktionen zur Integritätsüberwachung

Unified Manager basiert auf einer Serverinfrastruktur, die Skalierbarkeit, Supportfähigkeit und erweiterte Überwachungs- und Benachrichtigungsfunktionen bietet. Unified Manager unterstützt die Überwachung von Systemen, auf denen ONTAP -Software ausgeführt wird.

Unified Manager umfasst die folgenden Funktionen:

- Erkennung, Überwachung und Benachrichtigungen für Systeme, auf denen ONTAP -Software installiert ist:
  - Physische Objekte: Knoten, Festplatten, Festplattenregale, SFO-Paare, Ports und Flash-Cache
  - Logische Objekte: Cluster, Storage Virtual Machines (SVMs), Aggregate, Volumes, LUNs, Namespaces, Qtrees, LIFs, Snapshot-Kopien, Junction-Pfade, NFS-Freigaben, SMB-Freigaben, Benutzer- und Gruppenkontingente, QoS-Richtliniengruppen und Initiatorgruppen
  - Protokolle: CIFS, NFS, FC, iSCSI, NVMe und FCoE
  - Speichereffizienz: SSD-Aggregate, Flash Pool-Aggregate, FabricPool -Aggregate, Deduplizierung und Komprimierung
  - Schutz: SnapMirror -Beziehungen (synchron und asynchron) und SnapVault -Beziehungen
- Anzeigen des Cluster-Erkennungs- und Überwachungsstatus
- MetroCluster über FC- und IP-Konfigurationen: Anzeigen und Überwachen der Konfiguration, Probleme und des Verbindungsstatus der Clusterkomponenten. MetroCluster -Switches und -Bridges für MetroCluster über FC-Konfigurationen
- Verbesserte Warn-, Ereignis- und Schwellenwertinfrastruktur
- LDAP, LDAPS, SAML-Authentifizierung und lokale Benutzerunterstützung
- RBAC (für einen vordefinierten Satz von Rollen)
- AutoSupport und Support-Paket
- Verbessertes Dashboard zur Anzeige von Kapazität, Verfügbarkeit, Schutz und Leistungszustand der

Umgebung

- Interoperabilität der Volume-Verschiebung, Verlauf der Volume-Verschiebung und Verlauf der Änderungen am Junction-Pfad
- Der Bereich „Auswirkungsumfang“ zeigt grafisch die Ressourcen an, die von Ereignissen wie „Einige ausgefallene Festplatten“, „MetroCluster Aggregate Mirroring Degraded“ und „MetroCluster Spare Disks Left Behind“ betroffen sind.
- Möglicher Effektbereich, der die Auswirkungen der MetroCluster -Ereignisse anzeigt
- Im Bereich „Vorgeschlagene Korrekturmaßnahmen“ werden die Maßnahmen angezeigt, die zur Behebung von Ereignissen wie „Einige ausgefallene Festplatten“, „MetroCluster Aggregate Mirroring Degraded“ und „MetroCluster Spare Disks Left Behind“ durchgeführt werden können.
- Der Bereich „Ressourcen, die betroffen sein könnten“ zeigt die Ressourcen an, die von Ereignissen wie dem Ereignis „Volume offline“, dem Ereignis „Volume eingeschränkt“ 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 Knotenstammvolumes
- Verbesserte Überwachung von Snapshot-Kopien, einschließlich der Berechnung des wiederherstellbaren Speicherplatzes und der Löschung von Snapshot-Kopien
- Anmerkungen zu Speicherobjekten
- Berichterstellung und Verwaltung von Speicherobjektinformationen wie physische und logische Kapazität, Auslastung, Platzeinsparungen, Leistung und verwandte Ereignisse
- Integration mit OnCommand Workflow Automation zur Ausführung von Workflows

  Der Storage Automation Store enthält NetApp-zertifizierte automatisierte Speicher-Workflow-Pakete, die für die Verwendung mit OnCommand Workflow Automation (WFA) entwickelt wurden. Sie können die Pakete herunterladen und sie dann in WFA importieren, um sie auszuführen. Die automatisierten Workflows sind hier verfügbar:

  "Speicherautomatisierungs-Shop"

Unified Manager-Schnittstellen zur Verwaltung der Speichersystemintegrität

Diese Abschnitte enthalten Informationen zu den beiden Benutzeroberflächen, die Active IQ Unified Manager zur Behebung von Problemen mit der Datenspeicherkapazität, -verfügbarkeit und dem Schutz bereitstellt. Die beiden Benutzeroberflächen sind die Unified Manager-Webbenutzeroberfläche und die Wartungskonsole.

Wenn Sie die Schutzfunktionen in Unified Manager verwenden möchten, müssen Sie auch OnCommand Workflow Automation (WFA) installieren und konfigurieren.

Unified Manager-Web-Benutzeroberfläche

Über die Web-Benutzeroberfläche von Unified Manager kann ein Administrator Clusterprobleme im Zusammenhang mit der Datenspeicherkapazität, -verfügbarkeit und -sicherheit überwachen und beheben.

In diesen Abschnitten werden einige allgemeine Arbeitsabläufe beschrieben, die ein Administrator befolgen kann, um Probleme mit der Speicherkapazität, der Datenverfügbarkeit oder dem Schutz zu beheben, die in der Web-Benutzeroberfläche von Unified Manager angezeigt werden.

Wartungskonsole

Mit der Wartungskonsole von Unified Manager kann ein Administrator Betriebssystemprobleme, Probleme bei Versionsaktualisierungen, Probleme beim Benutzerzugriff und Netzwerkprobleme im Zusammenhang mit dem Unified Manager-Server selbst überwachen, diagnostizieren und beheben. Wenn die Web-Benutzeroberfläche von Unified Manager nicht verfügbar ist, ist die Wartungskonsole die einzige Möglichkeit, auf Unified Manager zuzugreifen.

Sie können diese Informationen verwenden, um auf die Wartungskonsole zuzugreifen und damit Probleme im Zusammenhang mit der Funktion des Unified Manager-Servers zu lösen.

Verwalten und Überwachen der Integrität von Clustern und Clusterobjekten

Unified Manager verwendet regelmäßige API-Abfragen und eine Datenerfassungs-Engine, um Daten aus den Clustern zu erfassen. Durch das Hinzufügen von Clustern zur Unified Manager-Datenbank können Sie diese Cluster auf Verfügbarkeits- und Kapazitätsrisiken überwachen und verwalten.

Grundlegendes zur Clusterüberwachung

Sie können der Unified Manager-Datenbank Cluster hinzufügen, um Cluster auf Verfügbarkeit, Kapazität und andere Details zu überwachen, z. B. CPU-Auslastung, Schnittstellenstatistiken, freien Speicherplatz, Qtree-Auslastung und Gehäuseumgebung.

Ereignisse werden generiert, wenn der Status anormal ist oder ein vordefinierter Schwellenwert überschritten wird. Bei entsprechender Konfiguration sendet Unified Manager eine Benachrichtigung an einen angegebenen Empfänger, wenn ein Ereignis einen Alarm auslöst.

Grundlegendes zu Knotenstammvolumes

Sie können das Knotenstammvolume mit Unified Manager überwachen. Die beste Vorgehensweise besteht darin, dass das Stammvolume des Knotens über ausreichend Kapazität verfügt, um einen Ausfall des Knotens zu verhindern.

Wenn die genutzte Kapazität des Knotenstammdatenträgers 80 Prozent der Gesamtkapazität des Knotenstammdatenträgers überschreitet, wird das Ereignis „Speicherplatz des Knotenstammdatenträgers fast voll“ generiert. Sie können einen Alarm für das Ereignis konfigurieren, um eine Benachrichtigung zu erhalten. Sie können mithilfe des ONTAP System Manager oder der ONTAP CLI geeignete Maßnahmen ergreifen, um einen Ausfall des Knotens zu verhindern.

> Die Funktion zum Überwachen von Knoten-Root-Volumes ist nicht verfügbar, wenn auf Clustern ONTAP Version 9.14.1 oder höher ausgeführt wird.

Verstehen Sie Ereignisse und Schwellenwerte für Knotenstammaggregate

Sie können das Knotenstammaggregat mithilfe von Unified Manager überwachen. Die beste Vorgehensweise besteht darin, das Stammvolume im Stammaggregat dick bereitzustellen, um ein Anhalten des Knotens zu verhindern.

Standardmäßig werden für Root-Aggregate keine Kapazitäts- und Leistungsereignisse generiert. Außerdem sind die von Unified Manager verwendeten Schwellenwerte nicht auf die Knotenstammaggregate anwendbar. Nur ein Mitarbeiter des technischen Supports kann die Einstellungen für die Generierung dieser Ereignisse ändern. Wenn die Einstellungen vom technischen Supportmitarbeiter geändert werden, werden die Kapazitätsschwellenwerte auf das Knotenstammaggregat angewendet.

Sie können mithilfe des ONTAP System Manager oder der ONTAP CLI geeignete Maßnahmen ergreifen, um ein Anhalten des Knotens zu verhindern.

Die Funktion zur Überwachung von Knoten-Root-Aggregaten ist nicht verfügbar, wenn auf Clustern ONTAP Version 9.14.1 oder höher ausgeführt wird.

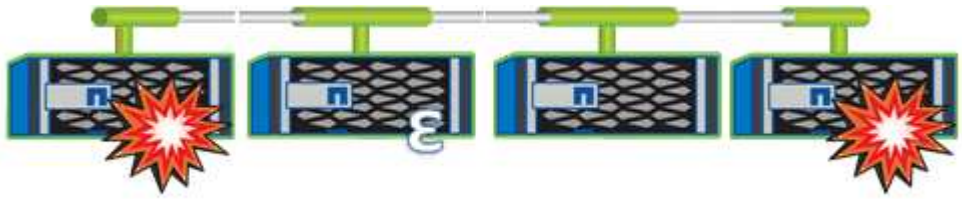
Quorum und Epsilon verstehen

Quorum und Epsilon sind wichtige Messwerte für die Gesundheit und Funktion von Clustern, die zusammen Aufschluss darüber geben, wie Cluster mit potenziellen Kommunikations- und Konnektivitätsproblemen umgehen.

Quorum ist eine Voraussetzung für einen voll funktionsfähigen Cluster. Wenn ein Cluster im Quorum ist, ist eine einfache Mehrheit der Knoten fehlerfrei und kann miteinander kommunizieren. Wenn das Quorum verloren geht, kann der Cluster keine normalen Clustervorgänge mehr durchführen. Es kann immer nur eine Knotensammlung das Quorum haben, da alle Knoten gemeinsam eine einzige Datenansicht nutzen. Wenn also zwei nicht kommunizierende Knoten die Daten auf unterschiedliche Weise ändern dürfen, ist es nicht mehr möglich, die Daten in einer einzigen Datenansicht zusammenzuführen.

Jeder Knoten im Cluster nimmt an einem Abstimmungsprotokoll teil, bei dem ein Knotenmaster gewählt wird; jeder verbleibende Knoten ist ein sekundärer Knoten. Der Masterknoten ist für die Synchronisierung von Informationen im gesamten Cluster verantwortlich. Wenn die Beschlussfähigkeit erreicht ist, wird sie durch fortlaufende Abstimmung aufrechterhalten. Wenn der Masterknoten offline geht und der Cluster noch im Quorum ist, wird von den Knoten, die online bleiben, ein neuer Master gewählt.

Da in einem Cluster mit einer geraden Anzahl von Knoten die Möglichkeit eines Gleichstands besteht, erhält ein Knoten ein zusätzliches, gebrochenes Stimmgewicht, das als Epsilon bezeichnet wird. Wenn die Konnektivität zwischen zwei gleichen Teilen eines großen Clusters ausfällt, behält die Gruppe von Knoten, die Epsilon enthält, das Quorum bei, vorausgesetzt, dass alle Knoten fehlerfrei sind. Die folgende Abbildung zeigt beispielsweise einen Cluster mit vier Knoten, in dem zwei Knoten ausgefallen sind. Da jedoch einer der überlebenden Knoten Epsilon hält, bleibt der Cluster im Quorum, auch wenn keine einfache Mehrheit gesunder 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 Offlineschalten eines Knotens kann die Fähigkeit des Clusters beeinträchtigen, im Quorum zu bleiben. Daher gibt ONTAP eine Warnmeldung aus, wenn Sie einen Vorgang versuchen, der den Cluster entweder aus

dem Quorum nimmt oder ihn einen Ausfall von einem Quorumverlust entfernt. Sie können die Quorum-Warnmeldungen deaktivieren, indem Sie den Befehl „cluster quorum-service options modify“ auf der erweiterten Berechtigungsebene verwenden.

Im Allgemeinen ist ein größerer Cluster stabiler als ein kleinerer Cluster, vorausgesetzt, die Konnektivität zwischen den Knoten des Clusters ist zuverlässig. Die Quorum-Anforderung einer einfachen Mehrheit von der Hälfte der Knoten plus Epsilon ist in einem Cluster mit 24 Knoten leichter einzuhalten als in einem Cluster mit zwei Knoten.

Ein Cluster mit zwei Knoten stellt einige einzigartige Herausforderungen hinsichtlich der Aufrechterhaltung des Quorums dar. Cluster mit zwei Knoten verwenden Cluster-HA, bei dem keiner der Knoten Epsilon hält. Stattdessen werden beide Knoten kontinuierlich abgefragt, um sicherzustellen, dass beim Ausfall eines Knotens der andere vollen Lese- und Schreibzugriff auf die Daten sowie Zugriff auf logische Schnittstellen und Verwaltungsfunktionen hat.

Anzeigen der Clusterliste und Details

Sie können die Ansicht „Integrität: Alle Cluster“ verwenden, um Ihren Clusterbestand anzuzeigen. In der Ansicht „Kapazität: Alle Cluster“ können Sie zusammengefasste Informationen zur Speicherkapazität und -auslastung in allen Clustern anzeigen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können auf der Seite „Cluster-/Integritätsdetails“ auch Details zu einzelnen Clustern anzeigen, z. B. Cluster-Integrität, Kapazität, Konfiguration, LIFs, Knoten und Datenträger in diesem Cluster.

Die Details in der Ansicht „Integrität: Alle Cluster“, in der Ansicht „Kapazität: Alle Cluster“ und auf der Seite „Cluster-/Integritätsdetails“ helfen Ihnen bei der Planung Ihres Speichers. Bevor Sie beispielsweise ein neues Aggregat bereitstellen, können Sie in der Ansicht „Integrität: Alle Cluster“ einen bestimmten Cluster auswählen und Kapazitätsdetails abrufen, um zu ermitteln, ob der Cluster über den erforderlichen Speicherplatz verfügt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Cluster**.
2. Wählen Sie im Menü „Ansicht“ die Ansicht „**Integrität: Alle Cluster**“, um Integritätsinformationen anzuzeigen, oder die Ansicht „**Kapazität: Alle Cluster**“, um Details zur Speicherkapazität und -auslastung in allen Clustern anzuzeigen.
3. Klicken Sie auf den Namen eines Clusters, um auf der Detailseite **Cluster/Integrität** alle Details des Clusters anzuzeigen.

Verwandte Informationen

- "Cluster-/Integritätsdetailseite"
- "Leistung: Ansicht „Alle Cluster“"
- "Überwachung von MetroCluster -Konfigurationen"
- "Sicherheitsstatus für Cluster und Storage-VMs anzeigen"
- "Welche Sicherheitskriterien werden bewertet"

Überprüfen Sie den Zustand von Clustern in einer MetroCluster -Konfiguration

Sie können Active IQ Unified Manager (Unified Manager) verwenden, um die Betriebsintegrität von Clustern und deren Komponenten in MetroCluster over FC- und MetroCluster over IP-Konfigurationen zu überprüfen. Wenn die Cluster an einem von Unified Manager erkannten Leistungsereignis beteiligt waren, können Sie anhand des Integritätsstatus feststellen, ob ein Hardware- oder Softwareproblem zu dem Ereignis beigetragen hat.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen ein Leistungsereignis für eine MetroCluster -Konfiguration analysiert und den Namen des betroffenen Clusters erhalten haben.
- Beide Cluster in der MetroCluster -Konfiguration über FC und IP müssen von derselben Instanz von Unified Manager überwacht werden.

Bestimmen Sie die Clusterintegrität in der MetroCluster -über-FC-Konfiguration

Befolgen Sie diese Schritte, um die Clusterintegrität in einer MetroCluster über-FC-Konfiguration zu bestimmen.

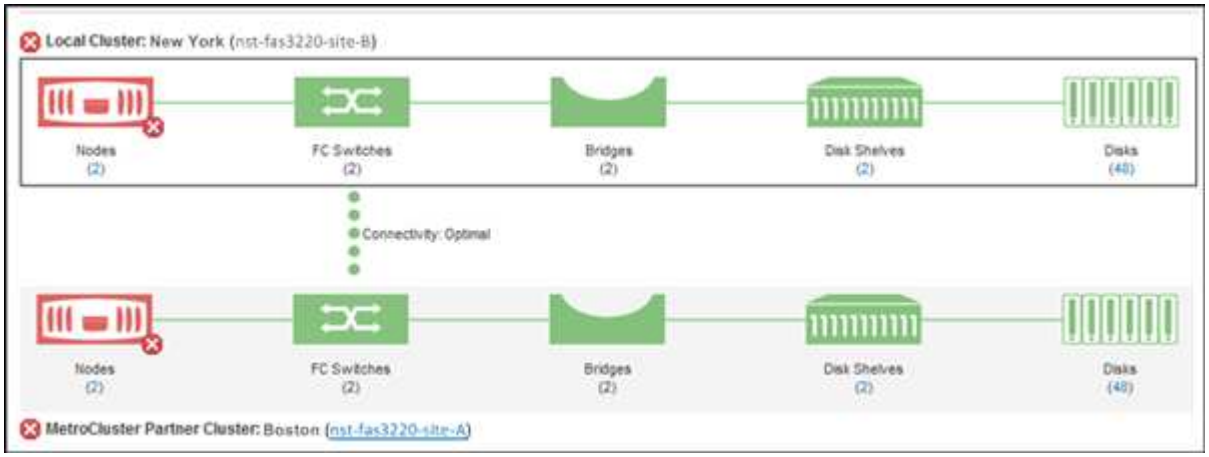
Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**, um die Eventliste anzuzeigen.
2. Wählen Sie im Filterbereich alle MetroCluster -Filter unter der Kategorie **Quelltyp** aus. Sie sehen alle in Ihrer Umgebung ausgelösten Ereignisse für alle MetroCluster -Konfigurationen.
3. Klicken Sie neben einem MetroCluster -Ereignis auf den Namen des Clusters.

> Wenn keine MetroCluster -Ereignisse angezeigt werden, können Sie mithilfe der Suchleiste nach dem Namen des Clusters suchen, der an dem Ereignis beteiligt ist, das mit Ihrer MetroCluster über-FC-Konfiguration zusammenhängt.

Die Ansicht „Integrität: Alle Cluster“ wird mit ausführlichen Informationen zum Ereignis angezeigt.

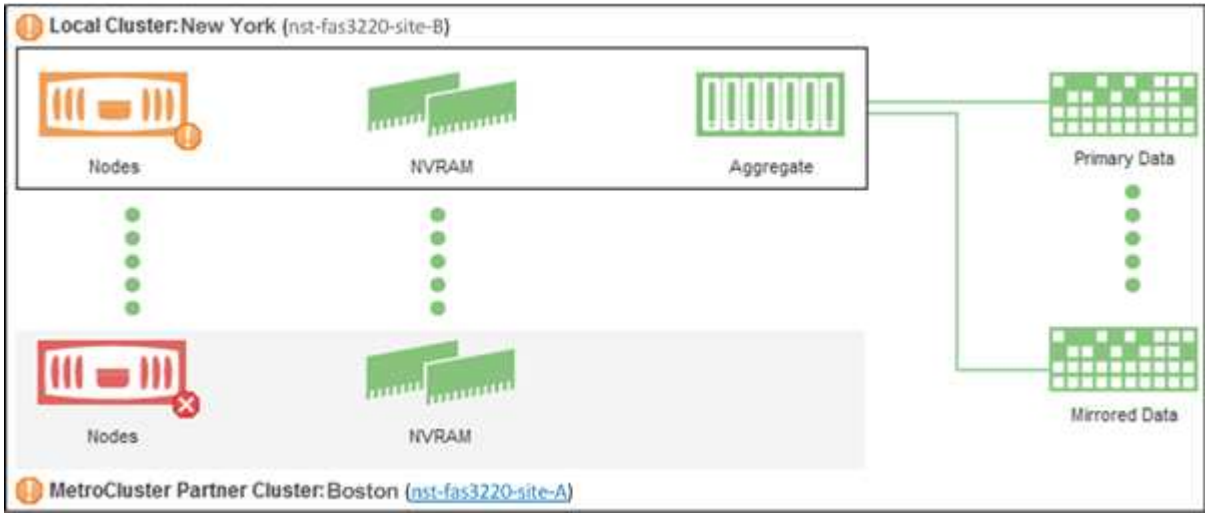
4. Wählen Sie die Registerkarte * MetroCluster -Konnektivität* aus, um den Zustand der Verbindung zwischen dem ausgewählten Cluster und seinem Partnercluster anzuzeigen.



In diesem Beispiel werden die Namen und Komponenten des lokalen Clusters und seines Partnerclusters angezeigt. Ein gelbes oder rotes Symbol weist auf ein Integritätsereignis für die hervorgehobene Komponente hin. Das Konnektivitätssymbol stellt die Verbindung zwischen den Clustern dar. Sie können mit dem Mauszeiger auf ein Symbol zeigen, um Ereignisinformationen anzuzeigen, oder auf das Symbol klicken, um die Ereignisse anzuzeigen. Ein Gesundheitsproblem auf einem der Cluster könnte zu dem Leistungsereignis beigetragen haben.

Unified Manager überwacht die NVRAM Komponente der Verbindung zwischen den Clustern. Wenn das FC-Switch-Symbol auf dem lokalen oder Partnercluster oder das Konnektivitätssymbol rot ist, könnte ein Verbindungsintegritätsproblem das Leistungsereignis verursacht haben.

5. Wählen Sie die Registerkarte * MetroCluster -Replikation*.



Wenn in diesem Beispiel das NVRAM -Symbol auf dem lokalen oder Partnercluster gelb oder rot ist, könnte ein Integritätsproblem mit dem NVRAM das Leistungsereignis verursacht haben. Wenn auf der Seite keine roten oder gelben Symbole angezeigt werden, kann das Leistungsereignis durch ein Leistungsproblem im Partnercluster verursacht worden sein.

Bestimmen Sie die Clusterintegrität in der MetroCluster over IP-Konfiguration

Befolgen Sie diese Schritte, um die Clusterintegrität in einer MetroCluster over-IP-Konfiguration zu bestimmen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**, um die Eventliste anzuzeigen.
2. Wählen Sie im Filterbereich unter der Kategorie **Quellentyp** die `MetroCluster Relationship` Filter. Sie sehen alle in Ihrer Umgebung ausgelösten Ereignisse für alle MetroCluster -Konfigurationen.

> Wenn Sie die gemeldeten MetroCluster -Ereignisse nicht sehen können, können Sie mithilfe der Suchleiste nach dem Namen des Clusters suchen, der an dem Ereignis beteiligt ist, das mit Ihrer MetroCluster over-IP-Konfiguration zusammenhängt.

3. Klicken Sie neben dem entsprechenden MetroCluster -Ereignis auf den Namen des Clusters. Die Seite „Cluster“ wird mit den Details dieses Clusters angezeigt. Informationen zur Feststellung gesundheitlicher Probleme finden Sie unter"Überwachen Sie Konnektivitätsprobleme in der MetroCluster -over-IP -Konfiguration" .

Anzeigen des Integritäts- und Kapazitätsstatus aller SAN-Array-Cluster

Sie können die Cluster-Inventarseiten verwenden, um den Integritäts- und Kapazitätsstatus Ihrer All-SAN-Array-Cluster anzuzeigen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können Übersichtsinformationen für alle SAN-Array-Cluster in der Ansicht „Integrität: Alle Cluster“ und in der Ansicht „Kapazität: Alle Cluster“ anzeigen. Darüber hinaus können Sie Details auf der Seite „Cluster-/Integritätsdetails“ anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Cluster**.
2. Stellen Sie sicher, dass die Spalte „Persönlichkeit“ in der Ansicht **Gesundheit: Alle Cluster** angezeigt wird, oder fügen Sie sie mithilfe des Steuerelements **Einblenden/Ausblenden** hinzu.

   In dieser Spalte wird „All SAN Array“ für Ihre All SAN Array-Cluster angezeigt.
3. Überprüfen Sie die Informationen.
4. Um Informationen zur Speicherkapazität in diesen Clustern anzuzeigen, wählen Sie die Ansicht „Kapazität: Alle Cluster“ aus.
5. Um detaillierte Informationen zum Zustand und zur Speicherkapazität dieser Cluster anzuzeigen, klicken Sie auf den Namen eines All-SAN-Array-Clusters.

   Zeigen Sie die Details auf den Registerkarten „Integrität“, „Kapazität“ und „Knoten“ auf der Seite „Cluster-/Integritätsdetails“ an.

Anzeigen der Knotenliste und Details

Sie können die Ansicht „Integrität: Alle Knoten“ verwenden, um die Liste der Knoten in Ihren Clustern anzuzeigen. Auf der Seite „Cluster-/Integritätsdetails“ können Sie ausführliche Informationen zu Knoten anzeigen, die Teil des überwachten Clusters sind.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können Details wie den Knotenstatus, den Cluster, der den Knoten enthält, Details zur Gesamtkapazität (verwendet und gesamt) und Details zur Rohkapazität (verwendbar, frei und gesamt) anzeigen. Sie können auch Informationen zu HA-Paaren, Festplatten-Shelves und Ports erhalten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Knoten**.
2. Klicken Sie in der Ansicht **Integrität: Alle Knoten** auf den Knoten, dessen Details Sie anzeigen möchten.

   Die detaillierten Informationen zum ausgewählten Knoten werden auf der Seite „Cluster-/Integritätsdetails“ angezeigt. Der linke Bereich zeigt die Liste der HA-Paare. Standardmäßig sind die HA-Details geöffnet, in denen Details zum HA-Status und Ereignisse im Zusammenhang mit dem ausgewählten HA-Paar angezeigt werden.

3. Um weitere Details zum Knoten anzuzeigen, führen Sie die entsprechende Aktion aus:

Zum Anzeigen…	Klicken…
Details zu den Disk Shelfs	**Festplattenregale**.
Hafenbezogene Informationen	**Anschlüsse**.

Weitere Informationen finden Sie unter:

- "Leistung: Alle Knoten anzeigen"
- "Anzeigen von Knoten- und aggregierten verfügbaren IOPS-Werten"
- "Anzeigen der verwendeten Knoten- und Gesamtleistungskapazitätswerte"

Erstellen Sie einen Hardware-Inventarbericht für die Vertragsverlängerung

Sie können einen Bericht erstellen, der eine vollständige Liste der Cluster- und Knoteninformationen enthält, z. B. Hardwaremodellnummern und Seriennummern, Datenträgertypen und -anzahl, installierte Lizenzen und mehr. Dieser Bericht ist hilfreich für die Vertragsverlängerung innerhalb sicherer Sites („dunkler“ Sites), die nicht mit der NetAppActive IQ-Plattform verbunden sind.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Knoten**.
2. Wechseln Sie zur Ansicht **Integrität: Alle Knoten** oder zur Ansicht **Leistung: Alle Knoten**.
3. Wählen Sie **Berichte** > ***** > Hardwareinventarbericht*.

   Der Hardwareinventarbericht wird als CSV-Datei mit vollständigen Informationen zum aktuellen Datum heruntergeladen.

4. Geben Sie diese Informationen an Ihren NetApp Support-Kontakt weiter, um den Vertrag zu verlängern.

Anzeigen der Storage-VM-Liste und Details

In der Ansicht „Integrität: Alle Storage-VMs“ können Sie Ihren Bestand an Storage-VMs (SVMs) überwachen. Auf der Seite „Storage VM / Health Details“ können Sie ausführliche Informationen zu den überwachten SVMs anzeigen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können SVM-Details wie Kapazität, Effizienz und Konfiguration einer SVM anzeigen. Sie können auch Informationen zu den zugehörigen Geräten und zugehörigen Warnungen für diese SVM anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Speicher-VMs**.
2. Wählen Sie eine der folgenden Möglichkeiten, um die SVM-Details anzuzeigen:
   - Um Informationen zum Zustand aller SVMs in allen Clustern anzuzeigen, wählen Sie im Menü „Ansicht“ die Option „Zustand: Alle Storage-VMs anzeigen“.
   - Klicken Sie auf den Namen der Storage-VM, um die vollständigen Details anzuzeigen.

     Sie können die vollständigen Details auch anzeigen, indem Sie im Dialogfeld mit den minimalen Details auf **Details anzeigen** klicken.
3. Zeigen Sie die mit der SVM verknüpften Objekte an, indem Sie im Dialogfeld mit den minimalen Details auf **Verwandte anzeigen** klicken.

Verwandte Informationen

- "Speicher-VM: Seite mit Integritätsdetails"
- "Leistung: Alle Storage-VMs anzeigen"
- "Sicherheit: Anti-Ransomware-Ansicht"
- "Sicherheitsstatus für Cluster und Storage-VMs anzeigen"
- "Beziehung: Ansicht „Alle Beziehungen““

Gesamtliste und Details anzeigen

In der Ansicht „Integrität: Alle Aggregate“ können Sie Ihren Aggregatbestand überwachen. Mit der Ansicht „Kapazität: Alle Aggregate“ können Sie Informationen zur Kapazität und Auslastung von Aggregaten in allen Clustern anzeigen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können Details wie Gesamtkapazität und -konfiguration sowie Datenträgerinformationen auf der Seite „Aggregat-/Integritätsdetails“ anzeigen. Sie können diese Angaben verwenden, bevor Sie bei Bedarf die Schwellenwerteinstellungen konfigurieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.
2. Wählen Sie eine der folgenden Möglichkeiten, um die aggregierten Details anzuzeigen:
   - Um Informationen zum Zustand aller Aggregate in allen Clustern anzuzeigen, wählen Sie im Menü „Ansicht“ die Option „Zustand: Alle Aggregate anzeigen“ aus.
   - Um Informationen zur Kapazität und Auslastung aller Aggregate in allen Clustern anzuzeigen, wählen Sie im Menü „Ansicht“ die Option „Kapazität: Alle Aggregate anzeigen“ aus.
   - Klicken Sie auf den Aggregatnamen, um die vollständigen Details anzuzeigen.

     Sie können die vollständigen Details auch anzeigen, indem Sie im Dialogfeld mit den minimalen Details auf **Details anzeigen** klicken.
3. Zeigen Sie die mit dem Aggregat verknüpften Objekte an, indem Sie im Dialogfeld mit den minimalen Details auf **Verwandte anzeigen** klicken.

Verwandte Informationen

- "Seite mit Aggregat-/Gesundheitsdetails"
- "Leistung: Alle Aggregate anzeigen"
- "Anpassen aggregierter Kapazitätsberichte"

Informationen zur FabricPool -Kapazität anzeigen

Sie können FabricPool Kapazitätsinformationen für Cluster, Aggregate und Volumes auf den Bestands- und Detailseiten „Kapazität und Leistung“ für diese Objekte anzeigen. Auf diesen Seiten werden auch FabricPool Spiegelinformationen angezeigt, wenn eine Spiegelebene konfiguriert wurde.

Auf diesen Seiten werden Informationen wie die verfügbare Kapazität auf der lokalen Leistungsebene und auf der Cloud-Ebene angezeigt, wie viel Kapazität in beiden Ebenen verwendet wird, welche Aggregate an eine Cloud-Ebene angehängt sind und welche Volumes die FabricPool -Funktionen implementieren, indem sie bestimmte Informationen in die Cloud-Ebene verschieben.

Wenn eine Cloud-Ebene auf einen anderen Cloud-Anbieter gespiegelt wird (die „Spiegelebene“), werden beide Cloud-Ebenen auf der Seite „Aggregat-/Integritätsdetails“ angezeigt.

Schritte

1. Führen Sie einen der folgenden Schritte aus:

So zeigen Sie Kapazitätsinformationen an für …	Machen Sie Folgendes…
Cluster	a. Klicken Sie in der Ansicht „Kapazität: Alle Cluster“ auf einen Cluster. b. Klicken Sie auf der Seite „Cluster-/Integritätsdetails“ auf die Registerkarte **Konfiguration**. Die Anzeige zeigt die Namen aller Cloud-Ebenen, mit denen dieser Cluster verbunden ist.

So zeigen Sie Kapazitätsinformationen an für …	Machen Sie Folgendes…
Aggregate	a. Klicken Sie in der Ansicht „Kapazität: Alle Aggregate“ auf ein Aggregat, bei dem im Feld „Typ“ „SSD (FabricPool)“ oder „HDD (FabricPool)“ angezeigt wird. b. Klicken Sie auf der Seite „Aggregat-/Integritätsdetails“ auf die Registerkarte **Kapazität**. Die Anzeige zeigt die gesamte im Cloud-Tier genutzte Kapazität. c. Klicken Sie auf die Registerkarte **Datenträgerinformationen**. Auf der Anzeige werden der Name der Cloud-Ebene und die genutzte Kapazität angezeigt. d. Klicken Sie auf die Registerkarte **Konfiguration**. Auf der Anzeige werden der Name der Cloud-Ebene und weitere detaillierte Informationen zur Cloud-Ebene angezeigt.
Bände	a. Klicken Sie in der Ansicht „Kapazität: Alle Volumes“ auf ein Volume, bei dem im Feld „Tiering-Richtlinie“ ein Richtlinienname angezeigt wird. b. Klicken Sie auf der Seite „Volume-/Integritätsdetails“ auf die Registerkarte **Konfiguration**. Auf der Anzeige wird der Name der dem Volume zugewiesenen FabricPool -Tiering -Richtlinie angezeigt.

2. Auf der Seite **Workload-Analyse** können Sie im Bereich **Kapazitätstrend** „Cloud-Tier-Ansicht“ auswählen, um die im letzten Monat im lokalen Performance-Tier und im Cloud-Tier genutzte Kapazität anzuzeigen.

Weitere Informationen zu FabricPool -Aggregaten finden Sie unter "Übersicht über Datenträger und Aggregate" .

Anzeigen von Speicherpooldetails

Sie können die Details des Speicherpools anzeigen, um den Zustand des Speicherpools, den gesamten und verfügbaren Cache sowie die verwendeten und verfügbaren Zuweisungen zu überwachen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.
2. Klicken Sie auf einen Aggregatnamen.

   Die Details des ausgewählten Aggregats werden angezeigt.

3. Klicken Sie auf die Registerkarte **Datenträgerinformationen**.

   Es werden detaillierte Festplatteninformationen angezeigt.

   Die Cache-Tabelle wird nur angezeigt, wenn das ausgewählte Aggregat einen Speicherpool verwendet.

4. Bewegen Sie in der Cache-Tabelle den Zeiger über den Namen des gewünschten Speicherpools.

   Die Details des Speicherpools werden angezeigt.

Anzeigen der Volumeliste und Details

In der Ansicht „Health: All Volumes“ können Sie Ihren Volume-Bestand überwachen. Mit der Ansicht „Kapazität: Alle Volumes“ können Sie Informationen zur Kapazität und Auslastung von Volumes in einem Cluster anzeigen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können auch die Seite „Volume-/Integritätsdetails“ verwenden, um ausführliche Informationen zu den überwachten Volumes anzuzeigen, einschließlich der Kapazität, Effizienz, Konfiguration und des Schutzes der Volumes. Sie können auch Informationen zu den zugehörigen Geräten und zugehörigen Warnungen für ein bestimmtes Volume anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie eine der folgenden Möglichkeiten, um die Volumedetails anzuzeigen:
   - Um ausführliche Informationen zum Zustand der Volumes in einem Cluster anzuzeigen, wählen Sie im Menü „Ansicht“ die Option „Integrität: Alle Volumes anzeigen“ aus.
   - Um detaillierte Informationen zur Kapazität und Auslastung von Volumes in einem Cluster anzuzeigen, wählen Sie im Menü „Ansicht“ die Option „Kapazität: Alle Volumes anzeigen“.
   - Klicken Sie auf den Datenträgernamen, um die vollständigen Details anzuzeigen.

     Sie können die vollständigen Details auch anzeigen, indem Sie im Dialogfeld mit den minimalen Details auf **Details anzeigen** klicken.

3. **Optional:** Zeigen Sie die mit dem Datenträger verknüpften Objekte an, indem Sie im Dialogfeld mit den minimalen Details auf **Verwandte anzeigen** klicken.

Verwandte Informationen

- "Band: Seite mit Gesundheitsdetails"
- "Leistung: Ansicht „Alle Volumes“"
- "Sicherheit: Anti-Ransomware-Ansicht"
- "Anzeigen von Volume-Schutzbeziehungen"
- "Erstellen eines Berichts zum Anzeigen von Diagrammen zur verfügbaren Datenträgerkapazität"

Details zu NFS-Freigaben anzeigen

Sie können Details zu allen NFS-Freigaben anzeigen, z. B. deren Status, den mit dem Volume verknüpften Pfad (FlexGroup Volumes oder FlexVol -Volumes), die Zugriffsebenen der Clients auf die NFS-Freigaben und die für die exportierten Volumes definierte Exportrichtlinie. Verwenden Sie die Ansicht „Integrität: Alle NFS-Freigaben“, um alle NFS-Freigaben auf allen überwachten Clustern anzuzeigen, und verwenden Sie die Seite „Speicher-VM/Integritätsdetails“, um alle NFS-Freigaben auf einer bestimmten virtuellen Speichermaschine (SVM) anzuzeigen.

Bevor Sie beginnen

- Die NFS-Lizenz muss auf dem Cluster aktiviert sein.
- Netzwerkschnittstellen, die die NFS-Freigaben bedienen, müssen konfiguriert werden.
- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritt

1. Führen Sie im linken Navigationsbereich die folgenden Schritte aus, je nachdem, ob Sie alle NFS-Freigaben oder nur die NFS-Freigaben für eine bestimmte SVM anzeigen möchten.

Zu…	Befolgen Sie diese Schritte…
Alle NFS-Freigaben anzeigen	Klicken Sie auf **Speicher** > **NFS-Freigaben**
NFS-Freigaben für einzelne SVM anzeigen	a. Klicken Sie auf **Speicher** > **Speicher-VMs** b. Klicken Sie auf die SVM, für die Sie die Details der NFS-Freigaben anzeigen möchten. c. Klicken Sie auf der Seite „Storage VM / Health Details“ auf die Registerkarte **NFS Shares**.

Weitere Informationen finden Sie unter"Bereitstellen von Dateifreigabevolumes" Und"Bereitstellung von CIFS- und NFS-Dateifreigaben mithilfe von APIs" .

Details zu SMB/CIFS-Freigaben anzeigen

Sie können Details zu allen SMB/CIFS-Freigaben anzeigen, z. B. Freigabename, Verbindungspfad, enthaltene Objekte, Sicherheitseinstellungen und für die Freigabe definierte Exportrichtlinien. Verwenden Sie die Ansicht „Integrität: Alle SMB-Freigaben“, um alle SMB-Freigaben auf allen überwachten Clustern anzuzeigen, und verwenden Sie die Seite „Speicher-VM/Integritätsdetails“, um alle SMB-Freigaben auf einer bestimmten

virtuellen Speichermaschine (SVM) anzuzeigen.

Bevor Sie beginnen

- Die CIFS-Lizenz muss auf dem Cluster aktiviert sein.
- Netzwerkschnittstellen, die die SMB/CIFS-Freigaben bedienen, müssen konfiguriert werden.
- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Freigaben in Ordnern werden nicht angezeigt.

Schritt

1. Führen Sie im linken Navigationsbereich die folgenden Schritte aus, je nachdem, ob Sie alle SMB/CIFS-Freigaben oder nur die Freigaben für eine bestimmte SVM anzeigen möchten.

Zu…	Befolgen Sie diese Schritte…
Alle SMB/CIFS-Freigaben anzeigen	Klicken Sie auf **Speicher** > **SMB-Freigaben**
SMB/CIFS-Freigaben für einzelne SVM anzeigen	a. Klicken Sie auf **Speicher** > **Speicher-VMs** b. Klicken Sie auf die SVM, für die Sie die SMB/CIFS-Freigabedetails anzeigen möchten. c. Klicken Sie auf der Seite „Storage VM / Health Details“ auf die Registerkarte **SMB Shares**.

Weitere Informationen finden Sie unter "Bereitstellung von CIFS- und NFS-Dateifreigaben mithilfe von APIs".

Liste der Snapshot-Kopien anzeigen

Sie können die Liste der Snapshot-Kopien für ein ausgewähltes Volume anzeigen. Mithilfe der Liste der Snapshot-Kopien können Sie die Menge an Speicherplatz berechnen, die zurückgewonnen werden kann, wenn eine oder mehrere Snapshot-Kopien gelöscht werden, und Sie können die Snapshot-Kopien bei Bedarf löschen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Das Volume mit den Snapshot-Kopien muss online sein.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie in der Ansicht **Health: All Volumes** das Volume aus, das die Snapshot-Kopien enthält, die Sie anzeigen möchten.
3. Klicken Sie auf der Detailseite **Volume/Integrität** auf die Registerkarte **Kapazität**.
4. Klicken Sie im Bereich **Details** der Registerkarte **Kapazität** im Abschnitt „Weitere Details“ auf den Link neben **Snapshot-Kopien**.

   Die Anzahl der Snapshot-Kopien ist ein Link, der die Liste der Snapshot-Kopien anzeigt.

Verwandte Informationen

"Seite „Zustand/Volumes“"

Löschen von Snapshot-Kopien

Sie können eine Snapshot-Kopie löschen, um Speicherplatz zu sparen oder freizugeben, oder Sie können die Snapshot-Kopie löschen, wenn sie nicht mehr benötigt wird.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Das Volume muss online sein.

Um eine Snapshot-Kopie zu löschen, die belegt oder gesperrt ist, müssen Sie die Snapshot-Kopie aus der Anwendung freigegeben haben, 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 -Volumes verwendet wird und den Status anzeigt `Busy` und Anwendungsabhängigkeit als `Busy, Vclone` im übergeordneten Volume.

- Sie können keine gesperrte Snapshot-Kopie löschen, die in einer SnapMirror -Beziehung verwendet wird.

  Die Snapshot-Kopie ist gesperrt und wird für das nächste Update benötigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie in der Ansicht **Health: All Volumes** das Volume aus, das die Snapshot-Kopien enthält, die Sie anzeigen möchten.

   Die Liste der Snapshot-Kopien wird angezeigt.

3. Klicken Sie auf der Detailseite **Volume/Integrität** auf die Registerkarte **Kapazität**.
4. Klicken Sie im Bereich **Details** der Registerkarte **Kapazität** im Abschnitt „Weitere Details“ auf den Link neben **Snapshot-Kopien**.

   Die Anzahl der Snapshot-Kopien ist ein Link, der die Liste der Snapshot-Kopien anzeigt.

5. Wählen Sie in der Ansicht **Snapshot-Kopien** die Snapshot-Kopien aus, die Sie löschen möchten, und klicken Sie dann auf **Ausgewählte löschen**.

Berechnen Sie den wiederherstellbaren Speicherplatz für Snapshot-Kopien

Sie können die Menge an Speicherplatz berechnen, die zurückgewonnen werden kann, wenn eine oder mehrere Snapshot-Kopien gelöscht werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

- Das Volume muss online sein.
- Das Volume muss ein FlexVol volume sein; diese Funktion wird bei FlexGroup -Volumes nicht unterstützt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie in der Ansicht **Health: All Volumes** das Volume aus, das die Snapshot-Kopien enthält, die Sie anzeigen möchten.

   Die Liste der Snapshot-Kopien wird angezeigt.

3. Klicken Sie auf der Detailseite **Volume/Integrität** auf die Registerkarte **Kapazität**.
4. Klicken Sie im Bereich **Details** der Registerkarte **Kapazität** im Abschnitt „Weitere Details“ auf den Link neben **Snapshot-Kopien**.

   Die Anzahl der Snapshot-Kopien ist ein Link, der die Liste der Snapshot-Kopien anzeigt.

5. Wählen Sie in der Ansicht **Snapshot-Kopien** die Snapshot-Kopien aus, für die Sie den zurückgewinnbaren Speicherplatz berechnen möchten.
6. Klicken Sie auf **Berechnen**.

   Der wiederherstellbare Speicherplatz (in Prozent und KB, MB, GB usw.) auf dem Volume wird angezeigt.

7. Um den wiederherstellbaren Speicherplatz neu zu berechnen, wählen Sie die erforderlichen Snapshot-Kopien aus und klicken Sie auf **Neu berechnen**.

Beschreibung der Clusterobjektfenster und Dialogfelder

Sie können alle Ihre Cluster und Clusterobjekte auf der jeweiligen Speicherobjektseite anzeigen. Sie können die Details auch auf der entsprechenden Detailseite des Speicherobjekts anzeigen. Sie können die Benutzeroberfläche des System Managers jetzt aus den folgenden Abschnitten SPEICHER und SCHUTZ des INVENTARS starten.

- Seiten „Cluster-Inventar“, „Cluster-Integrität“ und „Cluster-Leistung“
- Seiten „Aggregatinventar“, „Aggregatzustand“ und „Aggregatleistung“
- Seiten „Volume-Inventar“, „Volume-Zustand“ und „Volume-Leistung“
- Seiten „Knoteninventar“ und „Knotenleistung“
- Seiten „StorageVM-Inventar“, „StorageVM-Integrität“ und „StorageVM-Leistung“
- Schutzbeziehungsseiten

Allgemeine Unified Manager-Integritätsworkflows und -Aufgaben

Zu den allgemeinen administrativen Arbeitsabläufen und Aufgaben im Zusammenhang mit Unified Manager gehören die Auswahl der zu überwachenden Speichercluster, die Diagnose von Bedingungen, die sich negativ auf die Datenverfügbarkeit, -kapazität und -sicherheit auswirken, die Wiederherstellung verlorener Daten, die Konfiguration und Verwaltung von Volumes sowie das Bündeln und Senden von Diagnosedaten an den

technischen Support (falls erforderlich).

Mit Unified Manager können Speicheradministratoren ein Dashboard anzeigen, die Gesamtkapazität, Verfügbarkeit und den Schutzzustand der verwalteten Speichercluster beurteilen und dann eventuell auftretende spezifische Probleme schnell identifizieren, lokalisieren, diagnostizieren und zur Lösung zuweisen.

Die wichtigsten Probleme im Zusammenhang mit einem Cluster, einer Storage Virtual Machine (SVM), einem Volume oder einem FlexGroup Volume, die sich auf die Speicherkapazität oder Datenverfügbarkeit Ihrer verwalteten Speicherobjekte auswirken, werden in den Systemzustandsdiagrammen und Ereignissen auf der Dashboard-Seite angezeigt. Wenn kritische Probleme erkannt werden, bietet diese Seite Links zur Unterstützung entsprechender Workflows zur Fehlerbehebung.

Unified Manager kann auch in Workflows integriert werden, die zugehörige Verwaltungstools enthalten – wie etwa OnCommand Workflow Automation (WFA) –, um die direkte Konfiguration von Speicherressourcen zu unterstützen.

In diesem Dokument werden allgemeine Arbeitsabläufe im Zusammenhang mit den folgenden Verwaltungsaufgaben beschrieben:

- Diagnose und Verwaltung von Verfügbarkeitsproblemen

  Wenn Hardwarefehler oder Konfigurationsprobleme bei Speicherressourcen dazu führen, dass Datenverfügbarkeitsereignisse auf der Dashboard-Seite angezeigt werden, können Speicheradministratoren den eingebetteten Links folgen, um Konnektivitätsinformationen zur betroffenen Speicherressource anzuzeigen, Hinweise zur Fehlerbehebung zu erhalten und die Problemlösung anderen Administratoren zuzuweisen.

- Konfigurieren und Überwachen von Leistungsvorfällen

  Der Administrator kann die Leistung der überwachten Speichersystemressourcen überwachen und verwalten. Siehe die"Einführung in die Leistungsüberwachung von Active IQ Unified Manager" für weitere Informationen.

- Diagnostizieren und Verwalten von Volume-Kapazitätsproblemen

  Wenn auf der Dashboard-Seite Probleme mit der Speicherkapazität des Volumes angezeigt werden, können Speicheradministratoren den eingebetteten Links folgen, um die aktuellen und historischen Trends in Bezug auf die Speicherkapazität des betroffenen Volumes anzuzeigen, Hinweise zur Fehlerbehebung zu erhalten und die Problemlösung anderen Administratoren zuzuweisen.

- Konfigurieren, Überwachen und Diagnostizieren von Problemen mit Schutzbeziehungen

  Nach dem Erstellen und Konfigurieren von Schutzbeziehungen können Speicheradministratoren die potenziellen Probleme im Zusammenhang mit Schutzbeziehungen, den aktuellen Status der Schutzbeziehungen, die aktuellen und historischen Informationen zum Erfolg von Schutzaufträgen zu den betroffenen Beziehungen sowie Hinweise zur Fehlerbehebung anzeigen. Siehe die"Erstellen, Überwachen und Beheben von Problemen mit Schutzbeziehungen" für weitere Informationen.

- Erstellen von Sicherungsdateien und Wiederherstellen von Daten aus Sicherungsdateien.
- Zuordnen von Speicherobjekten zu Anmerkungen

  Durch die Verknüpfung von Speicherobjekten mit Anmerkungen können Speicheradministratoren die mit den Speicherobjekten verbundenen Ereignisse filtern und anzeigen. Dadurch können sie die mit den Ereignissen verbundenen Probleme priorisieren und lösen.

- Verwenden Sie REST-APIs, um Ihre Cluster zu verwalten, indem Sie die von Unified Manager erfassten Informationen zu Integrität, Kapazität und Leistung anzeigen. Sehen"Erste Schritte mit Active IQ Unified Manager REST-APIs" für weitere Informationen.
- Senden eines Support-Pakets an den technischen Support

  Speicheradministratoren können über die Wartungskonsole ein Supportpaket abrufen und an den technischen Support senden. Supportpakete müssen an den technischen Support gesendet werden, wenn das Problem eine detailliertere Diagnose und Fehlerbehebung erfordert, als eine AutoSupport -Nachricht bietet.

Überwachen und Beheben von Problemen mit der Datenverfügbarkeit

Unified Manager überwacht die Zuverlässigkeit, mit der autorisierte Benutzer auf Ihre gespeicherten Daten zugreifen können, weist Sie auf Bedingungen hin, die diesen Zugriff blockieren oder behindern, und ermöglicht Ihnen, diese Bedingungen zu diagnostizieren und ihre Lösung zuzuweisen und zu verfolgen.

Die Themen zum Verfügbarkeits-Workflow in diesem Abschnitt beschreiben Beispiele dafür, wie ein Speicheradministrator die Unified Manager-Web-Benutzeroberfläche verwenden kann, um Hardware- und Softwarezustände zu erkennen, zu diagnostizieren und zur Behebung zuzuweisen, die sich negativ auf die Datenverfügbarkeit auswirken.

Suchen und beheben Sie Verbindungsausfälle bei Speicher-Failovern

Dieser Workflow bietet ein Beispiel dafür, wie Sie nach ausgefallenen Speicher-Failover-Verbindungsverbindungen suchen, diese auswerten und beheben können. In diesem Szenario sind Sie ein Administrator, der Unified Manager verwendet, um nach Speicher-Failover-Risiken zu suchen, bevor Sie ein ONTAP -Versionsupgrade auf Ihren Knoten starten.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn die Speicher-Failover-Verbindungen zwischen HA-Paarknoten während eines unterbrechungsfreien Upgradeversuchs fehlschlagen, schlägt das Upgrade fehl. Daher ist es üblich, dass der Administrator vor Beginn eines Upgrades die Zuverlässigkeit des Speicher-Failovers auf den für das Upgrade vorgesehenen Clusterknoten überwacht und bestätigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.
2. Wählen Sie auf der Inventarseite **Event Management** die Option **Active Availability-Ereignisse** aus.
3. Klicken Sie oben in der Spalte **Name** der Inventarseite **Event Management** auf und geben Sie ein `*failover` in das Textfeld, um die Anzeige des Ereignisses auf Speicherfailover-bezogene Ereignisse zu beschränken.

   Alle vergangenen Ereignisse im Zusammenhang mit Speicher-Failover-Bedingungen werden angezeigt.

   In diesem Szenario zeigt der Unified Manager im Abschnitt „Verfügbarkeitsvorfälle“ das Ereignis „Storage Failover Interconnect One or More Links Down“ an.

4. Wenn auf der Inventarseite **Ereignisverwaltung** ein oder mehrere Ereignisse im Zusammenhang mit dem Speicherfailover angezeigt werden, führen Sie die folgenden Schritte aus:

   a. Klicken Sie auf den Link zum Ereignistitel, um die Ereignisdetails für dieses Ereignis anzuzeigen.

      In diesem Beispiel klicken Sie auf den Ereignistitel „Storage Failover Interconnect One or More Links Down“.

   Die Seite mit den Ereignisdetails für dieses Ereignis wird angezeigt.

   a. Auf der Seite „Ereignisdetails“ können Sie eine oder mehrere der folgenden Aufgaben ausführen:
      - Überprüfen Sie die Fehlermeldung im Feld „Ursache“ und bewerten Sie das Problem.
      - Weisen Sie das Ereignis einem Administrator zu.
      - Bestätigen Sie das Ereignis.

Verwandte Informationen

"Seite mit Veranstaltungsdetails"

"Unified Manager-Benutzerrollen und -Funktionen"

Führen Sie Korrekturmaßnahmen für ausgefallene Speicher-Failover-Verbindungsverbindungen durch

Wenn Sie die Seite mit den Ereignisdetails eines Speicherfailover-bezogenen Ereignisses anzeigen, können Sie die zusammenfassenden Informationen der Seite überprüfen, um die Dringlichkeit des Ereignisses, die mögliche Ursache des Problems und eine mögliche Lösung des Problems zu ermitteln.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

In diesem Beispielszenario enthält die Ereigniszusammenfassung auf der Seite „Ereignisdetails“ die folgenden Informationen zum Zustand der unterbrochenen Speicher-Failover-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 Speicher-Failover-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 Speicherfailover-Job kann weiterhin erfolgreich sein.

Um jedoch sicherzustellen, dass weder beide Links ausfallen noch der Speicher-Failover-Schutz vollständig deaktiviert wird, beschließen Sie, den Grund für den Ausfall von Link1 genauer zu untersuchen.

Schritte

1. Auf der Detailseite **Ereignis** können Sie auf den Link zum im Feld „Quelle“ angegebenen Ereignis klicken, um weitere Details zu anderen Ereignissen zu erhalten, die möglicherweise mit dem Zustand „Verbindungsunterbrechung der Speicher-Failover-Verbindung“ in Zusammenhang stehen.

   In diesem Beispiel ist die Quelle des Ereignisses der Knoten mit dem Namen „Erdferkel“. Wenn Sie auf diesen Knotennamen klicken, werden die HA-Details für das betroffene HA-Paar (Aardvark und Bonobo) auf der Registerkarte „Knoten“ der Seite „Cluster-/Integritätsdetails“ angezeigt und andere Ereignisse angezeigt, die kürzlich auf dem betroffenen HA-Paar aufgetreten sind.

2. Weitere Informationen zur Veranstaltung finden Sie in den **HA-Details**.

   In diesem Beispiel befinden sich die relevanten Informationen in der Ereignistabelle. Die Tabelle zeigt das Ereignis „Storage Failover Connection One or More Link Down“, den Zeitpunkt der Ereignisgenerierung und erneut den Knoten, von dem dieses Ereignis stammt.

Fordern Sie mithilfe der Knotenstandortinformationen in den HA-Details eine physische Inspektion und Reparatur des Speicher-Failover-Problems auf den betroffenen HA-Paarknoten an oder führen Sie diese selbst durch.

Verwandte Informationen

"Seite mit Veranstaltungsdetails"

"Unified Manager-Benutzerrollen und -Funktionen"

Beheben von Volume-Offline-Problemen

Dieser Workflow bietet ein Beispiel dafür, wie Sie ein Volume-Offline-Ereignis auswerten und lösen können, das Unified Manager möglicherweise auf der Inventarseite der Ereignisverwaltung anzeigt. In diesem Szenario sind Sie ein Administrator, der Unified Manager verwendet, um ein oder mehrere Volume-Offline-Ereignisse zu beheben.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Volumes können aus mehreren Gründen als offline gemeldet werden:

- Der SVM-Administrator hat das Volume absichtlich offline genommen.
- Der Host-Clusterknoten des Volumes ist ausgefallen und auch das Speicher-Failover zu seinem HA-Paar-Partner ist fehlgeschlagen.
- Die Storage Virtual Machine (SVM) des Volumes wird gestoppt, da der Knoten, auf dem sich das Stammvolume dieser SVM befindet, ausgefallen ist.
- Das Hosting-Aggregat des Volumes ist aufgrund des gleichzeitigen Ausfalls zweier RAID-Festplatten ausgefallen.

Sie können die Inventarseite der Ereignisverwaltung und die Detailseiten „Cluster/Integrität“, „Speicher-VM/Integrität“ und „Volume/Integrität“ verwenden, um eine oder mehrere dieser Möglichkeiten zu bestätigen oder auszuschließen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.
2. Wählen Sie auf der Inventarseite **Event Management** die Option **Active Availability-Ereignisse** aus.
3. Klicken Sie auf den Hypertext-Link, der für das Ereignis „Volume offline“ angezeigt wird.

   Die Seite mit den Ereignisdetails für den Verfügbarkeitsvorfall wird angezeigt.

4. Überprüfen Sie auf dieser Seite die Hinweise auf Hinweise, dass der SVM-Administrator das betreffende Volume offline genommen hat.
5. Auf der Detailseite des **Ereignisses** können Sie die Informationen für eine oder mehrere der folgenden Aufgaben überprüfen:
   - Überprüfen Sie die im Feld „Ursache“ angezeigten Informationen auf mögliche Diagnosehinweise.

     In diesem Beispiel informieren Sie die Informationen im Feld „Ursache“ nur darüber, dass das Volume offline ist.

   - Überprüfen Sie den Bereich „Hinweise und Updates“ auf Hinweise, dass der SVM-Administrator das betreffende Volume absichtlich offline genommen hat.
   - Klicken Sie auf die Quelle des Ereignisses, in diesem Fall das als offline gemeldete Volume, um weitere Informationen zu diesem Volume zu erhalten.
   - Weisen Sie das Ereignis einem Administrator zu.
   - Bestätigen Sie das Ereignis oder markieren Sie es gegebenenfalls als gelöst.

Führen Sie Diagnoseaktionen für Volume-Offline-Bedingungen durch

Nachdem Sie zur Seite mit den Volume-/Integritätsdetails eines Volumes navigiert sind, das als offline gemeldet wurde, können Sie nach zusätzlichen Informationen suchen, die für die Diagnose des Offlinezustands des Volumes hilfreich sind.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn das als offline gemeldete Volume nicht absichtlich offline genommen wurde, kann dies mehrere Gründe haben.

Von der Seite „Volume/Integritätsdetails“ des Offline-Volumes aus können Sie zu anderen Seiten und Bereichen navigieren, um mögliche Ursachen zu bestätigen oder auszuschließen:

- Klicken Sie auf die Links auf der Detailseite **Volume/Integrität**, um festzustellen, ob das Volume offline ist, weil sein Hostknoten ausgefallen ist und auch das Speicher-Failover zu seinem HA-Paarpartner fehlgeschlagen ist.

  Sehen"Feststellen, ob ein Volume-Offline-Zustand durch einen ausgefallenen Knoten verursacht wird" .

- Klicken Sie auf die Links zur Detailseite **Volume/Integrität**, um festzustellen, ob das Volume offline ist und die darauf gehostete Storage Virtual Machine (SVM) angehalten wurde, weil der Knoten, auf dem sich das Stammvolume dieser SVM befindet, ausgefallen ist.

  Sehen"Feststellen, ob ein Volume offline ist und SVM gestoppt wurde, weil ein Knoten ausgefallen ist" .

- Klicken Sie auf die Links zur Detailseite **Volume/Integrität**, um festzustellen, ob das Volume aufgrund defekter Festplatten in seinem Hostaggregat offline ist.

  Sehen"Feststellen, ob ein Volume aufgrund defekter Datenträger in einem Aggregat offline ist" .

Verwandte Informationen

"Unified Manager-Benutzerrollen und -Funktionen"

Ermitteln, ob ein Volume offline ist, weil sein Hostknoten ausgefallen ist

Sie können die Web-Benutzeroberfläche von Unified Manager verwenden, um die Möglichkeit zu bestätigen oder auszuschließen, dass ein Volume offline ist, weil sein Hostknoten ausgefallen ist und das Speicher-Failover zu seinem HA-Paarpartner nicht erfolgreich ist.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Um festzustellen, ob der Offlinezustand des Volumes durch einen Ausfall des Hostknotens und ein anschließendes fehlgeschlagenes Speicher-Failover verursacht wurde, führen Sie die folgenden Aktionen aus:

Schritte

1. Suchen Sie den Hypertext-Link, der unter SVM im Bereich **Verwandte Geräte** der Detailseite **Volume/Integrität** des Offline-Volumes angezeigt wird, und klicken Sie darauf.

Auf der Seite „Storage VM / Health Details“ werden Informationen zur hostenden Storage Virtual Machine (SVM) des Offline-Volumes angezeigt.

2. Suchen Sie im Bereich **Verwandte Geräte** der Detailseite **Storage VM / Health** den unter „Volumes“ angezeigten Hypertext-Link und klicken Sie darauf.

   Die Ansicht „Integrität: Alle Volumes“ zeigt eine Tabelle mit Informationen zu allen vom SVM gehosteten Volumes an.

3. Klicken Sie in der Spaltenüberschrift „Health: All Volumes“ der Ansicht „State“ auf das Filtersymbol , und wählen Sie dann die Option **Offline**.

   Es werden nur die SVM-Volumes aufgelistet, die sich im Offline-Status befinden.

4. Klicken Sie in der Ansicht „Health: All Volumes“ auf das Rastersymbol und wählen Sie dann die Option **Clusterknoten** aus.

   Möglicherweise müssen Sie im Rasterauswahlfeld scrollen, um die Option **Clusterknoten** zu finden.

   Die Spalte „Clusterknoten“ wird zum Volume-Inventar hinzugefügt und zeigt den Namen des Knotens an, der jedes Offline-Volume hostet.

5. Suchen Sie in der Ansicht „Integrität: Alle Volumes“ den Eintrag für das Offline-Volume und klicken Sie in der Spalte „Clusterknoten“ auf den Namen des zugehörigen Hosting-Knotens.

   Auf der Registerkarte „Knoten“ auf der Seite „Cluster-/Integritätsdetails“ wird der Status des HA-Knotenpaars angezeigt, zu dem der Hosting-Knoten gehört. Der Status des Hostknotens und der Erfolg aller Cluster-Failover-Vorgänge werden in der Anzeige angegeben.

Nachdem Sie bestätigt haben, dass das Volume offline ist, weil sein Hostknoten ausgefallen ist und das Speicher-Failover zum HA-Paar-Partner fehlgeschlagen ist, wenden Sie sich an den entsprechenden Administrator oder Operator, um den ausgefallenen Knoten manuell neu zu starten und das Speicher-Failover-Problem zu beheben.

Ermitteln Sie, ob ein Volume offline ist und sein SVM gestoppt wurde, weil ein Knoten ausgefallen ist

Sie können die Web-Benutzeroberfläche von Unified Manager verwenden, um die Möglichkeit zu bestätigen oder auszuschließen, dass ein Volume offline ist, weil die zugehörige Host-Storage-Virtual-Machine (SVM) angehalten wurde, weil der Knoten, auf dem sich das Stammvolume dieser SVM befindet, ausgefallen ist.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Um festzustellen, ob der Offlinezustand des Volumes darauf zurückzuführen ist, dass das Host-SVM angehalten wurde, weil der Knoten, auf dem sich das Stammvolume dieses SVM befindet, ausgefallen ist, führen Sie die folgenden Aktionen aus:

Schritte

1. Suchen Sie den Hypertext-Link, der unter dem SVM im Bereich **Verwandte Geräte** der Detailseite **Volume/Integrität** des Offline-Volumes angezeigt wird, und klicken Sie darauf.

   Auf der Seite „Storage VM / Health Details“ wird der Status „Läuft“ oder „Gestoppt“ der Host-SVM angezeigt. Wenn der SVM-Status „Läuft“ lautet, wird der Offline-Zustand des Volumes nicht dadurch

verursacht, dass der Knoten, auf dem sich das Stammvolume dieses SVM befindet, ausgefallen ist.

2. Wenn der SVM-Status „Beendet“ lautet, klicken Sie auf „SVMs anzeigen“, um die Ursache für das Beenden des Hosting-SVMs genauer zu ermitteln.
3. Klicken Sie in der Spaltenüberschrift der Ansicht „SVM“ **Health: All Storage VMs** auf das Filtersymbol und geben Sie dann den Namen der gestoppten SVM ein.

   Die Informationen zu diesem SVM werden in einer Tabelle angezeigt.

4. Klicken Sie in der Ansicht **Health: All Storage VMs** auf und wählen Sie dann die Option **Root Volume**.

   Die Spalte „Root-Volume“ wird zum SVM-Inventar hinzugefügt und zeigt den Namen des Root-Volumes der gestoppten SVM an.

5. Klicken Sie in der Spalte „Root-Volume“ auf den Namen des Root-Volumes, um die Detailseite **Storage VM / Health** für dieses Volume anzuzeigen.

   Wenn der Status des SVM-Stammvolumes (Online) lautet, liegt der Offline-Zustand des ursprünglichen Volumes nicht daran, dass der Knoten, auf dem sich das Stammvolume dieses SVM befindet, ausgefallen ist.

6. Wenn der Status des SVM-Stammvolumes (Offline) lautet, suchen Sie den Hypertext-Link, der unter „Aggregat“ im Bereich „Verwandte Geräte“ der Seite „Volume-/Integritätsdetails“ des SVM-Stammvolumes angezeigt wird, und klicken Sie darauf.
7. Suchen Sie den Hypertext-Link, der unter „Knoten“ im Bereich „Verwandte Geräte“ der Detailseite „Aggregat/Integrität“ des Aggregats angezeigt wird, und klicken Sie darauf.

   Auf der Registerkarte „Knoten“ auf der Seite „Cluster-/Integritätsdetails“ wird der Status des HA-Knotenpaars angezeigt, zu dem der Hosting-Knoten des SVM-Stammvolumes gehört. Der Zustand des Knotens wird im Display angezeigt.

Nachdem Sie bestätigt haben, dass der Offlinezustand des Volumes durch den Offlinezustand des Host-SVM dieses Volumes verursacht wird, der wiederum durch den Ausfall des Knotens verursacht wird, der das Stammvolume dieses SVM hostet, wenden Sie sich an den entsprechenden Administrator oder Operator, um den ausgefallenen Knoten manuell neu zu starten.

Ermitteln, ob ein Volume aufgrund defekter Datenträger in einem Aggregat offline ist

Sie können die Web-Benutzeroberfläche von Unified Manager verwenden, um die Möglichkeit zu bestätigen oder auszuschließen, dass ein Volume offline ist, weil das Host-Aggregat aufgrund von RAID-Festplattenproblemen offline gegangen ist.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Um festzustellen, ob der Offlinezustand des Volumes durch RAID-Festplattenprobleme verursacht wird, die das Hosting-Aggregat offline schalten, führen Sie die folgenden Aktionen aus:

Schritte

1. Suchen Sie den Hypertext-Link, der unter „Aggregat“ im Bereich „Verwandte Geräte“ der Detailseite „Volume/Integrität“ angezeigt wird, und klicken Sie darauf.

   Auf der Seite „Aggregat-/Integritätsdetails“ wird der Online- oder Offline-Status des Hosting-Aggregats

angezeigt. Wenn der Aggregatstatus „Online“ lautet, sind RAID-Festplattenprobleme nicht die Ursache dafür, dass das Volume offline ist.

2. Wenn der Aggregatstatus „Offline“ lautet, klicken Sie auf „Datenträgerinformationen“ und suchen Sie in der Liste „Ereignisse“ auf der Registerkarte „Datenträgerinformationen“ nach Ereignissen bezüglich defekter Datenträger.
3. Um die defekten Festplatten genauer zu identifizieren, klicken Sie auf den Hypertext-Link, der unter „Knoten“ im Bereich „Verwandte Geräte“ angezeigt wird.

   Die Seite mit den Cluster-/Integritätsdetails wird angezeigt.

4. Klicken Sie auf **Datenträger** und wählen Sie dann im Bereich **Filter** die Option **Beschädigt** aus, um alle Datenträger im Zustand „Beschädigt“ aufzulisten.

   Wenn die Festplatten im defekten Zustand den Offline-Zustand des Hostaggregats verursacht haben, wird der Name des Aggregats in der Spalte „Betroffenes Aggregat“ angezeigt.

Nachdem Sie bestätigt haben, dass der Offline-Zustand des Volumes durch defekte RAID-Festplatten und das daraus resultierende Offline-Host-Aggregat verursacht wird, wenden Sie sich an den entsprechenden Administrator oder Bediener, um die defekten Festplatten manuell zu ersetzen und das Aggregat wieder online zu schalten.

Beheben Sie Kapazitätsprobleme

Dieser Workflow bietet ein Beispiel dafür, wie Sie ein Kapazitätsproblem lösen können. In diesem Szenario sind Sie ein Administrator oder Operator und greifen auf die Dashboard-Seite des Unified Managers zu, um zu sehen, ob bei einem der überwachten Speicherobjekte Kapazitätsprobleme vorliegen. Sie möchten die mögliche Ursache des Problems ermitteln und eine Lösung dafür finden.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Suchen Sie auf der Dashboard-Seite im Kapazitätsbereich unter der Dropdown-Liste „Ereignisse“ nach einem Fehlerereignis „Volume Space Full“.

Schritte

1. Klicken Sie im Bereich **Kapazität** der Seite **Dashboard** auf den Namen des Fehlerereignisses „Volume-Speicherplatz voll“.

   Die Seite mit den Ereignisdetails für den Fehler wird angezeigt.

2. Auf der Detailseite **Ereignis** können Sie eine oder mehrere der folgenden Aufgaben ausführen:
   - Überprüfen Sie die Fehlermeldung im Feld „Ursache“ und klicken Sie auf die Vorschläge unter „Vorgeschlagene Abhilfemaßnahmen“, um Beschreibungen möglicher Abhilfemaßnahmen zu überprüfen.
   - Klicken Sie im Feld „Quelle“ auf den Objektnamen (in diesem Fall ein Volume), um Details zum Objekt zu erhalten.
   - Suchen Sie nach Notizen, die möglicherweise zu diesem Ereignis hinzugefügt wurden.
   - Fügen Sie dem Ereignis eine Notiz hinzu.

- Weisen Sie das Ereignis einem anderen Benutzer zu.
- Bestätigen Sie das Ereignis.
- Markieren Sie das Ereignis als gelöst.

Verwandte Informationen

"Seite mit Veranstaltungsdetails"

Führen Sie die vorgeschlagenen Abhilfemaßnahmen für ein vollständiges Volumen durch

Nachdem Sie das Fehlerereignis „Volume Space Full“ erhalten haben, überprüfen Sie die vorgeschlagenen Abhilfemaßnahmen auf der Seite mit den Ereignisdetails und entscheiden, eine der vorgeschlagenen Maßnahmen durchzuführen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Ein Benutzer mit einer beliebigen Rolle kann alle Aufgaben in diesem Workflow ausführen, die Unified Manager verwenden.

In diesem Beispiel haben Sie auf der Inventarseite von Unified ManagerEvent Management ein Fehlerereignis „Volume Space Full“ gesehen und auf den Namen des Ereignisses geklickt.

Zu den möglichen Abhilfemaßnahmen, die Sie für ein vollständiges Volume durchführen können, gehören die folgenden:

- Aktivieren von Autogrow, Deduplizierung oder Komprimierung auf dem Volume
- Ändern der Größe oder Verschieben des Volumes
- Löschen oder Verschieben von Daten vom Volume

Obwohl alle diese Aktionen entweder vom ONTAP System Manager oder der ONTAP CLI aus ausgeführt werden müssen, können Sie mit Unified Manager Informationen finden, die Sie möglicherweise benötigen, um zu bestimmen, welche Aktionen ausgeführt werden müssen.

Schritte

1. Klicken Sie auf der Detailseite **Ereignis** auf den Volumenamen im Feld „Quelle“, um Details zum betroffenen Volume anzuzeigen.
2. Auf der Detailseite **Volume/Integrität** klicken Sie auf **Konfiguration** und sehen, dass Deduplizierung und Komprimierung auf dem Volume bereits aktiviert sind.

   Sie entscheiden sich, die Größe des Volumes zu ändern.

3. Klicken Sie im Bereich **Verwandte Geräte** auf den Namen des Hosting-Aggregats, um zu sehen, ob das Aggregat ein größeres Volumen aufnehmen kann.
4. Auf der Detailseite **Aggregat/Integrität** sehen Sie, dass das Aggregat, auf dem sich das gesamte Volume befindet, über genügend nicht zugewiesene Kapazität verfügt. Sie verwenden also ONTAP System Manager, um die Größe des Volumes anzupassen und ihm mehr Kapazität zu geben.

Verwandte Informationen

"Seite mit Veranstaltungsdetails"

Verwalten von Integritätsschwellenwerten

Sie können globale Integritätsschwellenwerte für alle Aggregate, Volumes und Qtrees konfigurieren, um alle Verletzungen der Integritätsschwellenwerte zu verfolgen.

Welche Schwellenwerte für die Speicherkapazität gelten

Ein Integritätsschwellenwert für die Speicherkapazität ist der Punkt, an dem der Unified Manager-Server Ereignisse generiert, um etwaige Kapazitätsprobleme mit Speicherobjekten zu melden. Sie können Warnmeldungen konfigurieren, um bei Auftreten solcher Ereignisse eine Benachrichtigung zu senden.

Die Integritätsschwellenwerte der Speicherkapazität für alle Aggregate, Volumes und Qtrees sind auf Standardwerte eingestellt. Sie können die Einstellungen nach Bedarf für ein Objekt oder eine Gruppe von Objekten ändern.

Konfigurieren der globalen Integritätsschwellenwerteinstellungen

Sie können globale Integritätsschwellenwerte für Kapazität, Wachstum, Snapshot-Reserve, Kontingente und Inodes konfigurieren, um Ihre Gesamt-, Volumen- und Qtree-Größe effektiv zu überwachen. Sie können auch die Einstellungen zum Generieren von Ereignissen beim Überschreiten von Verzögerungsschwellenwerten bearbeiten.

Globale Integritätsschwellenwerteinstellungen gelten für alle Objekte, mit denen sie verknüpft sind, z. B. Aggregate, Volumes usw. Beim Überschreiten von Schwellenwerten wird ein Ereignis generiert und, sofern Warnmeldungen konfiguriert sind, eine Warnmeldung gesendet. Die Schwellenwerte sind standardmäßig auf empfohlene Werte eingestellt, Sie können sie jedoch ändern, um Ereignisse in Intervallen zu generieren, die Ihren spezifischen Anforderungen entsprechen. Wenn Schwellenwerte geändert werden, werden Ereignisse im nächsten Überwachungszyklus generiert oder verworfen.

Auf die globalen Integritätsschwellenwerteinstellungen kann über den Abschnitt „Ereignisschwellenwerte“ im linken Navigationsmenü zugegriffen werden. Sie können die Schwellenwerteinstellungen für einzelne Objekte auch auf der Inventarseite oder der Detailseite für das jeweilige Objekt ändern.

- Weitere Informationen finden Sie unter"Konfigurieren globaler aggregierter Integritätsschwellenwerte" .

  Sie können die Integritätsschwellenwerteinstellungen für Kapazität, Wachstum und Snapshot-Kopien für alle Aggregate konfigurieren, um alle Schwellenwertüberschreitungen zu verfolgen.

- Weitere Informationen finden Sie unter"Konfigurieren globaler Schwellenwerte für die Volumeintegrität" .

  Sie können die Integritätsschwellenwerteinstellungen für Kapazität, Snapshot-Kopien, Qtree-Kontingente, Volume-Wachstum, Reservespeicherplatz zum Überschreiben und Inodes für alle Volumes bearbeiten, um etwaige Schwellenwertüberschreitungen zu verfolgen.

- Weitere Informationen finden Sie unter"Konfigurieren globaler Qtree-Integritätsschwellenwerte" .

  Sie können die Integritätsschwellenwerteinstellungen für die Kapazität aller Qtrees bearbeiten, um alle Schwellenwertüberschreitungen zu verfolgen.

- Weitere Informationen finden Sie unter"Bearbeiten der Lag-Health-Schwellenwerteinstellungen für nicht verwaltete Schutzbeziehungen" .

Sie können den Prozentsatz der Verzögerungszeit für Warnungen oder Fehler erhöhen oder verringern, sodass Ereignisse in Intervallen generiert werden, die Ihren Anforderungen besser entsprechen.

Konfigurieren globaler Schwellenwerte für die Gesamtintegrität

Sie können globale Integritätsschwellenwerte für alle Aggregate konfigurieren, um alle Schwellenwertüberschreitungen zu verfolgen. Bei Grenzwertüberschreitungen werden entsprechende Ereignisse generiert und Sie können auf Basis dieser Ereignisse vorbeugende Maßnahmen ergreifen. Sie können die globalen Werte basierend auf den Best Practice-Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten Aggregate gelten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn Sie die Optionen global konfigurieren, werden die Standardwerte der Objekte geändert. Wenn die Standardwerte jedoch auf Objektebene geändert wurden, werden die globalen Werte nicht geändert.

Die Schwellenwertoptionen verfügen über Standardwerte zur besseren Überwachung. Sie können die Werte jedoch ändern, um sie an die Anforderungen Ihrer Umgebung anzupassen.

Wenn Autogrow auf Volumes aktiviert ist, die sich auf dem Aggregat befinden, gelten die Schwellenwerte für die Aggregatkapazität als überschritten, und zwar basierend auf der durch Autogrow festgelegten maximalen Volumegröße, nicht basierend auf der ursprünglichen Volumegröße.

Integritätsschwellenwerte sind auf das Stammaggregat des Knotens nicht anwendbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisschwellenwerte** > **Aggregat**.
2. Konfigurieren Sie die entsprechenden Schwellenwerte für Kapazität, Wachstum und Snapshot-Kopien.
3. Klicken Sie auf **Speichern**.

Verwandte Informationen

"Benutzer hinzufügen"

Konfigurieren globaler Schwellenwerte für die Volumeintegrität

Sie können die globalen Integritätsschwellenwerte für alle Volumes konfigurieren, um alle Schwellenwertüberschreitungen zu verfolgen. Bei Verletzungen von Integritätsschwellenwerten werden entsprechende Ereignisse generiert und Sie können auf Grundlage dieser Ereignisse vorbeugende Maßnahmen ergreifen. Sie können die globalen Werte basierend auf den Best Practice-Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten Volumes gelten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die meisten Schwellenwertoptionen verfügen über Standardwerte zur besseren Überwachung. Sie können die Werte jedoch ändern, um sie an die Anforderungen Ihrer Umgebung anzupassen.

Beachten Sie, dass bei aktivierter Autogrow-Funktion auf einem Volume die Kapazitätsschwellenwerte auf Grundlage der durch Autogrow festgelegten maximalen Volumegröße und nicht auf Grundlage der ursprünglichen Volumegröße als überschritten gelten.

> 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, die mit älteren Versionen der ONTAP -Software installiert sind, beträgt die maximale Anzahl 250 Snapshot-Kopien pro Volume. Bei diesen älteren Versionen interpretiert Unified Manager diese 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 Sie diesen Schwellenwert für diese älteren Versionen auf weniger als 250 festlegen möchten, müssen Sie den Schwellenwert hier in der Ansicht „Integrität: Alle Volumes“ oder auf der Seite „Volume-/Integritätsdetails“ auf 250 oder weniger festlegen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisschwellenwerte** > **Lautstärke**.
2. Konfigurieren Sie die entsprechenden Schwellenwerte für Kapazität, Snapshot-Kopien, Qtree-Kontingente, Volume-Wachstum und Inodes.
3. Klicken Sie auf **Speichern**.

Verwandte Informationen

"Benutzer hinzufügen"

Konfigurieren Sie globale Qtree-Integritätsschwellenwerte

Sie können die globalen Integritätsschwellenwerte für alle Qtrees konfigurieren, um alle Schwellenwertüberschreitungen zu verfolgen. Bei Verletzungen von Integritätsschwellenwerten werden entsprechende Ereignisse generiert und Sie können auf Grundlage dieser Ereignisse vorbeugende Maßnahmen ergreifen. Sie können die globalen Werte basierend auf den Best-Practice-Einstellungen für Schwellenwerte konfigurieren, die für alle überwachten Qtrees gelten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die Schwellenwertoptionen verfügen über Standardwerte zur besseren Überwachung. Sie können die Werte jedoch ändern, um sie an die Anforderungen Ihrer Umgebung anzupassen.

Ereignisse werden für einen Qtree nur generiert, wenn für den Qtree ein Qtree-Kontingent oder ein Standardkontingent festgelegt wurde. Es werden keine Ereignisse generiert, wenn der in einem Benutzer- oder Gruppenkontingent definierte Speicherplatz den Schwellenwert überschritten hat.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisschwellenwerte** > **Qtree**.
2. Konfigurieren Sie die entsprechenden Kapazitätsschwellenwerte.
3. Klicken Sie auf **Speichern**.

Konfigurieren von Verzögerungsschwellenwerten für nicht verwaltete Schutzbeziehungen

Sie können die globalen Standardeinstellungen für Verzögerungswarnungen und Fehlerzustandsschwellenwerte für nicht verwaltete Schutzbeziehungen bearbeiten, sodass Ereignisse in Intervallen generiert werden, die Ihren Anforderungen entsprechen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die Verzögerungszeit darf nicht länger sein als das definierte Übertragungsintervall. Wenn beispielsweise stündlich verkehrt, darf die Verzögerungszeit nicht mehr als eine Stunde betragen. Der Verzögerungsschwellenwert gibt einen Prozentsatz an, den die Verzögerungszeit nicht überschreiten darf. Wenn im Beispiel einer Stunde der Verzögerungsschwellenwert auf 150 % festgelegt ist, erhalten Sie ein Ereignis, wenn die Verzögerungszeit mehr als 1,5 Stunden beträgt.

Die in dieser Aufgabe beschriebenen Einstellungen werden global auf alle nicht verwalteten Schutzbeziehungen angewendet. Die Einstellungen können nicht ausschließlich für eine nicht verwaltete Schutzbeziehung festgelegt und angewendet werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ereignisschwellenwerte** > **Beziehung**.
2. Erhöhen oder verringern Sie den Prozentsatz der globalen Standardwarnungs- oder Fehlerverzögerungszeit nach Bedarf.
3. Um zu verhindern, dass bei einem beliebigen Verzögerungsschwellenwert ein Warn- oder Fehlerereignis ausgelöst wird, deaktivieren Sie das Kontrollkästchen neben **Aktiviert**.
4. Klicken Sie auf **Speichern**.

Verwandte Informationen

"Benutzer hinzufügen"

Bearbeiten Sie die einzelnen Schwellenwerteinstellungen für die Gesamtintegrität

Sie können die Integritätsschwellenwerteinstellungen für die Aggregatkapazität, das Wachstum und die Snapshot-Kopien eines oder mehrerer Aggregate bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen generiert und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, basierend auf dem generierten Ereignis vorbeugende Maßnahmen zu ergreifen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Basierend auf Änderungen der Schwellenwerte werden im nächsten Überwachungszyklus Ereignisse generiert oder verworfen.

Wenn Autogrow auf Volumes aktiviert ist, die sich auf dem Aggregat befinden, gelten die Schwellenwerte für die Aggregatkapazität als überschritten, und zwar basierend auf der durch Autogrow festgelegten maximalen Volumegröße, nicht basierend auf der ursprünglichen Volumegröße.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.

2. Wählen Sie in der Ansicht **Health: Alle Aggregate** ein oder mehrere Aggregate aus und klicken Sie dann auf **Schwellenwerte bearbeiten**.
3. Bearbeiten Sie im Dialogfeld **Aggregatschwellenwerte bearbeiten** die Schwellenwerteinstellungen für eine der folgenden Optionen: Kapazität, Wachstum oder Snapshot-Kopien, indem Sie das entsprechende Kontrollkästchen aktivieren und dann die Einstellungen ändern.
4. Klicken Sie auf **Speichern**.

Verwandte Informationen

"Benutzer hinzufügen"

Bearbeiten der Schwellenwerteinstellungen für die Integrität einzelner Volumes

Sie können die Integritätsschwellenwerteinstellungen für Volumekapazität, 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, basierend auf dem generierten Ereignis vorbeugende Maßnahmen zu ergreifen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Basierend auf Änderungen der Schwellenwerte werden im nächsten Überwachungszyklus Ereignisse generiert oder verworfen.

Beachten Sie, dass bei aktivierter Autogrow-Funktion auf einem Volume die Kapazitätsschwellenwerte auf Grundlage der durch Autogrow festgelegten maximalen Volumegröße und nicht auf Grundlage der ursprünglichen Volumegröße als überschritten gelten.

> 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, die mit älteren Versionen der ONTAP -Software installiert sind, beträgt die maximale Anzahl 250 Snapshot-Kopien pro Volume. Bei diesen älteren Versionen interpretiert Unified Manager diese 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 Sie diesen Schwellenwert für diese älteren Versionen auf weniger als 250 festlegen möchten, müssen Sie den Schwellenwert hier in der Ansicht „Integrität: Alle Volumes“ oder auf der Seite „Volume-/Integritätsdetails“ auf 250 oder weniger festlegen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie in der Ansicht **Health: All Volumes** ein oder mehrere Volumes aus und klicken Sie dann auf **Edit Thresholds**.
3. Bearbeiten Sie im Dialogfeld **Volume-Schwellenwerte bearbeiten** die Schwellenwerteinstellungen für einen der folgenden Punkte: Kapazität, Snapshot-Kopien, Qtree-Kontingent, Wachstum oder Inodes, indem Sie das entsprechende Kontrollkästchen aktivieren und dann die Einstellungen ändern.
4. Klicken Sie auf **Speichern**.

Verwandte Informationen

"Benutzer hinzufügen"

Bearbeiten Sie die individuellen Qtree-Integritätsschwellenwerteinstellungen

Sie können die Integritätsschwellenwerteinstellungen für die Qtree-Kapazität für einen oder mehrere Qtrees bearbeiten. Wenn ein Schwellenwert überschritten wird, werden Warnungen generiert und Sie erhalten Benachrichtigungen. Diese Benachrichtigungen helfen Ihnen, basierend auf dem generierten Ereignis vorbeugende Maßnahmen zu ergreifen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Basierend auf Änderungen der Schwellenwerte werden im nächsten Überwachungszyklus Ereignisse generiert oder verworfen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Qtrees**.
2. Wählen Sie in der Ansicht **Kapazität: Alle Qtrees** einen oder mehrere Qtrees aus und klicken Sie dann auf **Schwellenwerte bearbeiten**.
3. Ändern Sie im Dialogfeld **Qtree-Schwellenwerte bearbeiten** die Kapazitätsschwellenwerte für den oder die ausgewählten Qtrees und klicken Sie auf **Speichern**.

> Sie können auch einzelne Qtree-Schwellenwerte auf der Registerkarte „Qtrees“ auf der Seite „Storage VM / Health Details“ festlegen.

Verwalten von Cluster-Sicherheitszielen

Unified Manager bietet ein Dashboard, das anhand der im „NetApp Security Hardening Guide for ONTAP 9“ definierten Empfehlungen ermittelt, wie sicher Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes sind.

Das Ziel des Sicherheits-Dashboards besteht darin, alle Bereiche anzuzeigen, in denen Ihre ONTAP Cluster nicht den von NetApp empfohlenen Richtlinien entsprechen, damit Sie diese potenziellen Probleme beheben können. In den meisten Fällen können Sie die Probleme mit dem ONTAP System Manager oder der ONTAP CLI beheben. Ihre Organisation befolgt möglicherweise nicht alle Empfehlungen, sodass Sie in einigen Fällen keine Änderungen vornehmen müssen.

Siehe die "NetApp Security Hardening Guide für ONTAP 9" (TR-4569) für detaillierte Empfehlungen und Lösungen.

Zusätzlich zur Meldung des Sicherheitsstatus generiert Unified Manager auch Sicherheitsereignisse für alle Cluster oder SVMs mit Sicherheitsverletzungen. Sie können diese Probleme auf der Inventarseite der Ereignisverwaltung verfolgen und Warnmeldungen für diese Ereignisse konfigurieren, sodass Ihr Speicheradministrator benachrichtigt wird, wenn neue Sicherheitsereignisse auftreten.

Weitere Informationen finden Sie unter "Welche Sicherheitskriterien werden bewertet".

Welche Sicherheitskriterien werden bewertet

Im Allgemeinen werden die Sicherheitskriterien für Ihre ONTAP Cluster, Storage Virtual Machines (SVMs) und Volumes anhand der im *NetApp Security Hardening Guide für ONTAP 9* definierten Empfehlungen bewertet.

Zu den Sicherheitskontrollen gehören unter anderem:

- ob ein Cluster eine sichere Authentifizierungsmethode wie SAML verwendet
- ob die Kommunikation zwischen Peering-Clustern verschlüsselt ist
- ob für eine Speicher-VM das Überwachungsprotokoll aktiviert ist
- ob auf Ihren Volumes Software- oder Hardwareverschlüsselung aktiviert ist

Siehe die Themen zu Compliance-Kategorien und den "NetApp Security Hardening Guide für ONTAP 9" für detaillierte Informationen.

> Von der Active IQ Plattform gemeldete Upgrade-Ereignisse gelten ebenfalls als Sicherheitsereignisse. Diese Ereignisse identifizieren Probleme, bei denen zur Lösung ein Upgrade der ONTAP -Software, der Knoten-Firmware oder der Betriebssystemsoftware (für Sicherheitshinweise) erforderlich ist. Diese Ereignisse werden nicht im Sicherheitsbereich angezeigt, sind aber auf der Inventarseite der Ereignisverwaltung verfügbar.

Weitere Informationen finden Sie unter "Verwalten von Cluster-Sicherheitszielen".

Cluster-Compliance-Kategorien

Diese Tabelle beschreibt die von Unified Manager ausgewerteten Parameter zur Cluster-Sicherheitskonformität, die NetApp -Empfehlung und ob der Parameter die Gesamtfeststellung beeinflusst, ob der Cluster den Anforderungen entspricht oder nicht.

Wenn sich in einem Cluster nicht konforme SVMs befinden, wirkt sich dies auf den Konformitätswert des Clusters aus. Daher müssen Sie in einigen Fällen möglicherweise ein Sicherheitsproblem mit einem SVM beheben, bevor die Sicherheit Ihres Clusters als konform angesehen wird.

Beachten Sie, dass nicht jeder der unten aufgeführten Parameter bei allen Installationen angezeigt wird. Wenn Sie beispielsweise keine Peering-Cluster haben oder AutoSupport auf einem Cluster deaktiviert haben, werden die Elemente „Cluster-Peering“ oder „AutoSupport HTTPS-Transport“ auf der UI-Seite nicht angezeigt.

Parameter	Beschreibung	Empfehlung	Beeinflusst die Cluster-Compliance
Globales FIPS	Gibt an, ob der Konformitätsmodus Global FIPS (Federal Information Processing Standard) 140-2 aktiviert oder deaktiviert ist. Wenn FIPS aktiviert ist, sind TLSv1 und SSLv3 deaktiviert und nur TLSv1.1 und TLSv1.2 sind zulässig.	Ermöglicht	Ja
Telnet	Gibt an, ob der Telnet-Zugriff auf das System aktiviert oder deaktiviert ist. NetApp empfiehlt Secure Shell (SSH) für sicheren Fernzugriff.	Deaktiviert	Ja
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, beispielsweise Chiffren, die mit *cbc beginnen.	Nein	Ja
Login-Banner	Gibt an, ob das Anmeldebanner für Benutzer, die auf das System zugreifen, aktiviert oder deaktiviert ist.	Ermöglicht	Ja
Cluster-Peering	Gibt an, ob die Kommunikation zwischen Peering-Clustern verschlüsselt oder unverschlüsselt ist. Damit dieser Parameter als konform gilt, muss die Verschlüsselung sowohl auf dem Quell- als auch auf dem Zielcluster konfiguriert sein.	Verschlüsselt	Ja

Parameter	Beschreibung	Empfehlung	Beeinflusst die Cluster-Compliance
Netzwerkzeitprotokoll	Gibt an, ob der Cluster über einen oder mehrere konfigurierte NTP-Server verfügt. Aus Redundanzgründen und für einen optimalen Service empfiehlt NetApp , dem Cluster mindestens drei NTP-Server zuzuordnen.	Konfiguriert	Ja
OCSP	Ab Version 9.14.1 bietet Active IQ Unified Manager Statusinformationen zum Online Certificate Status Protocol (OCSP) auf der Ebene der Storage Virtual Machine (SVM, früher als Vserver bezeichnet). Dies bedeutet, dass die OCSP-Validierung auf alle SSL/TLS-Verbindungen zum SVM angewendet wird und die Integrität und Gültigkeit der in diesen Verbindungen verwendeten Zertifikate gewährleistet.	Ermöglicht	Nein
Remote-Audit-Protokollierung	Gibt an, ob die Protokollweiterleitung (Syslog) verschlüsselt oder unverschlüsselt ist.	Verschlüsselt	Ja
AutoSupport HTTPS-Transport	Gibt an, ob HTTPS als Standardtransportprotokoll zum Senden von AutoSupport -Nachrichten an den NetApp Support verwendet wird.	Ermöglicht	Ja
Standard-Administratorbenutzer	Gibt an, ob der Standardadministratorbenutzer (integriert) aktiviert oder deaktiviert ist. NetApp empfiehlt, alle nicht benötigten integrierten Konten zu sperren (deaktivieren).	Deaktiviert	Ja

Parameter	Beschreibung	Empfehlung	Beeinflusst die Cluster-Compliance
SAML-Benutzer	Gibt an, ob SAML konfiguriert ist. SAML ermöglicht Ihnen die Konfiguration der Multi-Faktor-Authentifizierung (MFA) als Anmeldemethode für Single Sign-On.	Nein	Nein
Active Directory-Benutzer	Gibt 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 die bevorzugten Authentifizierungsmechanismen für Benutzer, die Cluster gegenüber lokalen Benutzern verwalten.	Nein	Nein
Zertifikatsbenutzer	Gibt an, ob ein Zertifikatsbenutzer für die Anmeldung beim Cluster konfiguriert ist.	Nein	Nein
Lokale Benutzer	Gibt an, ob lokale Benutzer für die Anmeldung beim Cluster konfiguriert sind.	Nein	Nein
Remote-Shell	Gibt an, ob RSH aktiviert ist. Aus Sicherheitsgründen sollte RSH deaktiviert werden. Für den sicheren Fernzugriff wird die Secure Shell (SSH) bevorzugt.	Deaktiviert	Ja

Parameter	Beschreibung	Empfehlung	Beeinflusst die Cluster-Compliance
MD5 im Einsatz	Gibt an, ob ONTAP Benutzerkonten die weniger sichere MD5-Hash-Funktion verwenden. Die Migration von MD5-gehashten Benutzerkonten zur sichereren kryptografischen Hashfunktion wie SHA-512 wird bevorzugt.	Nein	Ja
Zertifikatsausstellertyp	Gibt den Typ des verwendeten digitalen Zertifikats an.	CA-signiert	Nein

Storage-VM-Compliance-Kategorien

Diese Tabelle beschreibt die Sicherheitskonformitätskriterien für virtuelle Speichermaschinen (SVMs), die Unified Manager auswertet, die NetApp -Empfehlung und ob der Parameter die Gesamtfeststellung beeinflusst, ob die SVM den Anforderungen entspricht oder nicht.

Parameter	Beschreibung	Empfehlung	Beeinflusst die SVM-Konformität
Prüfprotokoll	Gibt an, ob die Überwachungsprotokollierung aktiviert oder deaktiviert ist.	Ermöglicht	Ja
Unsichere SSH-Einstellungen	Gibt an, ob SSH unsichere Chiffren verwendet, beispielsweise Chiffren, die mit `cbc*` .	Nein	Ja
Login-Banner	Gibt an, ob das Anmeldebanner für Benutzer aktiviert oder deaktiviert ist, die auf SVMs im System zugreifen.	Ermöglicht	Ja
LDAP-Verschlüsselung	Gibt an, ob die LDAP-Verschlüsselung aktiviert oder deaktiviert ist.	Ermöglicht	Nein

Parameter	Beschreibung	Empfehlung	Beeinflusst die SVM-Konformität
NTLM-Authentifizierung	Gibt an, ob die NTLM-Authentifizierung aktiviert oder deaktiviert ist.	Ermöglicht	Nein
LDAP-Nutzlastsignatur	Gibt an, ob die LDAP-Nutzlastsignatur aktiviert oder deaktiviert ist.	Ermöglicht	Nein
CHAP-Einstellungen	Gibt an, ob CHAP aktiviert oder deaktiviert ist.	Ermöglicht	Nein
Kerberos V5	Gibt an, ob die Kerberos V5-Authentifizierung aktiviert oder deaktiviert ist.	Ermöglicht	Nein
NIS-Authentifizierung	Gibt an, ob die Verwendung der NIS-Authentifizierung konfiguriert ist.	Deaktiviert	Nein
FPolicy-Status „Aktiv“	Gibt an, ob FPolicy erstellt wurde oder nicht.	Ja	Nein
SMB-Verschlüsselung aktiviert	Gibt an, ob SMB-Signieren und Versiegeln nicht aktiviert ist.	Ja	Nein
SMB-Signierung aktiviert	Gibt an, ob die SMB-Signatur nicht aktiviert ist.	Ja	Nein

Volumen-Compliance-Kategorien

Diese Tabelle beschreibt die Volume-Verschlüsselungsparameter, die Unified Manager auswertet, um zu bestimmen, ob die Daten auf Ihren Volumes ausreichend vor dem Zugriff durch nicht autorisierte Benutzer geschützt sind.

Beachten Sie, dass die Volume-Verschlüsselungsparameter keinen Einfluss darauf haben, ob der Cluster oder die Speicher-VM als konform gilt.

Parameter	Beschreibung
Softwareverschlüsselt	Zeigt die Anzahl der Volumes an, die mit den Softwareverschlüsselungslösungen NetApp Volume Encryption (NVE) oder NetApp Aggregate Encryption (NAE) geschützt sind.

Parameter	Beschreibung
Hardwareverschlüsselt	Zeigt die Anzahl der Volumes an, die mit der Hardwareverschlüsselung NetApp Storage Encryption (NSE) geschützt sind.
Software- und Hardwareverschlüsselung	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.

Was bedeutet nicht konform

Cluster und virtuelle Speichermaschinen (SVMs) gelten als nicht konform, wenn eines der Sicherheitskriterien, die anhand der im „NetApp Security Hardening Guide für ONTAP 9“ definierten Empfehlungen bewertet werden, nicht erfüllt ist. Darüber hinaus gilt ein Cluster als nicht konform, wenn ein SVM als nicht konform gekennzeichnet ist.

Die Statussymbole in den Sicherheitskarten haben im Hinblick auf ihre Konformität folgende Bedeutung:

- - Der Parameter ist wie empfohlen konfiguriert.
- - Der Parameter ist nicht wie empfohlen konfiguriert.
- – Entweder ist die Funktionalität auf dem Cluster nicht aktiviert oder der Parameter ist nicht wie empfohlen konfiguriert, trägt aber nicht zur Konformität des Objekts bei.

Beachten Sie, dass der Volume-Verschlüsselungsstatus keinen Einfluss darauf hat, ob der Cluster oder die SVM als konform gelten.

Sicherheitsstatus für Cluster und Storage-VMs anzeigen

Mit Active IQ Unified Manager können Sie den Sicherheitsstatus der Speicherobjekte in Ihrer Umgebung von verschiedenen Punkten der Benutzeroberfläche aus anzeigen. Sie können Informationen und Berichte basierend auf definierten Parametern sammeln und analysieren und verdächtiges Verhalten oder nicht autorisierte Systemänderungen auf den überwachten Clustern und Speicher-VMs erkennen.

Die Sicherheitsempfehlungen finden Sie im "NetApp Security Hardening Guide für ONTAP 9"

Zeigen Sie den Sicherheitsstatus auf Objektebene auf der Seite „Sicherheit“ an

Als Systemadministrator können Sie die Seite **Sicherheit** verwenden, um Einblick in die Sicherheitsstärke Ihrer ONTAP -Cluster und Speicher-VMs auf Rechenzentrums- und Standortebene zu erhalten. Die unterstützten Objekte sind Cluster, Speicher-VMs und Volumes. Gehen Sie folgendermaßen vor:

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Je nachdem, ob Sie den Sicherheitsstatus für alle überwachten Cluster oder für einen einzelnen Cluster

anzeigen möchten, wählen Sie **Alle Cluster** oder einen einzelnen Cluster aus dem Dropdown-Menü aus.

3. Klicken Sie im Bereich **Sicherheit** auf den Rechtspfeil. Die Seite „Sicherheit“ wird angezeigt.

Klicken Sie auf die Balkendiagramme, Zählungen und `View Reports` Über diese Links gelangen Sie zur Seite „Volumes“, „Cluster“ oder „Storage-VMs“, wo Sie die entsprechenden Details anzeigen oder bei Bedarf Berichte erstellen können.

Auf der Seite „Sicherheit“ werden die folgenden Bereiche angezeigt:

- **Cluster-Compliance**: der Sicherheitsstatus (Anzahl der Cluster, die konform oder nicht konform sind) aller Cluster in einem Rechenzentrum
- **Storage VM Compliance**: der Sicherheitsstatus (Anzahl der Storage VMs, die konform oder nicht konform sind) für alle Storage VMs in Ihrem Rechenzentrum
- **Volume-Verschlüsselung**: Der Volume-Verschlüsselungsstatus (Anzahl der verschlüsselten oder nicht verschlüsselten Volumes) aller Volumes in Ihrer Umgebung
- **Volume Anti-Ransomware-Status**: der Sicherheitsstatus (Anzahl der Volumes mit aktiviertem oder deaktiviertem Anti-Ransomware-Schutz) aller Volumes in Ihrer Umgebung
- **Clusterauthentifizierung und -zertifikate**: Die Anzahl der Cluster, die die einzelnen Authentifizierungsmethoden verwenden, z. B. SAML, Active Directory oder Zertifikate und lokale Authentifizierung. Das Panel zeigt auch die Anzahl der Cluster an, deren Zertifikate entweder abgelaufen sind oder in 60 Tagen ablaufen.

Sicherheitsdetails aller Cluster auf der Seite „Cluster“ anzeigen

Auf der Detailseite **Cluster/Sicherheit** können Sie den Sicherheitskonformitätsstatus auf Clusterebene anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher > Cluster**.
2. Wählen Sie **Ansicht > Sicherheit > Alle Cluster**.

Standardsicherheitsparameter wie Global FIPS, Telnet, unsichere SSH-Einstellungen, Anmeldebanner, Netzwerkzeitprotokoll, AutoSupport HTTPS-Transport und der Status des Ablaufs des Clusterzertifikats werden angezeigt.

Sie können auf das Symbol Klicken Sie auf die Schaltfläche „Weitere Optionen“ und wählen Sie, ob Sie die Sicherheitsdetails auf der Seite „Sicherheit“ von Unified Manager oder im System Manager anzeigen möchten. Sie sollten über gültige Anmeldeinformationen verfügen, um die Details im System Manager anzuzeigen.

Wenn ein Cluster ein abgelaufenes Zertifikat hat, können Sie auf `expired` unter **Gültigkeit des Cluster-Zertifikats** und erneuern Sie es über System Manager (9.10.1 und höher). Sie können nicht auf `expired` wenn die System Manager-Instanz eine Version vor 9.10.1 hat.

Sicherheitsdetails aller Cluster auf der Seite „Speicher-VMs“ anzeigen

Auf der Detailseite **Speicher-VMs/Sicherheit** können Sie den Sicherheitskonformitätsstatus auf Speicher-VM-Ebene anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher > Speicher-VMs**.

2. Wählen Sie **Ansicht > Sicherheit > Alle Speicher-VMs**. Es wird eine Liste der Cluster mit den Sicherheitsparametern angezeigt.

Sie können eine Standardansicht der Sicherheitskonformität der Speicher-VMs erhalten, indem Sie die Sicherheitsparameter wie Speicher-VMs, Cluster, Anmeldebanner, Prüfprotokoll und unsichere SSH-Einstellungen überprüfen.

Sie können auf das Symbol ⋮ Klicken Sie auf die Schaltfläche „Weitere Optionen“ und wählen Sie, ob Sie die Sicherheitsdetails auf der Seite „Sicherheit“ von Unified Manager oder im System Manager anzeigen möchten. Sie sollten über gültige Anmeldeinformationen verfügen, um die Details im System Manager anzuzeigen.

Weitere Informationen zur Anti-Ransomware-Sicherheit für Volumes und Speicher-VMs finden Sie unter"Anzeigen des Anti-Ransomware-Status aller Volumes und Storage-VMs" .

Zeigen Sie Sicherheitsereignisse an, die möglicherweise Software- oder Firmware-Updates erfordern

Es gibt bestimmte Sicherheitsereignisse, die den Auswirkungsbereich „Upgrade“ haben. Diese Ereignisse werden von der Active IQ Plattform gemeldet und identifizieren Probleme, für deren Lösung Sie ein Upgrade der ONTAP -Software, der Knoten-Firmware oder der Betriebssystemsoftware (für Sicherheitshinweise) durchführen müssen.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Bei einigen dieser Probleme möchten Sie möglicherweise sofort Abhilfemaßnahmen ergreifen, während andere Probleme möglicherweise bis zu Ihrer nächsten planmäßigen Wartung warten können. Sie können alle diese Ereignisse anzeigen und sie Benutzern zuweisen, die die Probleme lösen können. Wenn es außerdem bestimmte Sicherheitsupgrade-Ereignisse gibt, über die Sie nicht benachrichtigt werden möchten, kann Ihnen diese Liste dabei helfen, diese Ereignisse zu identifizieren, sodass Sie sie deaktivieren können.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.

   Standardmäßig werden alle aktiven (neuen und bestätigten) Ereignisse auf der Inventarseite der Ereignisverwaltung angezeigt.

2. Wählen Sie im Menü „Ansicht“ die Option „Upgrade-Ereignisse“ aus.

   Auf der Seite werden alle aktiven Upgrade-Sicherheitsereignisse angezeigt.

Anzeigen, wie die Benutzerauthentifizierung auf allen Clustern verwaltet wird

Auf der Seite „Sicherheit“ werden die Authentifizierungstypen angezeigt, die zur Authentifizierung der Benutzer in den einzelnen Clustern verwendet werden, sowie die Anzahl der Benutzer, die mit den einzelnen Typen auf den Cluster zugreifen. Auf diese Weise können Sie überprüfen, ob die Benutzerauthentifizierung gemäß den Vorgaben Ihrer Organisation sicher durchgeführt wird.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.

2. Wählen Sie oben im Dashboard im Dropdown-Menü **Alle Cluster** aus.
3. Klicken Sie im Bereich **Sicherheit** auf den Rechtspfeil, und die Seite **Sicherheit** wird angezeigt.
4. Zeigen Sie die Karte **Cluster-Authentifizierung** an, um die Anzahl der Benutzer anzuzeigen, die mit jedem Authentifizierungstyp auf das System zugreifen.
5. Zeigen Sie die Karte **Clustersicherheit** an, um die Authentifizierungsmechanismen anzuzeigen, die zur Authentifizierung von Benutzern in jedem Cluster verwendet werden.

Wenn einige Benutzer mit einer unsicheren Methode auf das System zugreifen oder eine Methode verwenden, die von NetApp nicht empfohlen wird, können Sie die Methode deaktivieren.

Den Verschlüsselungsstatus aller Volumes anzeigen

Sie können eine Liste aller Volumes und ihres aktuellen Verschlüsselungsstatus anzeigen, um festzustellen, ob die Daten auf Ihren Volumes ausreichend vor dem Zugriff durch unbefugte Benutzer geschützt sind.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die folgenden Verschlüsselungstypen können auf ein Volume angewendet werden:

- 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. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Integrität“ > „Volumes-Verschlüsselung“ aus.
3. Sortieren Sie in der Ansicht **Integrität: Volume-Verschlüsselung** nach dem Feld **Verschlüsselungstyp** oder verwenden Sie den Filter, um Volumes anzuzeigen, die einen bestimmten Verschlüsselungstyp haben oder die nicht verschlüsselt sind (Verschlüsselungstyp „Keine“).

Anzeigen des Anti-Ransomware-Status aller Volumes und Speicher-VMs

Sie können eine Liste aller Volumes und Storage-VMs (SVMs) und deren aktuellen Anti-Ransomware-Status anzeigen, sodass Sie feststellen können, ob die Daten auf Ihren Volumes und SVMs ausreichend vor Ransomware-Angriffen geschützt sind.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Weitere Informationen zu den verschiedenen Anti-Ransomware-Status finden Sie unter"ONTAP: Anti-Ransomware aktivieren" .

Zeigen Sie Sicherheitsdetails aller Volumes mit Anti-Ransomware-Erkennung an

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Integrität“ > „Sicherheit“ > „Anti-Ransomware“
3. In der Ansicht **Sicherheit: Anti-Ransomware** können Sie nach den verschiedenen Feldern sortieren oder den Filter verwenden.

> Anti-Ransomware wird nicht für Offline-Volumes, eingeschränkte Volumes, SnapLock Volumes, FlexGroup Volumes, FlexCache Volumes, reine SAN-Volumes, Volumes gestoppter Speicher-VMs, Root-Volumes von Speicher-VMs oder Datensicherungs-Volumes unterstützt.

Sicherheitsdetails aller Storage-VMs mit Anti-Ransomware-Erkennung anzeigen

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher > Speicher-VMs**.
2. Wählen Sie **Ansicht > Sicherheit > Anti-Ransomware**. Es wird eine Liste der SVMs mit dem Anti-Ransomware-Status angezeigt.

> Die Anti-Ransomware-Überwachung wird auf Speicher-VMs, bei denen das NAS-Protokoll nicht aktiviert ist, nicht unterstützt.

Alle aktiven Sicherheitsereignisse anzeigen

Sie können alle aktiven Sicherheitsereignisse anzeigen und jedes davon einem Benutzer zuweisen, der das Problem lösen kann. Wenn es außerdem bestimmte Sicherheitsereignisse gibt, die Sie nicht erhalten möchten, kann Ihnen diese Liste dabei helfen, die Ereignisse zu identifizieren, die Sie deaktivieren möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Event Management**.

   Standardmäßig werden neue und bestätigte Ereignisse auf der Inventarseite der Ereignisverwaltung angezeigt.

2. Wählen Sie im Menü „Ansicht“ die Option „Aktive Sicherheitsereignisse“ aus.

   Auf der Seite werden alle neuen und bestätigten Sicherheitsereignisse angezeigt, die in den letzten 7 Tagen generiert wurden.

Hinzufügen von Warnungen für Sicherheitsereignisse

Sie können Warnungen für einzelne Sicherheitsereignisse konfigurieren, genau wie für alle anderen Ereignisse, die von Unified Manager empfangen werden. Wenn Sie außerdem alle Sicherheitsereignisse gleich behandeln und E-Mails an dieselbe Person senden möchten, können Sie eine einzelne Warnung erstellen, die Sie benachrichtigt,

wenn Sicherheitsereignisse ausgelöst werden.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Das folgende Beispiel zeigt, wie Sie eine Warnung für das Sicherheitsereignis „Telnet-Protokoll aktiviert“ erstellen. Dadurch wird eine Warnung gesendet, wenn der Telnet-Zugriff für den Remote-Verwaltungszugriff auf den Cluster konfiguriert ist. Mit derselben Methode können Sie Warnungen für alle Sicherheitsereignisse erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
2. Klicken Sie auf der Seite **Alarm-Setup** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Warnung hinzufügen** auf **Name** und geben Sie einen Namen und eine Beschreibung für die Warnung ein.
4. Klicken Sie auf **Ressourcen** und wählen Sie den Cluster oder die Cluster aus, für die Sie diese Warnung aktivieren möchten.
5. Klicken Sie auf **Ereignisse** und führen Sie die folgenden Aktionen aus:
   a. Wählen Sie in der Liste „Ereignisschweregrad“ **Warnung** aus.
   b. Wählen Sie in der Liste „Übereinstimmende Ereignisse“ **Telnet-Protokoll aktiviert** aus.
6. Klicken Sie auf **Aktionen** und wählen Sie dann im Feld **Diese Benutzer benachrichtigen** den Namen des Benutzers aus, der die Warn-E-Mail erhalten soll.
7. Konfigurieren Sie auf dieser Seite alle anderen Optionen für die Benachrichtigungshäufigkeit, das Ausgeben von SNMP-Taps und das Ausführen eines Skripts.
8. Klicken Sie auf **Speichern**.

Deaktivieren bestimmter Sicherheitsereignisse

Alle Ereignisse sind standardmäßig aktiviert. Sie können bestimmte Ereignisse deaktivieren, um die Generierung von Benachrichtigungen für Ereignisse zu verhindern, die in Ihrer Umgebung nicht wichtig sind. Sie können deaktivierte Ereignisse aktivieren, wenn Sie weiterhin Benachrichtigungen dafür erhalten möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn Sie Ereignisse deaktivieren, werden die zuvor generierten Ereignisse im System als veraltet markiert und die für diese Ereignisse konfigurierten Warnungen werden nicht ausgelöst. Wenn Sie deaktivierte Ereignisse aktivieren, werden die Benachrichtigungen für diese Ereignisse ab dem nächsten Überwachungszyklus generiert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Ereigniseinrichtung**.
2. Deaktivieren oder aktivieren Sie Ereignisse auf der Seite „Ereignis-Setup“, indem Sie eine der folgenden Optionen auswählen:

Wenn Sie wollen…	Dann tun Sie Folgendes …
Ereignisse deaktivieren	a. Klicken Sie auf **Deaktivieren**. b. Wählen Sie im Dialogfeld „Ereignisse deaktivieren“ den Schweregrad **Warnung** aus. Dies ist die Kategorie für alle Sicherheitsereignisse. c. Wählen Sie in der Spalte „Übereinstimmende Ereignisse“ die Sicherheitsereignisse aus, die Sie deaktivieren möchten, und klicken Sie dann auf den Rechtspfeil, um diese Ereignisse in die Spalte „Ereignisse deaktivieren“ zu verschieben. d. Klicken Sie auf **Speichern und schließen**. e. Überprüfen Sie, ob die von Ihnen deaktivierten Ereignisse in der Listenansicht der Seite „Ereigniseinrichtung“ angezeigt werden.
Ereignisse aktivieren	a. Aktivieren Sie in der Liste der deaktivierten Ereignisse das Kontrollkästchen für das bzw. die Ereignisse, die Sie wieder aktivieren möchten. b. Klicken Sie auf **Aktivieren**.

Sicherheitsereignisse

Sicherheitsereignisse liefern Ihnen Informationen zum Sicherheitsstatus von ONTAP -Clustern, Storage Virtual Machines (SVMs) und Volumes basierend auf den im *NetApp Security Hardening Guide für ONTAP 9* definierten Parametern. Diese Ereignisse benachrichtigen Sie über potenzielle Probleme, sodass Sie deren Schweregrad einschätzen und das Problem gegebenenfalls beheben können.

Sicherheitsereignisse werden nach Quelltyp gruppiert und enthalten den Ereignis- und Trap-Namen, die Auswirkungsstufe und den Schweregrad. Diese Ereignisse werden in den Cluster- und Speicher-VM-Ereigniskategorien angezeigt.

Verwalten von Sicherungs- und Wiederherstellungsvorgängen

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 einem neuen (Remote-)System wiederherzustellen.

Abhängig vom Betriebssystem, auf dem Sie Unified Manager installiert haben, und von der Anzahl der verwalteten Cluster und Knoten gibt es drei Sicherungs- und Wiederherstellungsmethoden:

Betriebssystem	Größe der Bereitstellung	Empfohlene Sicherungsmethode
VMware vSphere	Beliebig	VMware-Snapshot der virtuellen Unified Manager-Appliance
Red Hat Enterprise Linux	Klein	Unified Manager MySQL-Datenbank-Dump
	Groß	NetApp Snapshot der Unified Manager-Datenbank
Microsoft Windows	Klein	Unified Manager MySQL-Datenbank-Dump
	Groß	NetApp Snapshot der Unified Manager-Datenbank mit iSCSI-Protokoll

Diese verschiedenen Methoden werden in den folgenden Abschnitten beschrieben.

Sicherung und Wiederherstellung für Unified Manager auf virtueller Appliance

Das Sicherungs- und Wiederherstellungsmodell für Unified Manager bei Installation auf einer virtuellen Appliance besteht darin, ein Image der vollständigen virtuellen Anwendung zu erfassen und wiederherzustellen.

Mit den folgenden Aufgaben können Sie eine Sicherung der virtuellen Appliance durchführen:

1. Schalten Sie die VM aus und erstellen Sie einen VMware-Snapshot der virtuellen Unified Manager-Appliance.
2. Erstellen Sie eine NetApp -Snapshot-Kopie auf dem Datenspeicher, um den VMware-Snapshot zu erfassen.

   Wenn der Datenspeicher nicht auf einem System gehostet wird, auf dem ONTAP -Software ausgeführt wird, befolgen Sie die Richtlinien des Speicheranbieters, um eine Sicherung des VMware-Snapshots zu erstellen.

3. Replizieren Sie die NetApp Snapshot-Kopie oder ein Snapshot-Äquivalent auf einen alternativen Speicher.
4. Löschen Sie den VMware-Snapshot.

Sie sollten mithilfe dieser Aufgaben einen Sicherungszeitplan implementieren, um sicherzustellen, dass die virtuelle Unified Manager-Appliance geschützt ist, falls Probleme auftreten.

Um die VM wiederherzustellen, können Sie den von Ihnen erstellten VMware-Snapshot verwenden, um die VM in den Zustand zum Zeitpunkt der Sicherung zurückzusetzen.

Sichern und Wiederherstellen mithilfe eines MySQL-Datenbank-Dumps

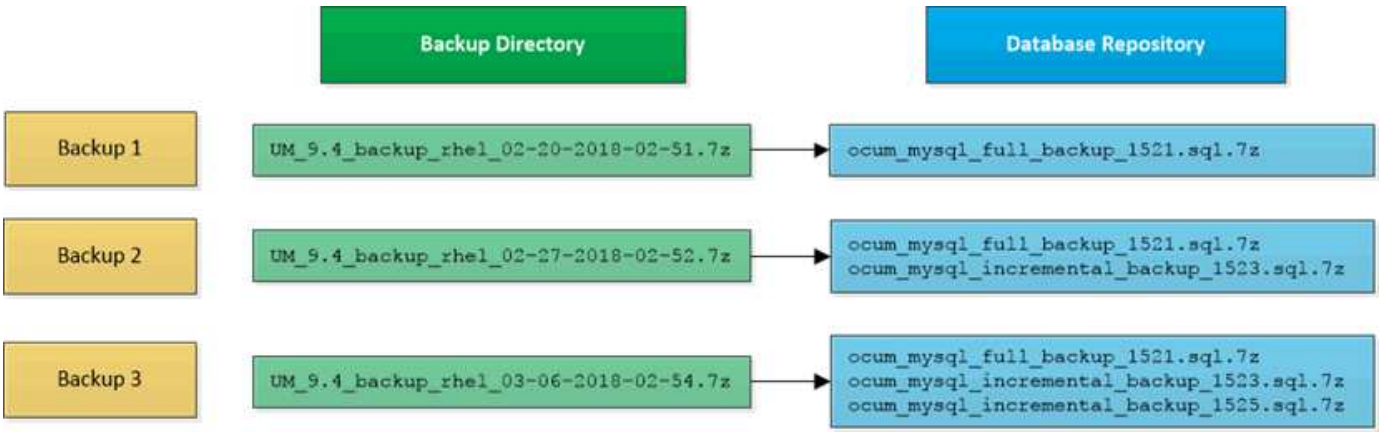
Ein MySQL-Datenbank-Dump-Backup ist eine Kopie der Active IQ Unified Manager -Datenbank und der Konfigurationsdateien, die Sie im Falle eines Systemausfalls oder

Datenverlusts verwenden können. Sie können eine Sicherung so planen, dass sie an ein lokales oder ein Remoteziel geschrieben wird. Es wird dringend empfohlen, einen Remote-Standort außerhalb des Active IQ Unified Manager Hostsystems zu definieren.

Der MySQL-Datenbank-Dump ist der Standard-Sicherungsmechanismus, wenn Unified Manager auf einem Linux- und Windows-Server installiert ist. Wenn Unified Manager jedoch eine große Anzahl von Clustern und Knoten verwaltet oder die Fertigstellung Ihrer MySQL-Sicherungen viele Stunden dauert, können Sie mithilfe von Snapshot-Kopien eine Sicherung durchführen. Diese Funktionalität ist unter Red Hat Enterprise Linux und Windows verfügbar.

Eine Datenbank-Dump-Sicherung besteht aus einer einzelnen Datei im Sicherungsverzeichnis und einer oder mehreren Dateien im Datenbank-Repository-Verzeichnis. Die Datei im Sicherungsverzeichnis ist sehr klein, da sie nur einen Zeiger auf die Dateien im Datenbank-Repository-Verzeichnis enthält, die zum erneuten Erstellen der Sicherung erforderlich sind.

Wenn Sie zum ersten Mal eine Datenbanksicherung erstellen, wird eine einzelne Datei im Sicherungsverzeichnis und eine vollständige Sicherungsdatei im Datenbank-Repository-Verzeichnis erstellt. Wenn Sie das nächste Mal eine Sicherung erstellen, wird eine einzelne Datei im Sicherungsverzeichnis und eine inkrementelle Sicherungsdatei im Datenbank-Repository-Verzeichnis erstellt, die die Unterschiede zur vollständigen Sicherungsdatei enthält. Dieser Vorgang wird fortgesetzt, während Sie weitere Sicherungen erstellen, bis die maximale Aufbewahrungseinstellung erreicht ist, wie in der folgenden Abbildung dargestellt.



Benennen Sie keine der Sicherungsdateien in diesen beiden Verzeichnissen um und entfernen Sie sie auch nicht, da sonst alle nachfolgenden Wiederherstellungsvorgänge fehlschlagen.

Wenn Sie Ihre Sicherungsdateien auf das lokale System schreiben, sollten Sie einen Prozess zum Kopieren der Sicherungsdateien an einen Remote-Speicherort einleiten, damit sie verfügbar sind, falls ein Systemproblem auftritt, das eine vollständige Wiederherstellung erfordert.

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 wird überprüft, ob auf dem System genügend Speicherplatz zum Erstellen der Sicherungsdatei vorhanden ist.

Konfigurieren Sie das Ziel und den Zeitplan für Datenbank-Dump-Backups

Sie können die Einstellungen für die Datenbank-Dump-Sicherung von Unified Manager konfigurieren, um den Datenbank-Sicherungspfad, die Aufbewahrungsanzahl und den Sicherungszeitplan festzulegen. Sie können täglich oder wöchentlich geplante

Sicherungen aktivieren. Standardmäßig sind geplante Sicherungen deaktiviert, Sie sollten jedoch einen Sicherungszeitplan festlegen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- An dem Speicherort, den Sie als Sicherungspfad definieren, müssen mindestens 150 GB Speicherplatz verfügbar sein.

  Es wird empfohlen, einen Remote-Standort außerhalb des Unified Manager-Hostsystems zu verwenden.

- Wenn Unified Manager auf einem Linux-System installiert ist und MySQL-Backup verwendet, stellen Sie sicher, dass die folgenden Berechtigungen und Eigentümer für das Backup-Verzeichnis festgelegt sind.

  Berechtigungen: 0750, Eigentum: jboss:maintenance

- Wenn Unified Manager auf einem Windows-System installiert ist und MySQL-Backup verwendet, stellen Sie sicher, dass nur der Administrator Zugriff auf das Backup-Verzeichnis hat.

Für die Durchführung einer ersten Sicherung ist mehr Zeit erforderlich als für nachfolgende Sicherungen, da es sich bei der ersten Sicherung um eine vollständige Sicherung handelt. Eine vollständige Sicherung kann über 1 GB groß sein und drei bis vier Stunden dauern. Nachfolgende Sicherungen erfolgen inkrementell und benötigen weniger Zeit.

- Wenn Sie feststellen, dass die Anzahl der inkrementellen Sicherungsdateien für den für Sicherungen zugewiesenen Speicherplatz zu groß ist, können Sie regelmäßig eine vollständige Sicherung durchführen, um die alte Sicherung und ihre inkrementellen Dateien zu ersetzen. Alternativ können Sie mithilfe von Snapshot-Kopien eine Sicherung erstellen.
- Die Sicherung, die während der ersten 15 Tage nach der Hinzufügung eines neuen Clusters erstellt wurde, ist möglicherweise nicht genau genug, um die historischen Leistungsdaten zu erhalten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Datenbanksicherung**.
2. Klicken Sie auf der Seite **Datenbanksicherung** auf **Sicherungseinstellungen**.
3. Konfigurieren Sie die entsprechenden Werte für einen Sicherungspfad, eine Aufbewahrungsanzahl und einen Zeitplan.

   Der Standardwert für die Aufbewahrungsanzahl ist 10; Sie können 0 verwenden, um unbegrenzte Sicherungen zu erstellen.

4. Wählen Sie die Schaltfläche **Täglich geplant** oder **Wöchentlich geplant** und geben Sie dann die Zeitplandetails an.
5. Klicken Sie auf **Übernehmen**.

Datenbank-Dump-Sicherungsdateien werden basierend auf dem Zeitplan erstellt. Sie können die verfügbaren Sicherungsdateien auf der Seite „Datenbanksicherung“ sehen.

Was eine Datenbankwiederherstellung ist

Bei der Wiederherstellung einer MySQL-Datenbank handelt es sich um den Vorgang, bei dem eine vorhandene Unified Manager-Sicherungsdatei auf demselben oder einem

anderen Unified Manager-Server wiederhergestellt wird. Sie führen den Wiederherstellungsvorgang über die Wartungskonsole von Unified Manager aus.

Wenn Sie einen Wiederherstellungsvorgang auf demselben (lokalen) System durchführen und alle Sicherungsdateien lokal gespeichert sind, können Sie die Wiederherstellungsoption unter Verwendung des Standardspeicherorts ausführen. Wenn Sie einen Wiederherstellungsvorgang auf einem anderen Unified Manager-System (einem Remote-System) durchführen, müssen Sie die Sicherungsdatei(en) vom sekundären Speicher auf die lokale Festplatte kopieren, bevor Sie die Wiederherstellungsoption ausführen.

Während des Wiederherstellungsvorgangs werden Sie von Unified Manager abgemeldet. Sie können sich beim System anmelden, nachdem der Wiederherstellungsvorgang abgeschlossen ist.

Wenn Sie das Sicherungsimage auf einem neuen Server wiederherstellen, müssen Sie nach Abschluss des Wiederherstellungsvorgangs ein neues HTTPS-Sicherheitszertifikat generieren und den Unified Manager-Server neu starten. Sie müssen außerdem die SAML-Authentifizierungseinstellungen neu konfigurieren, falls diese erforderlich sind, wenn Sie das Sicherungsimage auf einem neuen Server wiederherstellen.

> Alte Sicherungsdateien können nicht zum Wiederherstellen eines Images verwendet werden, nachdem Unified Manager auf eine neuere Softwareversion aktualisiert wurde. Um Speicherplatz zu sparen, werden alle alten Sicherungsdateien, mit Ausnahme der neuesten Datei, automatisch entfernt, wenn Sie Unified Manager aktualisieren.

Verwandte Informationen

"Generieren eines HTTPS-Sicherheitszertifikats"

"Aktivieren der SAML-Authentifizierung"

"Authentifizierung mit Active Directory oder OpenLDAP"

Wiederherstellen einer MySQL-Datenbanksicherung unter Windows

Im Falle eines Datenverlusts oder einer Datenbeschädigung können Sie die Wiederherstellungsfunktion verwenden, um Unified Manager mit minimalem Verlust in den vorherigen stabilen Zustand zurückzusetzen. Sie können die Unified Manager MySQL-Datenbank mithilfe der Unified Manager-Wartungskonsole auf einem lokalen Windows-System oder einem Remote-Windows-System wiederherstellen.

Bevor Sie beginnen

- Sie müssen über Windows-Administratorrechte verfügen.
- Sie müssen die Unified Manager-Sicherungsdatei und den Inhalt des Datenbank-Repository-Verzeichnisses auf das System kopiert haben, auf dem Sie den Wiederherstellungsvorgang durchführen.

  Es wird empfohlen, die Sicherungsdatei in das Standardverzeichnis zu kopieren `\ProgramData\NetApp\OnCommandAppData\ocum\backup` . Die Datenbank-Repository-Dateien müssen in das `\database_dumps_repo` Unterverzeichnis unter dem `\backup` Verzeichnis.

- Die Sicherungsdateien müssen `.7z` Typ.

Die Wiederherstellungsfunktion ist plattform- und versionsspezifisch. Sie können ein Unified Manager MySQL-Backup nur auf derselben Version von Unified Manager wiederherstellen, und ein Windows-Backup kann nur auf einer Windows-Plattform wiederhergestellt werden.

Wenn die Ordnernamen ein Leerzeichen enthalten, müssen Sie den absoluten Pfad oder den relativen Pfad der Sicherungsdatei in doppelte Anführungszeichen setzen.

Schritte

1. Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager nicht die Benutzeroberfläche und konfigurieren Sie keine Cluster, Benutzer oder Authentifizierungseinstellungen, wenn die Installation abgeschlossen ist. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsvorgangs.
2. Melden Sie sich mit Administratoranmeldeinformationen beim Unified Manager-System an.
3. Starten Sie PowerShell oder die Eingabeaufforderung als Windows-Administrator.
4. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
5. Geben Sie im **Hauptmenü** der Wartungskonsole die Nummer für die Option **Backup-Wiederherstellung** ein.
6. Geben Sie die Nummer für die **Wiederherstellung des MySQL-Backups** ein.
7. Geben Sie bei der entsprechenden Aufforderung den absoluten Pfad der Sicherungsdatei ein.

   ```
   Bundle to restore from:
   \ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac
   kup_windows_02-20-2020-02-51.7z
   ```

   Nachdem der Wiederherstellungsvorgang abgeschlossen ist, können Sie sich bei Unified Manager anmelden.

Wenn der OnCommand Workflow Automation -Server nach der Wiederherstellung der Sicherung nicht funktioniert, führen Sie die folgenden Schritte aus:

1. Ändern Sie auf dem Workflow Automation-Server die IP-Adresse des Unified Manager-Servers, sodass sie auf die neueste Maschine verweist.
2. Setzen Sie auf dem Unified Manager-Server das Datenbankkennwort zurück, wenn die Erfassung in Schritt 1 fehlschlägt.

Sichern und Wiederherstellen mit NetApp Snapshots

Eine NetApp Snapshot-Kopie erstellt ein zeitpunktbezogenes Image der Unified Manager-Datenbank und der Konfigurationsdateien, das Sie im Falle eines Systemausfalls oder Datenverlusts zur Wiederherstellung verwenden können. Sie planen, dass regelmäßig eine Snapshot-Kopie auf ein Volume auf einem Ihrer ONTAP Cluster geschrieben wird, sodass Sie immer über eine aktuelle Kopie verfügen.

Diese Funktionalität ist für Active IQ Unified Manager, der auf einer virtuellen Appliance installiert ist, nicht verfügbar.

Konfigurieren der Sicherung unter Linux

Wenn Ihr Active IQ Unified Manager auf einem Linux-Computer installiert ist, können Sie Ihre Sicherung und Wiederherstellung mithilfe von NetApp Snapshots konfigurieren.

Snapshot-Kopien dauern nur sehr wenig Zeit, normalerweise nur wenige Minuten, und die Unified Manager-Datenbank wird für einen sehr kurzen Zeitraum gesperrt, sodass Ihre Installation kaum unterbrochen wird. Das Image benötigt nur minimalen Speicherplatz und verursacht nur einen vernachlässigbaren Leistungsaufwand, da es nur die Änderungen an Dateien seit der letzten Snapshot-Kopie aufzeichnet. Da der Snapshot auf einem ONTAP Cluster erstellt wird, können Sie bei Bedarf andere NetApp -Funktionen wie SnapMirror nutzen, um einen sekundären Schutz zu erstellen.

Vor Beginn eines Sicherungsvorgangs führt Unified Manager eine Integritätsprüfung durch, um sicherzustellen, dass das Zielsystem verfügbar ist.

- Sie können eine Snapshot-Kopie nur auf derselben Version von Active IQ Unified Manager wiederherstellen.

  Wenn Sie beispielsweise ein Backup auf Unified Manager 9.16 erstellt haben, kann das Backup nur auf Unified Manager 9.16-Systemen wiederhergestellt werden.

- Wenn sich die Snapshot-Konfiguration ändert, kann dies dazu führen, dass der Snapshot ungültig wird.

Konfigurieren des Speicherorts für die Snapshot-Kopie

Sie können das Volume, auf dem Snapshot-Kopien gespeichert werden, auf einem Ihrer ONTAP Cluster mithilfe des ONTAP System Manager oder der ONTAP CLI konfigurieren.

Bevor Sie beginnen

Cluster, Speicher-VM und Volume müssen die folgenden Anforderungen erfüllen:

- Clusteranforderungen:
  - ONTAP 9.3 oder höher muss installiert sein
  - Es sollte sich geografisch in der Nähe des Unified Manager-Servers befinden
  - Es kann von Unified Manager überwacht werden, ist aber nicht erforderlich
- Anforderungen an die Speicher-VM:
  - Der Namensschalter und die Namenszuordnung müssen auf die Verwendung von „`files`“ eingestellt sein.
  - Lokale Benutzer, die zur Korrespondenz mit clientseitigen Benutzern erstellt wurden
  - Stellen Sie sicher, dass „Alle Lese-/Schreibzugriffe“ ausgewählt ist.
  - Stellen Sie sicher, dass der Superuser-Zugriff in der Exportrichtlinie auf „any“ eingestellt ist.
  - 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 Speicher-VM angegeben sein
  - Das Volume sollte mindestens doppelt so groß sein wie das Verzeichnis Unified Manager/opt/netapp/data

    Verwenden Sie den Befehl du -sh /opt/netapp/data/, um die aktuelle Größe zu überprüfen.

- Volumenanforderungen:
  - Das Volume sollte mindestens doppelt so groß sein wie das Unified Manager-Verzeichnis /opt/netapp/data

- Der Sicherheitsstil muss auf UNIX eingestellt sein
- Die lokale Snapshot-Richtlinie muss deaktiviert sein
- Die automatische Volume-Größe sollte aktiviert sein
- Das Leistungs-Servicelevel sollte auf eine Richtlinie mit hohen IOPS und geringer Latenz eingestellt werden, z. B. „Extrem“.

Ausführliche Schritte zum Erstellen des NFS-Volumes finden Sie unter "So konfigurieren Sie NFSv4 in ONTAP 9" und die "ONTAP 9 NFS-Konfigurations-Expresshandbuch" .

Geben Sie den Zielspeicherort für Snapshot-Kopien an

Sie sollten den Zielspeicherort für Active IQ Unified Manager Snapshot-Kopien auf einem Volume konfigurieren, das Sie bereits in einem Ihrer ONTAP Cluster konfiguriert haben. Sie sollten die Wartungskonsole verwenden, um den Standort zu definieren.

- Sie müssen über die Root-Benutzeranmeldeinformationen für den Linux-Host verfügen, auf dem Active IQ Unified Manager installiert ist.
- Sie müssen über eine Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.
- Sie müssen über die Cluster-Management-IP-Adresse, den Namen der Speicher-VM, den Namen des Volumes sowie den Benutzernamen und das Kennwort des Speichersystems verfügen.
- Sie müssen das Volume auf dem Active IQ Unified Manager Host gemountet haben und Sie müssen über den Mount-Pfad verfügen.

Schritte

1. Verwenden Sie Secure Shell, um eine Verbindung mit der IP-Adresse oder dem FQDN des Active IQ Unified Manager -Systems herzustellen.
2. Melden Sie sich mit dem Namen und Kennwort des Wartungsbenutzers (umadmin) beim System an.
3. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
4. Geben Sie im **Hauptmenü** der Wartungskonsole die Nummer für die Option **Backup-Wiederherstellung** ein.
5. Geben Sie die Nummer für * NetApp Snapshot Backup konfigurieren* ein.
6. Geben Sie die Nummer ein, um NFS zu konfigurieren.
7. Überprüfen Sie die Informationen, die Sie angeben müssen, und geben Sie dann die Nummer für **Backup-Konfigurationsdetails eingeben** ein.
8. Um das Volume zu identifizieren, auf das der Snapshot geschrieben wird, geben Sie die IP-Adresse der Cluster-Management-Schnittstelle, den Namen der Speicher-VM, den Namen des Volumes, den LUN-Namen, den Benutzernamen und das Kennwort des Speichersystems sowie den Mount-Pfad ein.
9. Überprüfen Sie diese Informationen und geben Sie `y` .

   Das System führt die folgenden Aufgaben aus:

   - Stellt die Verbindung zum Cluster her
   - Stoppt alle Dienste
   - Erstellt ein neues Verzeichnis im Volume und kopiert die Konfigurationsdateien der Active IQ Unified Manager Datenbank

- Löscht die Dateien aus Active IQ Unified Manager und erstellt einen Symlink zum neuen Datenbankverzeichnis
- Startet alle Dienste neu

10. Beenden Sie die Wartungskonsole und starten Sie die Active IQ Unified Manager Schnittstelle, um einen Zeitplan für die Snapshot-Kopie zu erstellen, falls Sie dies noch nicht getan haben.

Konfigurieren der Sicherung unter Windows

Active IQ Unified Manager unterstützt die Sicherung und Wiederherstellung mithilfe von NetApp Snapshots auf dem Windows-Betriebssystem mithilfe von LUN unter Verwendung des iSCSI-Protokolls.

Snapshot-basierte Sicherungen können durchgeführt werden, während alle Unified Manager-Dienste ausgeführt werden. Ein konsistenter Status der Datenbank wird als Teil des Snapshots erfasst, da das Backup eine globale Lesesperre auf die gesamte Datenbank setzt, die alle gleichzeitigen Schreibvorgänge verhindert. Damit Ihr unter Windows installiertes Unified Manager-System mithilfe von NetApp Snapshots Sicherungen und Wiederherstellungen durchführen kann, sollten Sie zunächst mithilfe der Wartungskonsole die Unified Manager-Sicherung auf Snapshot-Basis konfigurieren.

Bevor Sie Unified Manager zum Erstellen von Snapshot-Kopien konfigurieren, sollten Sie die folgenden Konfigurationsaufgaben durchführen.

- ONTAP Cluster konfigurieren
- Konfigurieren des Windows-Hostcomputers

Konfigurieren des Sicherungsspeicherorts für Windows

Sie sollten das Volume zum Speichern von Snapshot-Kopien konfigurieren, nachdem Sie Unified Manager unter Windows gesichert haben.

Bevor Sie beginnen

Cluster, Speicher-VM und Volume müssen die folgenden Anforderungen erfüllen:

- Clusteranforderungen:
  - ONTAP 9.3 oder höher muss installiert sein
  - Es sollte sich geografisch in der Nähe des Unified Manager-Servers befinden
  - Es wird von Unified Manager überwacht
- Anforderungen an die Speicher-VM:
  - iSCSI-Konnektivität auf ONTAP Cluster
  - Das iSCSI-Protokoll muss für die konfigurierte Maschine aktiviert sein
  - Sie sollten über ein dediziertes Volume und LUN für die Sicherungskonfiguration verfügen. Das ausgewählte Volume sollte nur eine LUN und sonst nichts enthalten.
  - Die Größe der LUN sollte mindestens doppelt so groß sein wie die Datengröße, die voraussichtlich im 9.9 Active IQ Unified Manager verarbeitet werden kann.

    Dadurch werden auch für das Volumen dieselben Größenanforderungen festgelegt.

  - Stellen Sie sicher, dass „Alle Lese-/Schreibzugriffe“ ausgewählt ist.

    - Stellen Sie sicher, dass der Superuser-Zugriff in der Exportrichtlinie auf „any“ eingestellt ist.
- Volume- und LUN-Anforderungen:
    - Das Volume sollte mindestens doppelt so groß sein wie das MySQL-Datenverzeichnis von Unified Manager.
    - Der Sicherheitsstil muss auf Windows eingestellt sein
    - Die lokale Snapshot-Richtlinie muss deaktiviert sein
    - Die automatische Volume-Größe sollte aktiviert sein
    - Das Leistungs-Servicelevel sollte auf eine Richtlinie mit hohen IOPS und geringer Latenz eingestellt werden, z. B. „Extrem“.

ONTAP Cluster konfigurieren

Sie müssen einige Vorkonfigurationsschritte auf ONTAP -Clustern durchführen, bevor Sie Active IQ Unified Manager mithilfe einer Snapshot-Kopie auf Windows-Systemen sichern und wiederherstellen können.

Sie können den ONTAP Cluster entweder über die Eingabeaufforderung oder die Benutzeroberfläche des System Managers konfigurieren. Die Konfiguration des ONTAP Clusters umfasst die Konfiguration von Daten-LIFs, die als iSCSI-LIFs der Speicher-VM zugewiesen werden können. Der nächste Schritt besteht darin, eine iSCSI-fähige Speicher-VM über die Benutzeroberfläche des System Managers zu konfigurieren. Sie müssen eine statische Netzwerkroute für diese Speicher-VM konfigurieren, um zu steuern, wie LIFs das Netzwerk für ausgehenden Datenverkehr verwenden.

> Sie sollten über ein dediziertes Volume und eine LUN für die Sicherungskonfiguration verfügen. Das ausgewählte Volume sollte nur eine LUN enthalten. Die Größe der LUN sollte mindestens doppelt so groß sein wie die Datengröße, die voraussichtlich von Active IQ Unified Manager verarbeitet wird.

Sie müssen die folgende Konfiguration durchführen:

Schritte

1. Konfigurieren Sie eine iSCSI-fähige Speicher-VM oder verwenden Sie eine vorhandene Speicher-VM mit derselben Konfiguration.
2. Konfigurieren Sie eine Netzwerkroute für die konfigurierte Speicher-VM.
3. Konfigurieren Sie ein Volume mit entsprechender Kapazität und einer einzelnen LUN darin und stellen Sie sicher, dass das Volume nur für diese LUN reserviert ist.

> In einem Szenario, in dem die LUN im System Manager erstellt wird, kann das Aufheben der Zuordnung der LUN dazu führen, dass die igroup gelöscht wird und die Wiederherstellung fehlschlägt. Um dieses Szenario zu vermeiden, stellen Sie sicher, dass beim Erstellen einer LUN diese explizit erstellt und nicht gelöscht wird, wenn die Zuordnung der LUN aufgehoben wird.

4. Konfigurieren Sie eine Initiatorgruppe in der Speicher-VM.
5. Konfigurieren Sie einen Portsatz.
6. Integrieren Sie die Igroup mit dem Portset.
7. Ordnen Sie die LUN der igroup zu.

Konfigurieren des Windows-Hostcomputers

Sie müssen Ihren Windows-Hostcomputer konfigurieren, bevor Sie NetApp Snapshot zum Sichern und Wiederherstellen von Active IQ Unified Manager verwenden können. Um den Microsoft iSCSI-Initiator auf einem Windows-Hostcomputer zu starten, geben Sie „`iscsi`“ in die Suchleiste ein und klicken Sie auf **iSCSI-Initiator**.

Bevor Sie beginnen

Sie sollten alle vorherigen Konfigurationen auf dem Hostcomputer bereinigen.

Wenn Sie versuchen, den iSCSI-Initiator bei einer Neuinstallation von Windows zu starten, werden Sie zur Bestätigung aufgefordert. Nach Ihrer Bestätigung wird das Dialogfeld „iSCSI-Eigenschaften“ angezeigt. Wenn es sich um eine vorhandene Windows-Installation handelt, wird das Dialogfeld „iSCSI-Eigenschaften“ mit einem Ziel angezeigt, das entweder inaktiv ist oder versucht, eine Verbindung herzustellen. Sie müssen also sicherstellen, dass alle vorherigen Konfigurationen auf dem Windows-Host entfernt werden.

Schritte

1. Bereinigen Sie alle vorherigen Konfigurationen auf dem Hostcomputer.
2. Entdecken Sie das Zielportal.
3. Stellen Sie eine Verbindung zum Zielportal her.
4. Stellen Sie über Multipath eine Verbindung zum Zielportal her.
5. Entdecken Sie beide LIFs.
6. Ermitteln Sie die im Windows-Computer als Gerät konfigurierte LUN.
7. Konfigurieren Sie die erkannte LUN als neues Volume-Laufwerk in Windows.

Geben Sie den Zielspeicherort für Snapshot-Kopien unter Windows an

Sie sollten den Zielspeicherort für Active IQ Unified Manager Snapshot-Kopien auf einem Volume konfigurieren, das Sie bereits in einem Ihrer ONTAP Cluster konfiguriert haben. Sie sollten die Wartungskonsole verwenden, um den Standort zu definieren.

- Sie müssen über Administratorrechte für den Windows-Host verfügen, auf dem Active IQ Unified Manager installiert ist.
- Sie müssen über eine Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.
- Sie müssen über die Cluster-Management-IP-Adresse, den Namen der Speicher-VM, den Namen des Volumes, den LUN-Namen sowie den Benutzernamen und das Kennwort des Speichersystems verfügen.
- Sie müssen das Volume als Netzwerklaufwerk auf dem Active IQ Unified Manager Host bereitgestellt haben und über das Bereitstellungslaufwerk verfügen.

Schritte

1. Stellen Sie mithilfe von Power Shell eine Verbindung zur IP-Adresse oder zum vollqualifizierten Domänennamen des Active IQ Unified Manager Systems her.
2. Melden Sie sich mit dem Namen und Kennwort des Wartungsbenutzers (umadmin) beim System an.
3. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
4. Geben Sie im **Hauptmenü** der Wartungskonsole die Nummer für die Option **Backup-Wiederherstellung** ein.

5. Geben Sie die Nummer für * NetApp Snapshot Backup konfigurieren* ein.
6. Geben Sie die Nummer ein, um iSCSI zu konfigurieren.
7. Überprüfen Sie die Informationen, die Sie angeben müssen, und geben Sie dann die Nummer für **Backup-Konfigurationsdetails eingeben** ein.
8. Um das Volume zu identifizieren, auf das der Snapshot geschrieben wird, geben Sie die IP-Adresse der Cluster-Management-Schnittstelle, den Namen der Speicher-VM, den Namen des Volumes, den LUN-Namen, den Benutzernamen und das Kennwort des Speichersystems sowie das Mount-Laufwerk ein.
9. Überprüfen Sie diese Informationen und geben Sie `y` .

   Das System führt die folgenden Aufgaben aus:

   - Speicher-VM ist validiert
   - Volumen ist validiert
   - Laufwerk einbinden und Status wird validiert
   - Existenz und Status der LUN
   - Existenz eines Netzlaufwerks
   - Das Vorhandensein des empfohlenen Speicherplatzes (mehr als das Doppelte des MySQL-Datenverzeichnisses) auf dem bereitgestellten Volume wird überprüft
   - LUN-Pfad, der der dedizierten LUN im Volume entspricht
   - igroup-Name
   - GUID des Volumes, auf dem das Netzlaufwerk eingebunden ist
   - iSCSI-Initiator zur Kommunikation mit ONTAP
10. Beenden Sie die Wartungskonsole und starten Sie die Active IQ Unified Manager Schnittstelle, um einen Zeitplan für Snapshot-Kopien zu erstellen.

Konfigurieren Sie die Sicherung per Snapshot-Kopie von der Wartungskonsole aus

Um mithilfe einer Snapshot-Kopie ein Active IQ Unified Manager -Backup durchzuführen, sollten Sie einige Konfigurationsschritte über die Wartungskonsole ausführen.

Bevor Sie beginnen

Sie sollten über die folgenden Details zu Ihrem System verfügen:

- Cluster-IP-Adresse
- Speicher-VM-Name
- Datenträgername
- LUN-Name
- Mount-Pfad
- Anmeldeinformationen für das Speichersystem

Schritte

1. Greifen Sie auf die Wartungskonsole von Unified Manager zu.
2. Geben Sie 4 ein, um **Backup-Wiederherstellung** auszuwählen.
3. Geben Sie 2 ein, um **Sichern und Wiederherstellen mit NetApp Snapshot** auszuwählen.

Wenn Sie die Sicherungskonfiguration ändern möchten, geben Sie 3 ein, um * NetApp Snapshot-Sicherungskonfiguration aktualisieren* auszuwählen. Sie können nur das Passwort aktualisieren.

4. Geben Sie im Menü 1 ein, um * NetApp Snapshot-Backup konfigurieren* auszuwählen.
5. Geben Sie 1 ein, um die erforderlichen Informationen bereitzustellen.
6. Geben Sie den Benutzernamen und das Kennwort für die Wartungskonsole ein und bestätigen Sie anschließend, dass die LUN auf dem Host gemountet ist.

   Der Prozess überprüft dann, ob das von Ihnen angegebene Datenverzeichnis, der LUN-Pfad, die Speicher-VM, die Volumes, die Speicherplatzverfügbarkeit, das Laufwerk usw. korrekt sind. Die im Hintergrund ablaufende Vorgänge sind:

   - Dienste werden gestoppt
   - Das Datenbankverzeichnis wird in den bereitgestellten Speicher verschoben
   - Datenbankverzeichnis wird gelöscht und Symlinks werden erstellt
   - Die Dienste werden neu gestartet. Nachdem die Konfiguration in der Active IQ Unified Manager Schnittstelle abgeschlossen ist, wird der Sicherungstyp in NetApp Snapshot geändert und in der Benutzeroberfläche als Datenbanksicherung (Snapshot-basiert) angezeigt.

Bevor Sie mit einem Sicherungsvorgang beginnen, müssen Sie prüfen, ob es Änderungen an der Snapshot-Konfiguration gibt, da dies dazu führen könnte, dass der Snapshot ungültig wird. Angenommen, Sie haben die Sicherung auf dem Laufwerk G konfiguriert und einen Snapshot erstellt. Sie haben die Sicherung später auf Laufwerk E neu konfiguriert und die Daten werden gemäß der neuen Konfiguration auf Laufwerk E gespeichert. Wenn Sie versuchen, einen Snapshot wiederherzustellen, der erstellt wurde, als er sich auf dem Laufwerk G befand, schlägt dies mit der Fehlermeldung fehl, dass das Laufwerk G nicht existiert.

Definieren Sie einen Sicherungszeitplan für Linux und Windows

Sie können den Zeitplan, nach dem Unified Manager-Snapshot-Kopien erstellt werden, mithilfe der Unified Manager-Benutzeroberfläche konfigurieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Einstellungen zum Erstellen von Snapshot-Kopien über die Wartungskonsole konfiguriert haben, um das Ziel zu identifizieren, 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.

Die Sicherung, die während der ersten 15 Tage nach der Hinzufügung eines neuen Clusters erstellt wurde, ist möglicherweise nicht genau genug, um die historischen Leistungsdaten zu erhalten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Datenbanksicherung**.
2. Klicken Sie auf der Seite **Datenbanksicherung** auf **Sicherungseinstellungen**.
3. Geben Sie im Feld **Aufbewahrungsanzahl** die maximale Anzahl der Snapshot-Kopien ein, die Sie aufbewahren möchten.

Der Standardwert für die Aufbewahrungsanzahl ist 10. Die maximale Anzahl von Snapshot-Kopien wird durch die Version der ONTAP -Software auf dem Cluster bestimmt. Sie können dieses Feld leer lassen, um den Maximalwert unabhängig von der ONTAP Version zu implementieren.

4. Wählen Sie die Schaltfläche **Täglich geplant** oder **Wöchentlich geplant** und geben Sie dann die Zeitplandetails an.
5. Klicken Sie auf **Übernehmen**.

Snapshot-Kopien werden basierend auf dem Zeitplan erstellt. Sie können die verfügbaren Sicherungsdateien auf der Seite „Datenbanksicherung“ sehen.

Aufgrund der Wichtigkeit dieses Volumes und der Snapshots möchten Sie möglicherweise ein oder zwei Warnmeldungen für dieses Volume erstellen, damit Sie benachrichtigt werden, wenn Folgendes eintritt:

- Der Speicherplatz des Volumes ist zu 90 % belegt. Verwenden Sie das Ereignis **Volume Space Full**, um die Warnung einzurichten.

  Sie können dem Volume mithilfe des ONTAP System Manager oder der ONTAP CLI Kapazität hinzufügen, damit der Speicherplatz in der Unified Manager-Datenbank nicht ausgeht.

- Die Anzahl der Snapshots hat fast die maximale Anzahl erreicht. Verwenden Sie das Ereignis **Zu viele Snapshot-Kopien**, um die Warnung einzurichten.

  Sie können ältere Snapshots mit dem ONTAP System Manager oder der ONTAP CLI löschen, sodass immer Platz für neue Snapshot-Kopien vorhanden ist.

Sie konfigurieren Warnungen auf der Seite „Warnungseinrichtung“.

Wiederherstellen von Unified Manager mithilfe von Snapshot-Kopien

Bei Datenverlust oder Datenbeschädigung können Sie Unified Manager mit minimalem Datenverlust in den vorherigen stabilen Zustand zurückversetzen. Sie können die Unified Manager Snapshot-Datenbank mithilfe der Unified Manager-Wartungskonsole auf einem lokalen oder Remote-Betriebssystem wiederherstellen.

Bevor Sie beginnen

- Sie müssen über die Root-Benutzeranmeldeinformationen für den Linux-Host und über Administratorrechte für den Windows-Hostcomputer verfügen, auf dem Unified Manager installiert ist.
- Sie müssen über eine Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.

Die Wiederherstellungsfunktion ist plattform- und versionsspezifisch. Sie können eine Unified Manager-Sicherung nur auf derselben Version von Unified Manager wiederherstellen.

Schritte

1. Stellen Sie eine Verbindung zur IP-Adresse oder zum vollqualifizierten Domänennamen des Unified Manager-Systems her.
   - Linux: Secure Shell
   - Windows: Power Shell
2. Melden Sie sich mit den Root-Benutzeranmeldeinformationen beim System an.

3. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
4. Geben Sie im **Hauptmenü** der Wartungskonsole 4 für die Option **Backup-Wiederherstellung** ein.
5. Geben Sie 2 ein, um **Sichern und Wiederherstellen mit NetApp Snapshot** auszuwählen.

   Wenn Sie eine Wiederherstellung auf einem neuen Server durchführen, starten Sie nach der Installation von Unified Manager nicht die Benutzeroberfläche und konfigurieren Sie keine Cluster, Benutzer oder Authentifizierungseinstellungen, wenn die Installation abgeschlossen ist. Geben Sie 1 ein, um * NetApp Snapshot Backup konfigurieren* auszuwählen, und konfigurieren Sie die Einstellungen für Snapshot-Kopien so, wie sie auf dem Originalsystem sind.

6. Geben Sie 3 ein, um **Wiederherstellen mit NetApp Snapshot** auszuwählen.
7. Wählen Sie die Snapshot-Kopie aus, von der Sie Unified Manager wiederherstellen möchten. Drücken Sie **Enter**.
8. Melden Sie sich nach Abschluss des Wiederherstellungsvorgangs bei der Benutzeroberfläche von Unified Manager an.

Wenn der Workflow Automation-Server nach der Wiederherstellung der Sicherung nicht funktioniert, führen Sie die folgenden Schritte aus:

1. Ändern Sie auf dem Workflow Automation-Server die IP-Adresse des Unified Manager-Servers, sodass sie auf die neueste Maschine verweist.
2. Setzen Sie auf dem Unified Manager-Server das Datenbankkennwort zurück, wenn die Erfassung in Schritt 1 fehlschlägt.

Ändern des Sicherungstyps

Wenn Sie den Sicherungstyp für Ihr Active IQ Unified Manager System ändern möchten, können Sie die Optionen der Wartungskonsole verwenden. Mit der Option * NetApp Snapshot Backup dekonfigurieren* können Sie auf das MySQL-basierte Backup zurückgreifen.

Bevor Sie beginnen

Sie müssen über eine Benutzer-ID und ein Kennwort verfügen, die Sie zum Anmelden bei der Wartungskonsole des Unified Manager-Servers berechtigen.

Schritte

1. Greifen Sie auf die Wartungskonsole zu.
2. Wählen Sie 4 aus dem **Hauptmenü** zum Sichern und Wiederherstellen.
3. Wählen Sie 2 aus dem **Sichern und Wiederherstellen-Menü**.
4. Wählen Sie 4 für * NetApp Snapshot Backup dekonfigurieren*.

   Die ausgeführten Aktionen werden angezeigt: Beenden Sie die Dienste, trennen Sie den symbolischen Link, verschieben Sie die Daten vom Speicher in das Verzeichnis und starten Sie die Dienste anschließend erneut.

   Nachdem die Sicherungsmethode geändert wurde, wird der Sicherungsmechanismus von der Snapshot-Kopie auf die standardmäßige MySQL-Sicherung geändert. Diese Änderung wird im Abschnitt „Datenbanksicherung“ der allgemeinen Einstellungen angezeigt.

On-Demand-Backup für Unified Manager

Sie können die Benutzeroberfläche von Active IQ Unified Manager verwenden, um bei Bedarf bei Bedarf ein Backup zu erstellen. Mit der On-Demand-Sicherung können Sie mithilfe der vorhandenen Sicherungsmethode sofort eine Sicherung erstellen. Bei der On-Demand-Sicherung wird nicht zwischen MySQL- oder NetApp Snapshot-basierter Sicherung unterschieden.

Sie können eine On-Demand-Sicherung mit der Schaltfläche **Jetzt sichern** auf der Seite „Datenbanksicherung“ durchführen. Die On-Demand-Sicherung ist nicht von den Zeitplänen abhängig, die Sie für Active IQ Unified Manager konfiguriert haben.

Migrieren einer virtuellen Unified Manager-Appliance auf ein Linux-System

Sie können ein Dump-Backup der MySQL-Datenbank von Unified Manager von einer virtuellen Appliance auf einem 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 müssen über die Rolle „Operator“, „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
  - Für den Wiederherstellungsvorgang müssen Sie den Namen des Unified Manager-Wartungsbenutzers kennen.
- Auf dem Linux-System:
  - Sie müssen Unified Manager auf einem Linux-Server installiert haben, indem Sie die Anweisungen in"Installieren von Unified Manager auf Linux-Systemen" .
  - Die Version von Unified Manager auf diesem Server muss mit der Version auf der virtuellen Appliance übereinstimmen, von der Sie die Sicherungsdatei verwenden.
  - Starten Sie nach der Installation nicht die Benutzeroberfläche und konfigurieren Sie keine Cluster, Benutzer oder Authentifizierungseinstellungen auf dem Linux-System. Die Sicherungsdatei füllt diese Informationen während des Wiederherstellungsvorgangs.
  - Sie müssen über die Root-Benutzeranmeldeinformationen für den Linux-Host verfügen.

Diese Schritte beschreiben, wie Sie eine Sicherungsdatei auf der virtuellen Appliance erstellen, die Sicherungsdateien auf Red Hat Enterprise Linux kopieren und dann die Datenbanksicherung auf dem neuen System wiederherstellen.

Schritte

1. Klicken Sie auf der virtuellen Appliance auf **Verwaltung** > **Datenbanksicherung**.
2. Klicken Sie auf der Seite **Datenbanksicherung** auf **Sicherungseinstellungen**.
3. Ändern Sie den Sicherungspfad in /jail/support.
4. Wählen Sie im Abschnitt „Zeitplan“ die Option „Täglich geplant“ aus und geben Sie eine Zeit ein, die einige Minuten nach der aktuellen Zeit liegt, damit die Sicherung in Kürze erstellt wird.
5. Klicken Sie auf **Übernehmen**.
6. Warten Sie einige Stunden, bis die Sicherung erstellt wurde.

Eine vollständige Sicherung kann über 1 GB groß sein und drei bis vier Stunden dauern.

7. Melden Sie sich als Root-Benutzer beim Linux-Host an, auf dem Unified Manager installiert ist, und kopieren Sie die Sicherungsdateien mithilfe von SCP von /support auf die virtuelle Appliance.`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

   ```
   root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
   ```

   Stellen Sie sicher, dass Sie die .7z-Sicherungsdatei und alle .7z-Repository-Dateien in das Unterverzeichnis /database-dumps-repo kopiert haben.

8. Stellen Sie die Sicherung in der Eingabeaufforderung wieder her: `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. Melden Sie sich nach Abschluss des Wiederherstellungsvorgangs bei der Unified Manager-Web-Benutzeroberfläche an.

Sie sollten die folgenden Aufgaben ausführen:

- Generieren Sie ein neues HTTPS-Sicherheitszertifikat und starten Sie den Unified Manager-Server neu.
- Ändern Sie den Sicherungspfad auf die Standardeinstellung für Ihr Linux-System (/data/ocum-backup) oder auf einen neuen Pfad Ihrer Wahl, da auf dem Linux-System kein Pfad /jail/support vorhanden ist.
- Konfigurieren Sie beide Seiten Ihrer Workflow Automation-Verbindung neu, wenn WFA verwendet wird.
- Konfigurieren Sie die SAML-Authentifizierungseinstellungen neu, wenn Sie SAML verwenden.

Nachdem Sie überprüft haben, dass auf Ihrem Linux-System alles wie erwartet läuft, können Sie die virtuelle Unified Manager-Appliance herunterfahren und entfernen.

Skripte verwalten

Sie können Skripte verwenden, um mehrere Speicherobjekte in Unified Manager automatisch zu ändern oder zu aktualisieren. Das Skript ist mit einer Warnung verknüpft. Wenn ein Ereignis eine Warnung auslöst, wird das Skript ausgeführt. Sie können benutzerdefinierte Skripte hochladen und deren Ausführung testen, wenn eine Warnung generiert wird.

Die Möglichkeit, Skripte in Unified Manager hochzuladen und auszuführen, ist standardmäßig aktiviert. Wenn Ihre Organisation diese Funktion aus Sicherheitsgründen nicht zulassen möchte, können Sie sie unter **Speicherverwaltung** > **Funktionseinstellungen** deaktivieren.

So funktionieren Skripte mit Warnungen

Sie können Ihrem Skript eine Warnung zuordnen, sodass das Skript ausgeführt wird, wenn für ein Ereignis in Unified Manager eine Warnung ausgelöst wird. Sie können die Skripts verwenden, um Probleme mit Speicherobjekten zu beheben oder zu ermitteln, welche Speicherobjekte die Ereignisse generieren.

Wenn für ein Ereignis in Unified Manager eine Warnung generiert wird, wird eine Warn-E-Mail an die

angegebenen Empfänger gesendet. Wenn Sie eine Warnung mit einem Skript verknüpft haben, wird das Skript ausgeführt. Die Einzelheiten zu den an das Skript übergebenen Argumenten können Sie der Warn-E-Mail entnehmen.

> Wenn Sie ein benutzerdefiniertes Skript erstellt und es mit einer Warnung für einen bestimmten Ereignistyp verknüpft haben, werden Aktionen basierend auf Ihrem benutzerdefinierten Skript für diesen Ereignistyp ausgeführt und die Aktionen **Fix it** sind standardmäßig auf der Seite „Verwaltungsaktionen“ oder im Unified Manager-Dashboard nicht verfügbar.

Das Skript verwendet die folgenden Argumente zur Ausführung:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Sie können die Argumente in Ihren Skripten verwenden und zugehörige Ereignisinformationen sammeln oder Speicherobjekte ändern.

Beispiel zum Abrufen von Argumenten aus Skripten

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

Wenn eine Warnung generiert wird, wird dieses Skript ausgeführt und die folgende Ausgabe angezeigt:

```
-eventID : 290
-eventSourceID : 4138
```

Skripts hinzufügen

Sie können in Unified Manager Skripte hinzufügen und die Skripte mit Warnungen verknüpfen. Diese Skripte werden automatisch ausgeführt, wenn eine Warnung generiert wird, und ermöglichen es Ihnen, Informationen zu Speicherobjekten zu erhalten, für die das Ereignis generiert wird.

Bevor Sie beginnen

- Sie müssen die Skripte erstellt und gespeichert haben, die Sie dem Unified Manager-Server hinzufügen möchten.
- 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 wird Perl 5 standardmäßig installiert und Skripte unterstützen nur das, was Perl 5 unterstützt. Wenn Perl nach Unified Manager installiert wurde, müssen Sie den Unified Manager-Server neu starten.
  - 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 Warnskripts zu verfolgen, müssen Sie sicherstellen, dass die Protokolldateien nicht irgendwo im Installationsordner von Unified Manager erstellt werden.

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können benutzerdefinierte Skripte hochladen und Ereignisdetails zur Warnung sammeln.

> Wenn diese Funktion in der Benutzeroberfläche nicht verfügbar ist, liegt das daran, dass Ihr Administrator sie deaktiviert hat. Bei Bedarf können Sie diese Funktion unter **Speicherverwaltung** > **Funktionseinstellungen** aktivieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Skripte**.
2. Klicken Sie auf der Seite **Skripte** auf **Hinzufügen**.
3. Klicken Sie im Dialogfeld **Skript hinzufügen** auf **Durchsuchen**, um Ihre Skriptdatei auszuwählen.
4. Geben Sie eine Beschreibung für das ausgewählte Skript ein.
5. Klicken Sie auf **Hinzufügen**.

Skripte löschen

Sie können ein Skript aus Unified Manager löschen, wenn das Skript nicht mehr benötigt wird oder nicht mehr gültig ist.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Das Skript darf nicht mit einer Warnung verknüpft sein.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Skripte**.
2. Wählen Sie auf der Seite **Skripte** das Skript aus, das Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang mit einem Klick auf **Ja**.

Testskriptausführung

Sie können überprüfen, ob Ihr Skript korrekt ausgeführt wird, wenn eine Warnung für ein Speicherobjekt generiert wird.

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen ein Skript im unterstützten Dateiformat in Unified Manager hochgeladen haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Skripte**.
2. Fügen Sie auf der Seite „Skripte“ Ihr Testskript hinzu.
3. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Alarm-Setup**.
4. Führen Sie auf der Seite **Alarm-Setup** eine der folgenden Aktionen aus:

Zu…	Machen Sie Folgendes…
Hinzufügen einer Benachrichtigung	a. Klicken Sie auf **Hinzufügen**. b. Ordnen Sie im Abschnitt „Aktionen“ die Warnung Ihrem Testskript zu.
Bearbeiten einer Benachrichtigung	a. Wählen Sie eine Warnung aus und klicken Sie dann auf **Bearbeiten**. b. Ordnen Sie im Abschnitt „Aktionen“ die Warnung Ihrem Testskript zu.

5. Klicken Sie auf **Speichern**.
6. Wählen Sie auf der Seite **Alarm-Setup** den Alarm aus, den Sie hinzugefügt oder geändert haben, und klicken Sie dann auf **Test**.

   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.

Verwalten und Überwachen von Gruppen

Sie können in Unified Manager Gruppen erstellen, um Speicherobjekte zu verwalten.

Gruppen verstehen

Sie können in Unified Manager Gruppen erstellen, um Speicherobjekte zu verwalten. Wenn Sie sich mit den Konzepten von Gruppen auskennen und wissen, wie Sie durch Gruppenregeln Speicherobjekte zu einer Gruppe hinzufügen können, können Sie die Speicherobjekte in Ihrer Umgebung besser verwalten.

Was eine Gruppe ist

Eine Gruppe ist eine dynamische Sammlung heterogener Speicherobjekte (Cluster, SVMs oder Volumes). Sie können in Unified Manager Gruppen erstellen, um eine Reihe

von Speicherobjekten einfach zu verwalten. Die Mitglieder einer Gruppe können sich ändern, abhängig von den Speicherobjekten, die zu einem bestimmten Zeitpunkt von Unified Manager überwacht werden.

- Jede Gruppe hat einen eindeutigen Namen.
- Sie müssen für jede Gruppe mindestens eine Gruppenregel konfigurieren.
- Sie können einer Gruppe mehr als eine Gruppenregel zuordnen.
- Jede Gruppe kann mehrere Arten von Speicherobjekten wie Cluster, SVMs oder Volumes enthalten.
- Speicherobjekte werden einer Gruppe dynamisch hinzugefügt, je nachdem, wann eine Gruppenregel erstellt wird oder wann Unified Manager einen Überwachungszyklus abschließt.
- Sie können Aktionen gleichzeitig auf alle Speicherobjekte in einer Gruppe anwenden, beispielsweise Schwellenwerte für Volumes festlegen.

So funktionieren Gruppenregeln für Gruppen

Eine Gruppenregel ist ein Kriterium, das Sie definieren, um die Aufnahme von Speicherobjekten (Volumes, Cluster oder SVMs) in eine bestimmte Gruppe zu ermöglichen. Sie können Bedingungsgruppen oder Bedingungen verwenden, um Gruppenregeln für eine Gruppe zu definieren.

- Sie müssen einer Gruppe eine Gruppenregel zuordnen.
- Sie müssen einer Gruppenregel einen Objekttyp zuordnen. Einer Gruppenregel ist nur ein Objekttyp zugeordnet.
- Speicherobjekte werden nach jedem Überwachungszyklus oder beim Erstellen, Bearbeiten oder Löschen einer Regel zur Gruppe hinzugefügt oder daraus entfernt.
- Eine Gruppenregel kann eine oder mehrere Bedingungsgruppen haben und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben.
- Speicherobjekte können basierend auf den von Ihnen erstellten Gruppenregeln mehreren Gruppen angehören.

Bedingungen

Sie können mehrere Bedingungsgruppen erstellen und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben. Sie können alle definierten Bedingungsgruppen in einer Gruppenregel für Gruppen anwenden, um festzulegen, welche Speicherobjekte in die Gruppe aufgenommen werden.

Bedingungen innerhalb einer Bedingungsgruppe werden mit einem logischen UND ausgeführt. Alle Bedingungen einer Bedingungsgruppe müssen erfüllt sein. Wenn Sie eine Gruppenregel erstellen oder ändern, wird eine Bedingung erstellt, die nur diejenigen Speicherobjekte anwendet, auswählt und gruppiert, die alle Bedingungen in der Bedingungsgruppe erfüllen. Sie können mehrere Bedingungen innerhalb einer Bedingungsgruppe verwenden, wenn Sie den Umfang der in eine Gruppe aufzunehmenden Speicherobjekte einschränken möchten.

Sie können Bedingungen mit Speicherobjekten erstellen, indem Sie die folgenden Operanden und Operatoren verwenden und den erforderlichen Wert angeben.

Speicherobjekttyp	Anwendbare Operanden
Volumen	• Objektname • Name des besitzenden Clusters • Name des besitzenden SVM • Anmerkungen
SVM	• Objektname • Name des besitzenden Clusters • Anmerkungen
Cluster	• Objektname • Anmerkungen

Wenn Sie eine Annotation als Operand für ein beliebiges Speicherobjekt auswählen, ist der Operator „Ist“ verfügbar. Für alle anderen Operanden können Sie als Operator entweder „Ist“ oder „Enthält“ auswählen.

- Operand

  Die Liste der Operanden im Unified Manager ändert sich je nach ausgewähltem Objekttyp. Die Liste enthält den Objektnamen, den Namen des besitzenden Clusters, den Namen des besitzenden SVM und Anmerkungen, die Sie in Unified Manager definieren.

- Operator

  Die Liste der Operatoren ändert sich basierend auf dem ausgewählten Operanden für eine Bedingung. Die in Unified Manager unterstützten Operatoren sind „Ist“ und „Enthält“.

  Wenn Sie den Operator „Ist“ auswählen, wird die Bedingung auf eine genaue Übereinstimmung des Operandenwerts mit dem für den ausgewählten Operanden bereitgestellten Wert geprüft.

  Wenn Sie den Operator „Enthält“ auswählen, wird die Bedingung ausgewertet, um eines der folgenden Kriterien zu erfüllen:

  ◦ Der Operandenwert entspricht genau dem für den ausgewählten Operanden angegebenen Wert.
  ◦ Der Operandenwert enthält den für den ausgewählten Operanden bereitgestellten Wert

- Wert

  Das Wertefeld ändert sich je nach ausgewähltem Operanden.

Beispiel einer Gruppenregel mit Bedingungen

Betrachten Sie eine Bedingungsgruppe für ein Volume mit den folgenden zwei Bedingungen:

- Name enthält „`vol`“
- Der SVM-Name lautet „`data_svm`“

Diese Bedingungsgruppe wählt alle Volumes aus, deren Namen „`vol`“ enthalten und die auf SVMs mit dem

Namen „data_svm“ gehostet werden.

Bedingungsgruppen

Bedingungsgruppen werden mithilfe eines logischen ODER ausgeführt und dann auf Speicherobjekte angewendet. Um in eine Gruppe aufgenommen zu werden, müssen die Speicherobjekte eine der Bedingungsgruppen erfüllen. Die Lagerobjekte aller Konditionsgruppen werden zusammengefasst. Mithilfe von Bedingungsgruppen können Sie den Umfang der in eine Gruppe aufzunehmenden Speicherobjekte erweitern.

Beispiel einer Gruppenregel mit Bedingungsgruppen

Betrachten Sie zwei Bedingungsgruppen für ein Volume, wobei jede Gruppe die folgenden zwei Bedingungen enthält:

- Bedingungsgruppe 1
  - Name enthält „vol“
  - Der SVM-Name lautet „data_svm“. Bedingungsgruppe 1 wählt alle Volumes aus, deren Namen „vol“ enthalten und die auf SVMs mit dem Namen „data_svm“ gehostet werden.
- Bedingungsgruppe 2
  - Name enthält „vol“
  - Der Annotationswert von data-priority ist „critical“. Bedingungsgruppe 2 wählt alle Volumes aus, deren Namen „vol“ enthalten und die mit dem Annotationswert data-priority als „critical“ annotiert sind.

Wenn eine Gruppenregel, die diese beiden Bedingungsgruppen enthält, auf Speicherobjekte angewendet wird, werden die folgenden Speicherobjekte zu einer ausgewählten Gruppe hinzugefügt:

- Alle Volumes, deren Namen „vol“ enthalten und die auf der SVM mit dem Namen „data_svm“ gehostet werden.
- Alle Datenträger, deren Namen „vol“ enthalten und die mit dem Datenprioritätsannotationswert „critical“ annotiert sind.

So funktionieren Gruppenaktionen bei Speicherobjekten

Eine Gruppenaktion ist ein Vorgang, der für alle Speicherobjekte in einer Gruppe ausgeführt wird. Sie können beispielsweise die Aktion „Volume-Schwellenwertgruppe“ so konfigurieren, dass die Volume-Schwellenwerte aller Volumes in einer Gruppe gleichzeitig geändert werden.

Gruppen unterstützen eindeutige Gruppenaktionstypen. Sie können eine Gruppe mit nur einem Gruppenaktionstyp für den Volume-Integritätsschwellenwert haben. Sie können jedoch für dieselbe Gruppe einen anderen Gruppenaktionstyp konfigurieren, sofern verfügbar. Der Rang einer Gruppenaktion bestimmt die Reihenfolge, in der die Aktion auf Speicherobjekte angewendet wird. Die Detailseite eines Speicherobjekts bietet Informationen darüber, welche Gruppenaktion auf das Speicherobjekt angewendet wird.

Beispiel für einzigartige Gruppenaktionen

Stellen Sie sich ein Volume A vor, das zu den Gruppen G1 und G2 gehört. Für diese Gruppen sind die folgenden Volume-Integritätsschwellenwert-Gruppenaktionen konfiguriert:

- `Change_capacity_threshold`Gruppenaktion mit Rang 1, zur Konfiguration der Kapazität des Volumes
- `Change_snapshot_copies`Gruppenaktion mit Rang 2, zum Konfigurieren der Snapshot-Kopien des Volumes

Der `Change_capacity_threshold` Gruppenaktionen haben immer Vorrang vor der `Change_snapshot_copies` Gruppenaktion und wird auf Volume A angewendet. Wenn Unified Manager einen Überwachungszyklus abschließt, werden die mit dem Integritätsschwellenwert verbundenen Ereignisse von Volume A gemäß der `Change_capacity_threshold` Gruppenaktion. Sie können für die Gruppenaktionen G1 und G2 keinen anderen Volumenschwellenwerttyp konfigurieren.

Gruppen hinzufügen

Sie können Gruppen erstellen, um Cluster, Volumes und virtuelle Speichermaschinen (SVMs) zur einfacheren Verwaltung zu kombinieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können Gruppenregeln definieren, um Mitglieder zur Gruppe hinzuzufügen oder daraus zu entfernen und um Gruppenaktionen für die Gruppe zu ändern.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppen** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Gruppe hinzufügen** einen Namen und eine Beschreibung für die Gruppe ein.
4. Klicken Sie auf **Hinzufügen**.

Gruppen bearbeiten

Sie können den Namen und die Beschreibung einer Gruppe bearbeiten, die Sie in Unified Manager erstellt haben.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn Sie eine Gruppe bearbeiten, um den Namen zu aktualisieren, müssen Sie einen eindeutigen Namen angeben. Sie können keinen vorhandenen Gruppennamen verwenden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppen** die Gruppe aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Gruppe bearbeiten** den Namen, die Beschreibung oder beides für die Gruppe.
4. Klicken Sie auf **Speichern**.

Gruppen löschen

Sie können eine Gruppe aus Unified Manager löschen, wenn die Gruppe nicht mehr benötigt wird.

Bevor Sie beginnen

- Keines der Speicherobjekte (Cluster, SVMs oder Volumes) darf einer Gruppenregel zugeordnet sein, die der Gruppe zugeordnet ist, die Sie löschen möchten.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppen** die Gruppe aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang mit einem Klick auf **Ja**.

   Durch das Löschen einer Gruppe werden die mit der Gruppe verknüpften Gruppenaktionen nicht gelöscht. Die Zuordnung dieser Gruppenaktionen wird jedoch aufgehoben, nachdem die Gruppe gelöscht wurde.

Gruppenregeln hinzufügen

Sie können Gruppenregeln für eine Gruppe erstellen, um Speicherobjekte wie Volumes, Cluster oder Storage Virtual Machines (SVMs) dynamisch zur Gruppe hinzuzufügen. Sie müssen mindestens eine Bedingungsgruppe mit mindestens einer Bedingung konfigurieren, um eine Gruppenregel zu erstellen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Aktuell überwachte Speicherobjekte werden hinzugefügt, sobald die Gruppenregel erstellt wird. Neue Objekte werden erst nach Abschluss des Überwachungszyklus hinzugefügt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Gruppenregel hinzufügen** einen Namen für die Gruppenregel an.
4. Wählen Sie im Feld **Zielobjekttyp** den Typ des Speicherobjekts aus, das Sie gruppieren möchten.
5. Wählen Sie im Feld **Gruppe** die gewünschte Gruppe aus, für die Sie Gruppenregeln erstellen möchten.
6. Führen Sie im Abschnitt **Bedingungen** die folgenden Schritte aus, um eine Bedingung, eine Bedingungsgruppe oder beides zu erstellen:

Erstellen….	Machen Sie Folgendes…
Eine Bedingung	a. Wählen Sie einen Operanden aus der Operandenliste aus. b. Wählen Sie als Operator entweder **Enthält** oder **Ist** aus. c. Geben Sie einen Wert ein oder wählen Sie einen Wert aus der verfügbaren Liste aus.

Erstellen….	Machen Sie Folgendes…
Eine Bedingungsgruppe	a. Klicken Sie auf **Bedingungsgruppe hinzufügen** b. Wählen Sie einen Operanden aus der Operandenliste aus. c. Wählen Sie als Operator entweder **Enthält** oder **Ist** aus. d. Geben Sie einen Wert ein oder wählen Sie einen Wert aus der verfügbaren Liste aus. e. Klicken Sie auf **Bedingung hinzufügen**, um bei Bedarf weitere Bedingungen zu erstellen, und wiederholen Sie die Schritte a bis d für jede Bedingung.

7. Klicken Sie auf **Hinzufügen**.

Beispiel zum Erstellen einer Gruppenregel

Führen Sie im Dialogfeld „Gruppenregel hinzufügen“ die folgenden Schritte aus, um eine Gruppenregel zu erstellen, einschließlich der Konfiguration einer Bedingung und des Hinzufügens einer Bedingungsgruppe:

Schritte

1. Geben Sie einen Namen für die Gruppenregel an.
2. Wählen Sie als Objekttyp „Storage Virtual Machine“ (SVM) aus.
3. Wählen Sie eine Gruppe aus der Gruppenliste aus.
4. Wählen Sie im Abschnitt „Bedingungen“ als Operanden „**Objektname**“ aus.
5. Wählen Sie als Operator **Enthält** aus.
6. Geben Sie den Wert als `svm_data` .
7. Klicken Sie auf **Bedingungsgruppe hinzufügen**.
8. Wählen Sie als Operand **Objektname**.
9. Wählen Sie als Operator **Enthält** aus.
10. Geben Sie den Wert als `vol` .
11. Klicken Sie auf **Bedingung hinzufügen**.
12. Wiederholen Sie die Schritte 8 bis 10, indem Sie in Schritt 8 **data-priority** als Operanden, in Schritt 9 **Is** als Operator und in Schritt 10 **critical** als Wert auswählen.
13. Klicken Sie auf **Hinzufügen**, um die Bedingung für die Gruppenregel zu erstellen.

Gruppenregeln bearbeiten

Sie können Gruppenregeln bearbeiten, um die Bedingungsgruppen und die Bedingungen innerhalb einer Bedingungsgruppe zu ändern und so Speicherobjekte zu einer bestimmten Gruppe hinzuzufügen oder daraus zu entfernen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppenregeln** die Gruppenregel aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Gruppenregel bearbeiten** den Gruppenregelnamen, den zugehörigen Gruppennamen, die Bedingungsgruppen und die Bedingungen nach Bedarf.

   Sie können den Zielobjekttyp für eine Gruppenregel nicht ändern.

4. Klicken Sie auf **Speichern**.

Gruppenregeln löschen

Sie können eine Gruppenregel aus Active IQ Unified Manager löschen, wenn die Gruppenregel nicht mehr benötigt wird.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn eine Gruppenregel gelöscht wird, werden die zugehörigen Speicherobjekte aus der Gruppe entfernt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppenregeln** die Gruppenregel aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang mit einem Klick auf **Ja**.

Gruppenaktionen hinzufügen

Sie können Gruppenaktionen konfigurieren, die Sie auf Speicherobjekte in einer Gruppe anwenden möchten. Durch das Konfigurieren von Aktionen für eine Gruppe können Sie Zeit sparen, da Sie diese Aktionen nicht jedem Objekt einzeln hinzufügen müssen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenaktionen** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Gruppenaktion hinzufügen** einen Namen und eine Beschreibung für die Aktion ein.
4. Wählen Sie im Menü **Gruppe** eine Gruppe aus, für die Sie die Aktion konfigurieren möchten.
5. Wählen Sie im Menü **Aktionstyp** einen Aktionstyp aus.

   Das Dialogfeld wird erweitert und ermöglicht Ihnen, den ausgewählten Aktionstyp mit den erforderlichen Parametern zu konfigurieren.

6. Geben Sie entsprechende Werte für die erforderlichen Parameter ein, um eine Gruppenaktion zu konfigurieren.
7. Klicken Sie auf **Hinzufügen**.

Gruppenaktionen bearbeiten

Sie können die Gruppenaktionsparameter bearbeiten, die Sie in Unified Manager konfiguriert haben, z. B. den Gruppenaktionsnamen, die Beschreibung, den zugehörigen Gruppennamen und die Parameter des Aktionstyps.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppenaktionen** die Gruppenaktion aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Gruppenaktion bearbeiten** den Gruppenaktionsnamen, die Beschreibung, den zugehörigen Gruppennamen und die Parameter des Aktionstyps nach Bedarf.
4. Klicken Sie auf **Speichern**.

Konfigurieren von Volume-Integritätsschwellenwerten für Gruppen

Sie können Volume-Integritätsschwellenwerte auf Gruppenebene für Kapazität, Snapshot-Kopien, Qtree-Kontingente, Wachstum und Inodes konfigurieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Der Gruppenaktionstyp „Volume-Integritätsschwelle“ wird nur auf Volumes einer Gruppe angewendet.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenaktionen** auf **Hinzufügen**.
3. Geben Sie einen Namen und eine Beschreibung für die Gruppenaktion ein.
4. Wählen Sie aus der Dropdown-Liste **Gruppe** eine Gruppe aus, für die Sie eine Gruppenaktion konfigurieren möchten.
5. Wählen Sie **Aktionstyp** als Schwellenwert für die Volumeintegrität aus.
6. Wählen Sie die Kategorie aus, für die Sie den Schwellenwert festlegen möchten.
7. Geben Sie die erforderlichen Werte für den Integritätsschwellenwert ein.
8. Klicken Sie auf **Hinzufügen**.

Gruppenaktionen löschen

Sie können eine Gruppenaktion aus Unified Manager löschen, wenn die Gruppenaktion nicht mehr benötigt wird.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn Sie die Gruppenaktion für den Volume-Integritätsschwellenwert löschen, werden globale Schwellenwerte auf die Speicherobjekte in dieser Gruppe angewendet. Auf Objektebene festgelegte Integritätsschwellenwerte für das Speicherobjekt sind hiervon nicht betroffen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Wählen Sie auf der Registerkarte **Gruppenaktionen** die Gruppenaktion aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Bestätigen Sie im Dialogfeld **Warnung** den Löschvorgang mit einem Klick auf **Ja**.

Gruppenaktionen neu anordnen

Sie können die Reihenfolge der Gruppenaktionen ändern, die auf die Speicherobjekte in einer Gruppe angewendet werden sollen. Gruppenaktionen werden auf Speicherobjekte nacheinander basierend auf ihrem Rang angewendet. Der niedrigste Rang wird der Gruppenaktion zugewiesen, die Sie zuletzt konfiguriert haben. Sie können den Rang der Gruppenaktion je nach Ihren Anforderungen ändern.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können entweder eine einzelne Zeile oder mehrere Zeilen auswählen und dann mehrere Drag-and-Drop-Vorgänge durchführen, um den Rang der Gruppenaktionen zu ändern. Sie müssen die Änderungen jedoch speichern, damit die Neupriorisierung im Gruppenaktionsraster angezeigt wird.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Gruppen**.
2. Klicken Sie auf der Registerkarte **Gruppenaktionen** auf **Neu anordnen**.
3. Ziehen Sie im Dialogfeld **Gruppenaktionen neu anordnen** die Zeilen per Drag & Drop, um die Reihenfolge der Gruppenaktionen nach Bedarf neu anzuordnen.
4. Klicken Sie auf **Speichern**.

Priorisieren Sie Speicherobjektereignisse mithilfe von Anmerkungen

Sie können Anmerkungsregeln erstellen und auf Speicherobjekte anwenden, sodass Sie diese Objekte basierend auf der Art der angewendeten Anmerkung und ihrer Priorität identifizieren und filtern können.

Erfahren Sie mehr über Anmerkungen

Wenn Sie die Konzepte zu Anmerkungen verstehen, können Sie die Ereignisse im Zusammenhang mit den Speicherobjekten in Ihrer Umgebung besser verwalten.

Was sind Anmerkungen

Eine Anmerkung ist eine Textzeichenfolge (der Name), die einer anderen

Textzeichenfolge (dem Wert) zugewiesen wird. Jedes Annotation-Name-Wert-Paar kann mithilfe von Annotationsregeln dynamisch mit Speicherobjekten verknüpft werden. Wenn Sie Speicherobjekte mit vordefinierten Anmerkungen verknüpfen, können Sie die damit verbundenen Ereignisse filtern und anzeigen. Sie können Anmerkungen auf Cluster, Volumes und virtuelle Speichermaschinen (SVMs) anwenden.

Jeder Annotationsname kann mehrere Werte haben; jedes Name-Wert-Paar kann über Regeln mit einem Speicherobjekt verknüpft werden.

Sie können beispielsweise eine Annotation mit dem Namen „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 einem Volume v1, das mit „data-center“ gekennzeichnet ist, eine Warnung generiert wird, gibt die generierte E-Mail den Speicherort des Volumes, „Boston“, an, sodass Sie das Problem priorisieren und beheben können.

So funktionieren Anmerkungsregeln in Unified Manager

Eine Annotationsregel ist ein von Ihnen definiertes Kriterium zum Annotieren von Speicherobjekten (Volumes, Clustern oder Storage Virtual Machines (SVMs)). Sie können zum Definieren von Anmerkungsregeln entweder Bedingungsgruppen oder Bedingungen verwenden.

- Sie müssen einer Anmerkung eine Anmerkungsregel zuordnen.
- Sie müssen einer Anmerkungsregel einen Objekttyp zuordnen. Einer Anmerkungsregel kann nur ein Objekttyp zugeordnet werden.
- Unified Manager fügt nach jedem Überwachungszyklus oder beim Erstellen, Bearbeiten, Löschen oder Neuordnen einer Regel Anmerkungen zu Speicherobjekten hinzu oder entfernt sie.
- Eine Anmerkungsregel kann eine oder mehrere Bedingungsgruppen haben und jede Bedingungsgruppe kann eine oder mehrere Bedingungen haben.
- Speicherobjekte können mehrere Anmerkungen haben. 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 haben. Sie können alle definierten Bedingungsgruppen in einer Annotationsregel einer Annotation anwenden, um Speicherobjekte zu annotieren.

Bedingungen innerhalb einer Bedingungsgruppe werden mit einem logischen UND ausgeführt. Alle Bedingungen einer Bedingungsgruppe müssen erfüllt sein. Wenn Sie eine Anmerkungsregel erstellen oder ändern, wird eine Bedingung erstellt, die nur diejenigen Speicherobjekte anwendet, auswählt und mit Anmerkungen versieht, die alle Bedingungen in der Bedingungsgruppe erfüllen. Sie können mehrere Bedingungen innerhalb einer Bedingungsgruppe verwenden, wenn Sie den Umfang der zu kommentierenden Speicherobjekte eingrenzen möchten.

Sie können Bedingungen mit Speicherobjekten erstellen, indem Sie die folgenden Operanden und Operatoren verwenden und den erforderlichen Wert angeben.

Speicherobjekttyp	Anwendbare Operanden
Volumen	• Objektname • Name des besitzenden Clusters • Name des besitzenden SVM • Anmerkungen
SVM	• Objektname • Name des besitzenden Clusters • Anmerkungen
Cluster	• Objektname • Anmerkungen

Wenn Sie eine Annotation als Operand für ein beliebiges Speicherobjekt auswählen, ist der Operator „Ist“ verfügbar. Für alle anderen Operanden können Sie als Operator entweder „Ist“ oder „Enthält“ auswählen. Wenn Sie den Operator „Ist“ auswählen, wird die Bedingung auf eine genaue Übereinstimmung des Operandenwerts mit dem für den ausgewählten Operanden bereitgestellten Wert ausgewertet. Wenn Sie den Operator „Enthält“ auswählen, wird die Bedingung ausgewertet, um eines der folgenden Kriterien zu erfüllen:

- Der Operandenwert entspricht genau dem Wert des ausgewählten Operanden.
- Der Operandenwert enthält den für den ausgewählten Operanden bereitgestellten Wert.

Beispiel einer Annotationsregel mit Bedingungen

Betrachten Sie eine Anmerkungsregel mit einer Bedingungsgruppe für ein Volume mit den folgenden zwei Bedingungen:

- Name enthält „`vol`“
- Der SVM-Name lautet „`data_svm`“

Diese Annotationsregel versieht alle Volumes, deren Namen „`vol`“ enthalten und die auf SVMs mit dem Namen „`data_svm`“ gehostet werden, mit der ausgewählten Annotation und dem Annotationstyp.

Bedingungsgruppen

Bedingungsgruppen werden mithilfe eines logischen ODER ausgeführt und dann auf Speicherobjekte angewendet. Um annotiert zu werden, müssen die Speicherobjekte die Anforderungen einer der Bedingungsgruppen erfüllen. Die Speicherobjekte, die die Bedingungen aller Bedingungsgruppen erfüllen, werden annotiert. Mithilfe von Bedingungsgruppen können Sie den Umfang der zu annotierenden Speicherobjekte erweitern.

Beispiel einer Annotationsregel mit Bedingungsgruppen

Betrachten Sie eine Anmerkungsregel mit zwei Bedingungsgruppen für ein Volume. Jede Gruppe enthält die folgenden zwei Bedingungen:

- Bedingungsgruppe 1

    - Name enthält „vol“
    - Der SVM-Name lautet „data_svm“. Diese Bedingungsgruppe kommentiert alle Volumes, deren Namen „vol“ enthalten und die auf SVMs mit dem Namen „data_svm“ gehostet werden.
- Bedingungsgruppe 2
    - Name enthält „vol“
    - Der Annotationswert von data-priority ist „critical“. Diese Bedingungsgruppe annotiert alle Volumes, deren Namen „vol“ enthalten und die mit dem Annotationswert data-priority als „critical“ annotiert sind.

Wenn eine Annotationsregel, die diese beiden Bedingungsgruppen enthält, auf Speicherobjekte angewendet wird, werden die folgenden Speicherobjekte annotiert:

- Alle Volumes, deren Namen „vol“ enthalten und die auf SVM mit dem Namen „data_svm“ gehostet werden.
- Alle Datenträger, deren Name „vol“ enthält und die mit dem Datenprioritätsannotationswert „critical“ annotiert sind.

Beschreibung vordefinierter Annotationswerte

Datenpriorität ist eine vordefinierte Anmerkung mit den Werten „Missionskritisch“, „Hoch“ und „Niedrig“. Mit diesen Werten können Sie Speicherobjekte basierend auf der Priorität der darin enthaltenen Daten mit Anmerkungen versehen. Sie können die vordefinierten Anmerkungswerte weder bearbeiten noch löschen.

- **Datenpriorität:Missionskritisch**

  Diese Annotation wird auf Speicherobjekte angewendet, die unternehmenskritische Daten enthalten. Beispielsweise können Objekte, die Produktionsanwendungen enthalten, als unternehmenskritisch betrachtet werden.

- **Datenpriorität: Hoch**

  Diese Annotation wird auf Speicherobjekte angewendet, die Daten mit hoher Priorität enthalten. Beispielsweise können Objekte, die Geschäftsanwendungen hosten, als Objekte mit hoher Priorität betrachtet werden.

- **Datenpriorität: Niedrig**

  Diese Annotation wird auf Speicherobjekte angewendet, die Daten mit niedriger Priorität enthalten. Beispielsweise können Objekte, die sich auf sekundären Speicherorten wie Sicherungs- und Spiegelzielen befinden, eine niedrige Priorität haben.

Anmerkungen dynamisch hinzufügen

Wenn Sie benutzerdefinierte Anmerkungen erstellen, verknüpft Unified Manager mithilfe von Regeln dynamisch Cluster, virtuelle Speichermaschinen (SVMs) und Volumes mit den Anmerkungen. Diese Regeln ordnen die Anmerkungen automatisch Speicherobjekten zu.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Klicken Sie auf der Seite **Anmerkungen** auf **Anmerkung hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkung hinzufügen** einen Namen und eine Beschreibung für die Anmerkung ein.
4. Optional: Klicken Sie im Abschnitt **Annotationswerte** auf **Hinzufügen**, um der Annotation Werte hinzuzufügen.
5. Klicken Sie auf **Speichern**.

Hinzufügen von Werten zu Anmerkungen

Sie können Anmerkungen Werte hinzufügen und dann Speicherobjekte mit einem bestimmten Name-Wert-Paar aus Anmerkungen verknüpfen. Durch das Hinzufügen von Werten zu Anmerkungen können Sie Speicherobjekte effektiver verwalten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können vordefinierten Anmerkungen keine Werte hinzufügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Wählen Sie auf der Seite **Anmerkungen** die Anmerkung aus, der Sie einen Wert hinzufügen möchten, und klicken Sie dann im Abschnitt **Werte** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkungswert hinzufügen** einen Wert für die Anmerkung an.

   Der von Ihnen angegebene Wert muss für die ausgewählte Anmerkung eindeutig sein.

4. Klicken Sie auf **Hinzufügen**.

Anmerkungen löschen

Sie können benutzerdefinierte Anmerkungen und ihre Werte löschen, wenn sie nicht mehr benötigt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Die Annotationswerte dürfen nicht in anderen Annotationen oder Gruppenregeln verwendet werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungen** die Anmerkung aus, die Sie löschen möchten.

   Die Details der ausgewählten Anmerkung werden angezeigt.

3. Klicken Sie auf **Aktionen** > **Löschen**, um die ausgewählte Anmerkung und ihren Wert zu löschen.

4. Klicken Sie im Warndialogfeld auf **Ja**, um den Löschvorgang zu bestätigen.

Anzeigen der Anmerkungsliste und Details

Sie können die Liste der Anmerkungen anzeigen, die dynamisch mit Clustern, Volumes und virtuellen Speichermaschinen (SVMs) verknüpft sind. Sie können auch Details wie die Beschreibung, den Ersteller, das Erstellungsdatum, Werte, Regeln und die mit der Anmerkung verknüpften Objekte anzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungen** auf den Namen der Anmerkung, um die zugehörigen Details anzuzeigen.

Werte aus Anmerkungen löschen

Sie können mit benutzerdefinierten Anmerkungen verknüpfte Werte löschen, wenn dieser Wert nicht mehr auf die Anmerkung zutrifft.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Der Annotationswert darf keinen Annotationsregeln oder Gruppenregeln zugeordnet sein.

Sie können keine Werte aus vordefinierten Anmerkungen löschen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Wählen Sie in der Anmerkungsliste auf der Registerkarte **Anmerkungen** die Anmerkung aus, aus der Sie einen Wert löschen möchten.
3. Wählen Sie im Bereich **Werte** der Registerkarte **Anmerkungen** den Wert aus, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
4. Klicken Sie im Dialogfeld **Warnung** auf **Ja**.

   Der Wert wird gelöscht und nicht mehr in der Werteliste der ausgewählten Annotation angezeigt.

Erstellen von Anmerkungsregeln

Sie können Anmerkungsregeln erstellen, die Unified Manager verwendet, um Speicherobjekte wie Volumes, Cluster oder Storage Virtual Machines (SVMs) dynamisch zu annotieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Speicherobjekte, die derzeit überwacht werden, werden mit Anmerkungen versehen, sobald die Anmerkungsregel erstellt wird. Neue Objekte werden erst nach Abschluss des Überwachungszyklus annotiert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Annotationsregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkungsregel hinzufügen** einen Namen für die Anmerkungsregel an.
4. Wählen Sie im Feld **Zielobjekttyp** den Typ des Speicherobjekts aus, das Sie mit Anmerkungen versehen möchten.
5. Wählen Sie in den Feldern **Anmerkung anwenden** die Anmerkung und den Anmerkungswert aus, die Sie verwenden möchten.
6. Führen Sie im Abschnitt „Bedingungen“ die entsprechende Aktion aus, um eine Bedingung, eine Bedingungsgruppe oder beides zu erstellen:

Erstellen…	Machen Sie Folgendes…
Eine Bedingung	a. Wählen Sie einen Operanden aus der Operandenliste aus. b. Wählen Sie als Operator entweder **Enthält** oder **Ist** aus. c. Geben Sie einen Wert ein oder wählen Sie einen Wert aus der verfügbaren Liste aus.
Eine Bedingungsgruppe	a. Klicken Sie auf **Bedingungsgruppe hinzufügen**. b. Wählen Sie einen Operanden aus der Operandenliste aus. c. Wählen Sie als Operator entweder **Enthält** oder **Ist** aus. d. Geben Sie einen Wert ein oder wählen Sie einen Wert aus der verfügbaren Liste aus. e. Klicken Sie auf **Bedingung hinzufügen**, um bei Bedarf weitere Bedingungen zu erstellen, und wiederholen Sie die Schritte a bis d für jede Bedingung.

7. Klicken Sie auf **Hinzufügen**.

Beispiel für das Erstellen einer Anmerkungsregel

Führen Sie im Dialogfeld „Anmerkungsregel hinzufügen“ die folgenden Schritte aus, um eine Anmerkungsregel zu erstellen, einschließlich der Konfiguration einer Bedingung und des Hinzufügens einer Bedingungsgruppe:

Schritte

1. Geben Sie einen Namen für die Anmerkungsregel an.
2. Wählen Sie als Zielobjekttyp „Storage Virtual Machine“ (SVM) aus.
3. Wählen Sie eine Anmerkung aus der Anmerkungsliste aus und geben Sie einen Wert an.
4. Wählen Sie im Abschnitt „Bedingungen“ als Operanden „**Objektname**“ aus.
5. Wählen Sie als Operator **Enthält** aus.

6. Geben Sie den Wert als `svm_data` .
7. Klicken Sie auf **Bedingungsgruppe hinzufügen**.
8. Wählen Sie als Operand **Objektname**.
9. Wählen Sie als Operator **Enthält** aus.
10. Geben Sie den Wert als `vol` .
11. Klicken Sie auf **Bedingung hinzufügen**.
12. Wiederholen Sie die Schritte 8 bis 10, indem Sie in Schritt 8 **data-priority** als Operanden, in Schritt 9 **Is** als Operator und in Schritt 10 **mission-critical** als Wert auswählen.
13. Klicken Sie auf **Hinzufügen**.

Fügen Sie einzelnen Speicherobjekten manuell Anmerkungen hinzu

Sie können ausgewählte Volumes, Cluster und SVMs manuell mit Anmerkungen versehen, ohne Anmerkungsregeln zu verwenden. Sie können ein einzelnes Speicherobjekt oder mehrere Speicherobjekte mit Anmerkungen versehen und die erforderliche Name-Wert-Paarkombination für die Anmerkung angeben.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Navigieren Sie zu den Speicherobjekten, die Sie mit Anmerkungen versehen möchten:

So fügen Sie eine Anmerkung hinzu zu…	Machen Sie Folgendes…
Cluster	a. Klicken Sie auf **Speicher** > **Cluster**. b. Wählen Sie einen oder mehrere Cluster aus.
Bände	a. Klicken Sie auf **Speicher** > **Volumes**. b. Wählen Sie ein oder mehrere Volumes aus.
SVMs	a. Klicken Sie auf **Speicher** > **SVMs**. b. Wählen Sie eine oder mehrere SVMs aus.

2. Klicken Sie auf **Kommentieren** und wählen Sie ein Name-Wert-Paar aus.
3. Klicken Sie auf **Übernehmen**.

Bearbeiten von Anmerkungsregeln

Sie können Anmerkungsregeln bearbeiten, um die Bedingungsgruppen und Bedingungen innerhalb der Bedingungsgruppe zu ändern und so Anmerkungen zu Speicherobjekten hinzuzufügen oder daraus zu entfernen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Anmerkungen werden von Speicherobjekten getrennt, wenn Sie die zugehörigen Anmerkungsregeln bearbeiten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungsregeln** die Anmerkungsregel aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Aktionen** > **Bearbeiten**.
3. Ändern Sie im Dialogfeld **Anmerkungsregel bearbeiten** den Regelnamen, den Anmerkungsnamen und -wert, die Bedingungsgruppen und die Bedingungen nach Bedarf.

   Sie können den Zielobjekttyp für eine Anmerkungsregel nicht ändern.

4. Klicken Sie auf **Speichern**.

Konfigurieren von Bedingungen für Anmerkungsregeln

Sie können eine oder mehrere Bedingungen konfigurieren, um Anmerkungsregeln zu erstellen, die Unified Manager auf die Speicherobjekte anwendet. Die Speicherobjekte, die die Annotationsregel erfüllen, werden mit dem in der Regel angegebenen Wert annotiert.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Annotationsregeln** auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Anmerkungsregel hinzufügen** einen Namen für die Regel ein.
4. Wählen Sie einen Objekttyp aus der Liste „Zielobjekttyp“ und wählen Sie dann einen Anmerkungsnamen und -wert aus der Liste aus.
5. Wählen Sie im Abschnitt **Bedingungen** des Dialogfelds einen Operanden und einen Operator aus der Liste aus und geben Sie einen Bedingungswert ein oder klicken Sie auf **Bedingung hinzufügen**, um eine neue Bedingung zu erstellen.
6. Klicken Sie auf **Speichern und hinzufügen**.

Beispiel für die Konfiguration einer Bedingung für eine Anmerkungsregel

Betrachten Sie eine Bedingung für den Objekttyp SVM, bei der der Objektname „`svm_data`“ enthält.

Führen Sie im Dialogfeld „Anmerkungsregel hinzufügen“ die folgenden Schritte aus, um die Bedingung zu konfigurieren:

Schritte

1. Geben Sie einen Namen für die Anmerkungsregel ein.
2. Wählen Sie als Zielobjekttyp SVM aus.
3. Wählen Sie eine Anmerkung aus der Liste der Anmerkungen und einen Wert aus.
4. Wählen Sie im Feld **Bedingungen** als Operanden **Objektname** aus.

5. Wählen Sie als Operator **Enthält** aus.
6. Geben Sie den Wert als `svm_data` .
7. Klicken Sie auf **Hinzufügen**.

Annotationsregeln löschen

Sie können Anmerkungsregeln aus Active IQ Unified Manager löschen, wenn die Regeln nicht mehr benötigt werden.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Wenn Sie eine Anmerkungsregel löschen, wird die Anmerkung getrennt und aus den Speicherobjekten entfernt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Wählen Sie auf der Registerkarte **Anmerkungsregeln** die Anmerkungsregel aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie im Dialogfeld **Warnung** auf **Ja**, um das Löschen zu bestätigen.

Neuordnen von Anmerkungsregeln

Sie können die Reihenfolge ändern, in der Unified Manager Anmerkungsregeln auf Speicherobjekte anwendet. Annotationsregeln werden auf Speicherobjekte sequenziell basierend auf ihrem Rang angewendet. Wenn Sie eine Anmerkungsregel konfigurieren, ist der Rang am niedrigsten. Sie können den Rang der Anmerkungsregel jedoch je nach Ihren Anforderungen ändern.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können entweder eine einzelne Zeile oder mehrere Zeilen auswählen und viele Drag-and-Drop-Vorgänge durchführen, um den Rang der Anmerkungsregeln zu ändern. Sie müssen die Änderungen jedoch speichern, damit die Neupriorisierung auf der Registerkarte „Anmerkungsregeln“ angezeigt wird.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Anmerkungen**.
2. Klicken Sie auf der Registerkarte **Anmerkungsregeln** auf **Neu anordnen**.
3. Im Dialogfeld **Anmerkungsregel neu anordnen** können Sie per Drag & Drop einzelne oder mehrere Zeilen verschieben, um die Reihenfolge der Anmerkungsregeln neu anzuordnen.
4. Klicken Sie auf **Speichern**.

   Damit die Nachbestellung angezeigt wird, müssen Sie die Änderungen speichern.

Senden Sie ein Support-Paket über die Web-Benutzeroberfläche und die Wartungskonsole

Sie sollten ein Supportpaket senden, wenn Ihr Problem eine detailliertere Diagnose und Fehlerbehebung erfordert, als eine AutoSupport -Nachricht bietet. Sie können über die Web-Benutzeroberfläche und Wartungskonsole von Unified Manager ein Support-Paket an den technischen Support senden.

Unified Manager speichert maximal zwei vollständige Support-Pakete und drei leichte Support-Pakete gleichzeitig.

Verwandte Informationen

"Unified Manager-Benutzerrollen und -Funktionen"

Senden Sie AutoSupport -Nachrichten und Support-Pakete an den technischen Support

Auf der AutoSupport -Seite können Sie vordefinierte und On-Demand AutoSupport Nachrichten an Ihr technisches Supportteam senden, um einen ordnungsgemäßen Betrieb Ihrer Umgebung sicherzustellen und Sie bei der Aufrechterhaltung 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 zum Unified Manager-Server in einer Nachricht senden, den regelmäßigen Versand einer Nachricht planen oder sogar Supportpakete erstellen und an das technische Supportteam senden.

> Ein Benutzer mit der Rolle eines Speicheradministrators kann bei Bedarf AutoSupport Nachrichten und Supportpakete generieren und an den technischen Support senden. Allerdings kann nur ein Administrator oder Wartungsbenutzer den regelmäßigen AutoSupport aktivieren oder deaktivieren und die HTTP-Einstellungen wie im Abschnitt „Einrichten des HTTP-Proxyservers“ beschrieben konfigurieren. In einer Umgebung, in der ein HTTP-Proxyserver verwendet werden muss, sollte die Konfiguration abgeschlossen sein, bevor ein Speicheradministrator On-Demand- AutoSupport Nachrichten und Support-Pakete an den technischen Support senden kann.

Senden Sie AutoSupport -Nachrichten auf Abruf

Sie können eine On-Demand-Nachricht generieren und an den technischen Support oder an einen angegebenen E-Mail-Empfänger oder an beide senden.

Schritte

1. Navigieren Sie zu **Allgemein** > * AutoSupport* und führen Sie eine oder beide der folgenden Aktionen aus:
2. Wenn Sie die AutoSupport -Nachricht an den technischen Support senden möchten, aktivieren Sie das Kontrollkästchen **An technischen Support senden**.
3. Wenn Sie die AutoSupport -Nachricht an einen bestimmten E-Mail-Empfänger senden möchten, aktivieren Sie das Kontrollkästchen **An E-Mail-Empfänger senden** und geben Sie die E-Mail-Adresse des Empfängers ein.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie auf * AutoSupport generieren und senden*.

Aktivieren Sie den regelmäßigen AutoSupport

Sie können dem technischen Support regelmäßig bestimmte, vordefinierte Nachrichten zur Problemdiagnose und -lösung senden. Diese Funktion ist standardmäßig aktiviert. Wenn deaktiviert, kann ein Administrator oder Wartungsbenutzer die Einstellungen aktivieren.

Schritte

1. Navigieren Sie zu **Allgemein** > * AutoSupport*.
2. Aktivieren Sie im Abschnitt „Periodischer AutoSupport“ das Kontrollkästchen **Regelmäßiges Senden von AutoSupport -Daten an Active IQ aktivieren**.
3. Definieren Sie bei Bedarf den Namen, den Port und die Authentifizierungsinformationen für den HTTP-Proxyserver, wie im Abschnitt „Einrichten des HTTP-Proxyservers“ beschrieben.
4. Klicken Sie auf **Speichern**.

Laden Sie ein On-Demand-Supportpaket hoch

Sie können je nach Bedarf zur Fehlerbehebung ein Supportpaket erstellen und an den technischen Support senden. Unified Manager speichert nur die beiden zuletzt erstellten Support-Pakete. Ältere Support-Pakete werden aus dem System gelöscht.

Da einige Supportdatentypen große Mengen an Clusterressourcen beanspruchen oder ihre Fertigstellung viel Zeit in Anspruch nehmen kann, können Sie bei Auswahl des vollständigen Supportpakets bestimmte Datentypen ein- oder ausschließen, um die Größe des Supportpakets zu reduzieren. Sie haben auch die Möglichkeit, ein einfaches Supportpaket zu erstellen, das nur 30 Tage Protokolle und Konfigurationsdatenbankeinträge enthält – Leistungsdaten, Erfassungsaufzeichnungsdateien und Server-Heap-Dumps sind davon ausgenommen.

Schritte

1. Navigieren Sie zu **Allgemein** > * AutoSupport*.
2. Klicken Sie im Abschnitt „On-Demand-Support-Paket“ auf **Support-Paket generieren und senden**.
3. Um ein Light-Support-Paket an den technischen Support zu senden, aktivieren Sie im Popup „Support-Paket generieren und senden“ das Kontrollkästchen **Light-Support-Paket generieren**.
4. Alternativ können Sie zum Senden eines vollständigen Support-Pakets das Kontrollkästchen **Vollständiges Support-Paket generieren** aktivieren. Wählen Sie die spezifischen Datentypen aus, die in das Support-Paket aufgenommen oder davon ausgeschlossen werden sollen.

   Auch wenn Sie keinen Datentyp auswählen, wird das Support-Paket dennoch mit anderen Unified Manager-Daten generiert.

5. Aktivieren Sie das Kontrollkästchen **Paket an den technischen Support senden**, um das Paket zu erstellen und an den technischen Support zu senden. Wenn Sie dieses Kontrollkästchen nicht aktivieren, wird das Paket generiert und lokal auf dem Unified Manager-Server gespeichert. Das generierte Support-Paket steht zur späteren Verwendung im Verzeichnis /support auf VMware-Systemen zur Verfügung, in `/opt/netapp/data/support/` auf Linux-Systemen und in `ProgramData\NetApp\OnCommandAppData\ocum\support` auf Windows-Systemen.
6. Klicken Sie auf **Senden**.

Einrichten eines 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 bietet. Dieser Abschnitt ist nur für

Administrator- und Wartungsbenutzer verfügbar.

- **HTTP-Proxy verwenden**

  Aktivieren Sie dieses Kontrollkästchen, um den als HTTP-Proxy verwendeten Server zu identifizieren.

  Geben Sie den Hostnamen oder die IP-Adresse des Proxyservers und die Portnummer ein, die für die Verbindung mit dem Server verwendet wird.

- **Authentifizierung verwenden**

  Aktivieren Sie dieses Kontrollkästchen, wenn Sie Authentifizierungsinformationen angeben müssen, um auf den als HTTP-Proxy verwendeten Server zuzugreifen.

  Geben Sie den Benutzernamen und das Kennwort ein, die zur Authentifizierung beim HTTP-Proxy erforderlich sind.

HTTP-Proxys, die nur eine Basisauthentifizierung bereitstellen, werden nicht unterstützt.

Zugriff auf die Wartungskonsole

Wenn die Benutzeroberfläche des Unified Managers nicht in Betrieb ist oder Sie Funktionen ausführen müssen, die in der Benutzeroberfläche nicht verfügbar sind, können Sie auf die Wartungskonsole zugreifen, um Ihr Unified Manager-System zu verwalten.

Bevor Sie beginnen

Sie müssen Unified Manager installiert und konfiguriert haben.

Nach 15 Minuten Inaktivität werden Sie von der Wartungskonsole abgemeldet.

Wenn Sie bei der Installation auf VMware bereits über die VMware-Konsole als Wartungsbenutzer angemeldet sind, können Sie sich nicht gleichzeitig über Secure Shell anmelden.

Schritt

1. Führen Sie die folgenden Schritte aus, um auf die Wartungskonsole zuzugreifen:

Auf diesem Betriebssystem …	Befolgen Sie diese Schritte…
VMware	a. Stellen Sie mithilfe von Secure Shell eine Verbindung zur IP-Adresse oder zum vollqualifizierten Domänennamen der virtuellen Unified Manager-Appliance her. b. Melden Sie sich mit Ihrem Wartungsbenutzernamen und Kennwort bei der Wartungskonsole an.

Auf diesem Betriebssystem …	Befolgen Sie diese Schritte…
Linux	a. Stellen Sie mithilfe von Secure Shell eine Verbindung zur IP-Adresse oder zum vollqualifizierten Domänennamen des Unified Manager-Systems her. b. Melden Sie sich mit dem Namen und Kennwort des Wartungsbenutzers (umadmin) beim System an. c. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.
Windows	a. Melden Sie sich mit Administratoranmeldeinformationen beim Unified Manager-System an. b. Starten Sie PowerShell als Windows-Administrator. c. Geben Sie den Befehl ein `maintenance_console` und drücken Sie die Eingabetaste.

Das Menü der Wartungskonsole von Unified Manager wird angezeigt.

Erstellen und Hochladen eines Support-Pakets

Sie können ein Support-Paket mit Diagnoseinformationen erstellen, sodass Sie es zur Hilfe bei der Fehlerbehebung an den technischen Support senden können.

Ab Unified Manager 9.8 können Sie das Support-Paket auch von der Wartungskonsole auf NetApp hochladen, wenn Ihr Unified Manager-Server mit dem Internet verbunden ist.

Bevor Sie beginnen

Sie müssen als Wartungsbenutzer Zugriff auf die Wartungskonsole haben.

Da manche Supportdatentypen große Mengen an Clusterressourcen beanspruchen oder ihre Verarbeitung viel Zeit in Anspruch nehmen kann, können Sie bei Auswahl des vollständigen Supportpakets die einzuschließenden oder auszuschließenden Datentypen angeben, um die Größe des Supportpakets zu reduzieren. Sie haben auch die Möglichkeit, ein einfaches Supportpaket zu erstellen, das nur 30 Tage Protokolle und Konfigurationsdatenbankeinträge enthält – Leistungsdaten, Erfassungsaufzeichnungsdateien und Server-Heap-Dumps sind davon ausgenommen.

Unified Manager speichert nur die beiden zuletzt erstellten Support-Pakete. Ältere Support-Pakete werden aus dem System gelöscht.

Schritte

1. Wählen Sie im **Hauptmenü** der Wartungskonsole **Support/Diagnose**.
2. Wählen Sie **Light-Support-Paket generieren** oder **Support-Paket generieren**, je nachdem, wie detailliert das Support-Paket sein soll.

3. Wenn Sie das vollständige Support-Paket auswählen, wählen Sie die folgenden Datentypen aus oder heben Sie die Auswahl auf, um sie in das Support-Paket aufzunehmen oder davon auszuschließen:

   - **Datenbank-Dump**

     Ein Dump der MySQL-Serverdatenbank.

   - **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-Paket dennoch mit anderen Unified Manager-Daten generiert.

4. Typ `g` und drücken Sie dann die Eingabetaste, um das Support-Paket zu generieren.

   Da die Generierung eines Support-Pakets ein speicherintensiver Vorgang ist, werden Sie aufgefordert zu bestätigen, dass Sie das Support-Paket zu diesem Zeitpunkt wirklich generieren möchten.

5. Typ `y` und drücken Sie dann die Eingabetaste, um das Support-Paket zu generieren.

   Wenn Sie das Support-Paket jetzt nicht generieren möchten, geben Sie `n` und drücken Sie dann die Eingabetaste.

6. Wenn Sie Datenbank-Dump-Dateien in das vollständige Support-Paket aufgenommen haben, werden Sie aufgefordert, den Zeitraum anzugeben, für den Leistungsstatistiken einbezogen werden sollen. Das Einbeziehen von Leistungsstatistiken kann viel Zeit und Speicherplatz beanspruchen. Sie können die Datenbank daher auch ohne Einbeziehen von Leistungsstatistiken sichern:

   a. Geben Sie das Startdatum im Format JJJJMMTT ein.

      Geben Sie beispielsweise `20210101` für den 1. Januar 2021. Eingeben `n` wenn Sie nicht möchten, dass Leistungsstatistiken einbezogen werden.

   b. Geben Sie die Anzahl der Tage ein, für die Statistiken ab 0:00 Uhr des angegebenen Startdatums einbezogen werden sollen.

      Sie können eine Zahl zwischen 1 und 10 eingeben.

   Wenn Sie Leistungsstatistiken einbeziehen, zeigt das System den Zeitraum an, für den Leistungsstatistiken erfasst werden.

7. Nachdem das Support-Paket erstellt wurde, werden Sie gefragt, ob Sie es zu NetApp hochladen möchten. Typ `y` und drücken Sie dann die Eingabetaste.

   Sie werden aufgefordert, Ihre Support-Fallnummer einzugeben.

8. Wenn Sie bereits eine Fallnummer haben, geben Sie die Nummer ein und drücken Sie die Eingabetaste. Andernfalls drücken Sie einfach die Eingabetaste.

Das Support-Paket wird auf NetApp hochgeladen.

Wenn Ihr Unified Manager-Server nicht mit dem Internet verbunden ist oder Sie das Support-Paket aus einem anderen Grund nicht hochladen können, können Sie es abrufen und manuell 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-Paket abzurufen.

Das generierte Support-Paket befindet sich auf VMware-Systemen im Verzeichnis /support, auf Linux-Systemen in /opt/netapp/data/support/ und auf Windows-Systemen in ProgramData\NetApp\OnCommandAppData\ocum\support.

Verwandte Informationen

"Unified Manager-Benutzerrollen und -Funktionen"

Abrufen des Support-Pakets mit einem Windows-Client

Wenn Sie ein Windows-Benutzer sind, können Sie ein Tool herunterladen und installieren, um das Support-Paket von Ihrem Unified Manager-Server abzurufen. Sie können das Support-Paket 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 auszuführen.

Sie müssen ein Tool verwenden, das SCP oder SFTP unterstützt.

Schritte

1. Laden Sie ein Tool herunter und installieren Sie es, um das Support-Paket abzurufen.
2. Öffnen Sie das Tool.
3. Stellen Sie über SFTP eine Verbindung zu Ihrem Unified Manager-Verwaltungsserver her.

   Das Tool zeigt den Inhalt des Verzeichnisses /support an und Sie können alle vorhandenen Support-Pakete anzeigen.
4. Wählen Sie das Zielverzeichnis für das Support-Paket aus, das Sie kopieren möchten.
5. Wählen Sie das Support-Paket aus, das Sie kopieren möchten, und verwenden Sie das Tool, um die Datei vom Unified Manager-Server auf Ihr lokales System zu kopieren.

Rufen Sie das Support-Paket mit einem UNIX- oder Linux-Client ab

Wenn Sie ein UNIX- oder Linux-Benutzer sind, können Sie das Support-Paket von Ihrer vApp abrufen, indem Sie die Befehlszeilenschnittstelle (CLI) auf Ihrem Linux-Clientserver verwenden. Sie können entweder SCP oder SFTP verwenden, um das Support-Paket abzurufen.

Bevor Sie beginnen

Sie müssen der Wartungsbenutzer sein, um diese Aufgabe auszuführen.

Sie müssen mithilfe der Wartungskonsole ein Support-Paket erstellt haben und über den Namen des Support-Pakets verfügen.

Schritte

1. Greifen Sie über Telnet oder die Konsole auf die CLI zu, indem Sie Ihren Linux-Clientserver verwenden.
2. Zugriff auf die/`support` Verzeichnis.
3. Rufen Sie das Support-Paket ab und kopieren Sie es mit dem folgenden Befehl in das lokale Verzeichnis:

Wenn Sie verwenden…	Verwenden Sie dann den folgenden Befehl …
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-Pakets wird Ihnen mitgeteilt, wenn Sie es mithilfe der Wartungskonsole generieren.

4. Geben Sie das Kennwort des Wartungsbenutzers ein.

Beispiele

Im folgenden Beispiel wird SCP zum Abrufen des Support-Pakets verwendet:

```
        `$ 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 zum Abrufen des Support-Pakets verwendet:

```
        `$ 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
```

Senden Sie ein Support-Paket an den technischen Support

Wenn ein Problem detailliertere Diagnose- und Fehlerbehebungsinformationen erfordert, als eine AutoSupport -Nachricht bietet, können Sie ein Support-Paket an den technischen Support senden.

Bevor Sie beginnen

Sie müssen Zugriff auf das Support-Paket haben, um es an den technischen Support senden zu können.

Sie müssen über eine Fallnummer verfügen, die über die Website des technischen Supports generiert wurde.

Schritte

1. Melden Sie sich bei der NetApp Support-Site an.
2. Laden Sie die Datei hoch.

   "So laden Sie eine Datei zu NetApp hoch"

Aufgaben und Informationen zu verschiedenen Arbeitsabläufen

Einige Aufgaben und Referenztexte, die Ihnen beim Verstehen und Abschließen eines Workflows helfen können, sind vielen Workflows in Unified Manager gemeinsam, darunter das Hinzufügen und Überprüfen von Notizen zu einem Ereignis, das Zuweisen eines Ereignisses, das Bestätigen und Auflösen von Ereignissen sowie Details zu Volumes, virtuellen Speichermaschinen (SVMs), Aggregaten usw.

Clusterkomponenten und warum sie kontrovers diskutiert werden können

Sie können Leistungsprobleme im Cluster erkennen, wenn eine Clusterkomponente in einen Konflikt gerät. Die Leistung von Workloads, die die Komponente verwenden, verlangsamt sich und ihre Antwortzeit (Latenz) für Clientanforderungen erhöht sich, was ein Ereignis in Unified Manager auslöst.

Eine Komponente, die im Streit liegt, kann nicht die optimale Leistung erbringen. Seine Leistung hat nachgelassen und die Leistung anderer Clusterkomponenten und Workloads, sogenannter *Opfer*, hat möglicherweise die Latenz erhöht. Um eine Komponente aus dem Wettbewerb zu nehmen, müssen Sie ihre Arbeitslast reduzieren oder ihre Fähigkeit erhöhen, mehr Arbeit zu bewältigen, damit die Leistung wieder auf ein normales Niveau zurückkehren kann. Da Unified Manager die Workload-Leistung in Fünf-Minuten-Intervallen erfasst und analysiert, erkennt er nur, wenn eine Clusterkomponente dauerhaft überbeansprucht wird. Vorübergehende Überlastungsspitzen, die innerhalb des Fünf-Minuten-Intervalls nur von kurzer Dauer sind, werden nicht erkannt.

Beispielsweise kann es zu einem Konflikt um ein Speicheraggregat kommen, weil eine oder mehrere Workloads darauf um die Erfüllung ihrer E/A-Anforderungen konkurrieren. Andere Arbeitslasten im Aggregat können beeinträchtigt werden, was zu einer Leistungsminderung führt. Um die Aktivität auf dem Aggregat zu reduzieren, können Sie verschiedene Schritte unternehmen, z. B. eine oder mehrere Arbeitslasten auf ein weniger ausgelastetes Aggregat oder einen weniger ausgelasteten Knoten verschieben, um die Gesamtarbeitslastanforderung an das aktuelle Aggregat zu verringern. Für eine QoS-Richtliniengruppe können Sie die Durchsatzgrenze anpassen oder Workloads in eine andere Richtliniengruppe verschieben, sodass die Workloads nicht mehr gedrosselt werden.

Unified Manager überwacht die folgenden Clusterkomponenten, um Sie zu warnen, wenn es zu Konflikten kommt:

- **Netzwerk**

  Stellt die Wartezeit von E/A-Anfragen durch die externen Netzwerkprotokolle im Cluster dar. Die Wartezeit ist die Zeit, die darauf gewartet wird, dass die „Transfer Ready“-Transaktionen abgeschlossen werden,

bevor der Cluster auf eine E/A-Anforderung antworten kann. Wenn es zu Konflikten mit der Netzwerkkomponente kommt, bedeutet dies, dass eine hohe Wartezeit auf der Protokollebene die Latenz einer 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 durchführt, hat sich möglicherweise seit der Erkennung des Ereignisses geändert. Wenn es bei der Netzwerkverarbeitungskomponente zu Konflikten kommt, bedeutet dies, dass eine hohe Auslastung des Netzwerkverarbeitungsknotens die Latenz einer oder mehrerer Arbeitslasten beeinträchtigt.

  Wenn Sie einen All-SAN-Array-Cluster in einer Aktiv-Aktiv-Konfiguration verwenden, wird der Latenzwert der Netzwerkverarbeitung für beide Knoten angezeigt, sodass Sie überprüfen können, ob die Knoten die Last gleichmäßig teilen.

- **QoS-Limit Max**

  Stellt die maximale Durchsatzeinstellung (Spitzenwert) der der Arbeitslast zugewiesenen Speicher-QoS-Richtliniengruppe (Quality of Service) dar. Wenn die Richtliniengruppenkomponente im Konflikt steht, bedeutet dies, dass alle Workloads in der Richtliniengruppe durch die festgelegte Durchsatzgrenze gedrosselt werden, was sich auf die Latenz eines oder mehrerer dieser Workloads auswirkt.

- **Mindest-QoS-Limit**

  Stellt die Latenz einer Arbeitslast dar, die durch die anderen Arbeitslasten zugewiesene Einstellung für den minimalen (erwarteten) QoS-Durchsatz verursacht wird. Wenn das für bestimmte Workloads festgelegte QoS-Minimum den Großteil der Bandbreite nutzt, um den versprochenen Durchsatz zu garantieren, werden andere Workloads gedrosselt und weisen eine höhere Latenz auf.

- **Cluster-Verbindung**

  Stellt die Kabel und Adapter dar, mit denen Clusterknoten physisch verbunden sind. Wenn es bei der Cluster-Interconnect-Komponente zu Konflikten kommt, bedeutet dies, dass die lange Wartezeit für E/A-Anfragen bei der Cluster-Interconnect-Komponente die Latenz einer oder mehrerer Workloads beeinträchtigt.

- * Data Processing*

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen dem Cluster und dem Speicheraggregat beteiligt ist, das die Arbeitslast enthält. Der Knoten, der die Datenverarbeitung durchführt, hat sich möglicherweise seit der Erkennung des Ereignisses geändert. Wenn es bei der Datenverarbeitungskomponente zu Konflikten kommt, bedeutet dies, dass eine hohe Auslastung des Datenverarbeitungsknotens die Latenz einer oder mehrerer Arbeitslasten beeinträchtigt.

- **Lautstärkeaktivierung**

  Stellt den Prozess dar, der die Nutzung aller aktiven Volumes verfolgt. In großen Umgebungen mit mehr als 1.000 aktiven Volumes verfolgt dieser Prozess, wie viele kritische Volumes gleichzeitig über den Knoten auf Ressourcen zugreifen müssen. Wenn die Anzahl gleichzeitig aktiver Volumes den empfohlenen Höchstschwellenwert überschreitet, kommt es bei einigen der nicht kritischen Volumes zu Latenzen, wie hier angegeben.

- * 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 die MetroCluster Komponente im Konflikt steht, bedeutet dies, dass ein hoher Schreibdurchsatz von Workloads auf dem lokalen Cluster oder ein Link-Health-Problem die Latenz einer oder mehrerer Workloads auf dem lokalen Cluster beeinträchtigt. Wenn sich der Cluster nicht in einer MetroCluster -Konfiguration befindet, wird dieses Symbol nicht angezeigt.

- **Aggregate- oder SSD-Aggregate-Operationen**

  Stellt das Speicheraggregat dar, auf dem die Workloads ausgeführt werden. Wenn es zu Konflikten bei der Aggregatkomponente kommt, bedeutet dies, dass eine hohe Auslastung des Aggregats die Latenz einer oder mehrerer Workloads beeinträchtigt. Ein Aggregat besteht aus allen HDDs oder einer Mischung aus HDDs und SSDs (ein Flash Pool-Aggregat) oder einer Mischung aus HDDs und einer Cloud-Ebene (ein FabricPool -Aggregat). Ein „SSD-Aggregat“ besteht aus allen SSDs (einem All-Flash-Aggregat) oder einer Mischung aus SSDs und einer Cloud-Ebene (einem FabricPool -Aggregat).

- **Cloud-Latenz**

  Stellt die Softwarekomponente im Cluster dar, die an der E/A-Verarbeitung zwischen dem Cluster und der Cloud-Ebene beteiligt ist, auf der Benutzerdaten gespeichert sind. Wenn die Cloud-Latenzkomponente in Konflikt steht, bedeutet dies, dass eine große Anzahl von Lesevorgängen von Volumes, die auf der Cloud-Ebene gehostet werden, die Latenz einer oder mehrerer Workloads beeinträchtigt.

- * SnapMirror synchronisieren*

  Stellt die Softwarekomponente im Cluster dar, die in einer synchronen SnapMirror -Beziehung an der Replikation von Benutzerdaten vom primären Volume auf das sekundäre Volume beteiligt ist. Wenn es bei der Synchronisierungskomponente von SnapMirror zu Konflikten kommt, bedeutet dies, dass die Aktivität der synchronen SnapMirror -Vorgänge die Latenz einer oder mehrerer Arbeitslasten beeinträchtigt.

Seite mit den Volumen-/Gesundheitsdetails

Auf der Seite „Volume-/Integritätsdetails“ können Sie ausführliche Informationen zu einem ausgewählten Volume anzeigen, beispielsweise Kapazität, Speichereffizienz, Konfiguration, Schutz, Anmerkungen und generierte Ereignisse. Sie können auch Informationen zu den zugehörigen Objekten und zugehörigen Warnungen für dieses Volume anzeigen.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für das ausgewählte Volume ausführen:

- **Zur Leistungsansicht wechseln**

  Ermöglicht Ihnen die Navigation zur Seite mit den Lautstärke-/Leistungsdetails.

- **Aktionen**

  - Benachrichtigung hinzufügen

    Ermöglicht Ihnen, dem ausgewählten Volume eine Warnung hinzuzufügen.

  - Schwellenwerte bearbeiten

Ermöglicht Ihnen, die Schwellenwerteinstellungen für das ausgewählte Volume zu ändern.

- Kommentieren

  Ermöglicht Ihnen, das ausgewählte Volumen mit Anmerkungen zu versehen.

- Schützen

  Ermöglicht Ihnen, entweder SnapMirror oder SnapVault -Beziehungen für das ausgewählte Volume zu erstellen.

- Beziehung

  Ermöglicht Ihnen die Ausführung der folgenden Schutzbeziehungsvorgänge:

  - Bearbeiten

    Öffnet das Dialogfeld „Beziehung bearbeiten“, in dem Sie vorhandene SnapMirror -Richtlinien, Zeitpläne und maximale Übertragungsraten für eine vorhandene Schutzbeziehung ändern können.

  - Abbrechen

    Bricht laufende Übertragungen für eine ausgewählte Beziehung ab. Optional können Sie den Neustart-Checkpoint für andere Übertragungen als die Basisübertragung entfernen. Sie können den Prüfpunkt für eine Baseline-Übertragung nicht entfernen.

  - Ruhen

    Deaktiviert vorübergehend geplante Updates für eine ausgewählte Beziehung. Bereits laufende Übertragungen müssen abgeschlossen sein, bevor die Beziehung beendet wird.

  - Brechen

    Bricht die Beziehung zwischen Quell- und Zielvolume auf und ändert das Ziel in ein Lese-/Schreibvolume.

  - Entfernen

    Löscht die Beziehung zwischen der ausgewählten Quelle und dem ausgewählten Ziel dauerhaft. Die Volumes werden nicht zerstört und die Snapshot-Kopien auf den Volumes werden nicht entfernt. Dieser Vorgang kann nicht rückgängig gemacht werden.

  - Wieder aufnehmen

    Ermöglicht geplante Übertragungen für eine ruhende Beziehung. Beim nächsten geplanten Übertragungsintervall wird ein Neustart-Checkpoint verwendet, sofern einer vorhanden ist.

  - Neu synchronisieren

    Ermöglicht Ihnen, eine zuvor unterbrochene Beziehung erneut zu synchronisieren.

  - Initialisieren/Aktualisieren

    Ermöglicht Ihnen die Durchführung einer erstmaligen Baseline-Übertragung für eine neue Schutzbeziehung oder die Durchführung einer manuellen Aktualisierung, wenn die Beziehung bereits initialisiert ist.

        - Umgekehrte Neusynchronisierung

          Ermöglicht Ihnen, eine zuvor unterbrochene Schutzbeziehung wiederherzustellen, indem Sie die Funktion von Quelle und Ziel umkehren, indem Sie die Quelle zu einer Kopie des ursprünglichen Ziels machen. Der Inhalt der Quelle wird durch den Inhalt des Ziels überschrieben und alle Daten, die neuer sind als die Daten auf der gemeinsamen Snapshot-Kopie, werden gelöscht.

    - Wiederherstellen

      Ermöglicht Ihnen, Daten von einem Volume auf einem anderen Volume wiederherzustellen. Weitere Informationen finden Sie unter"Wiederherstellen von Daten mithilfe der Seite „Volume-/Integritätsdetails“" .

> Die Schaltflächen „Wiederherstellen“ und „Beziehungsvorgang“ sind für Volumes in synchronen Schutzbeziehungen nicht verfügbar.

- **Volumen anzeigen**

  Ermöglicht Ihnen die Navigation zur Ansicht „Health: All Volumes“.

Registerkarte „Kapazität“

Auf der Registerkarte „Kapazität“ werden Details zum ausgewählten Volume angezeigt, z. B. seine physische Kapazität, logische Kapazität, Schwellenwerteinstellungen, Kontingentkapazität und Informationen zu allen Volume-Verschiebungsvorgängen:

- **Physische Kapazität**

  Details zur physischen Kapazität des Datenträgers:

    - Snapshot-Überlauf

      Zeigt den Datenspeicherplatz an, der von den Snapshot-Kopien belegt wird.

    - Gebraucht

      Zeigt den von Daten im Volume belegten Speicherplatz an.

    - Warnung

      Zeigt an, dass der Speicherplatz im Datenträger fast voll ist. Wenn dieser Schwellenwert überschritten wird, wird das Ereignis „Speicherplatz fast voll“ generiert.

    - Fehler

      Zeigt an, dass der Speicherplatz im Datenträger voll ist. Wenn dieser Schwellenwert überschritten wird, wird das Ereignis „Speicherplatz voll“ generiert.

    - Unbrauchbar

      Zeigt an, dass das Ereignis „Speicherplatz im Thin-Provisioned-Volume gefährdet“ generiert wird und dass der Speicherplatz im Thin-Provisioned-Volume aufgrund von Problemen mit der Gesamtkapazität gefährdet ist. Die nicht nutzbare Kapazität wird nur für Thin Provisioning-Volumes angezeigt.

◦ Datendiagramm

Zeigt die gesamte Datenkapazität und die verwendete Datenkapazität des Volumes an.

Wenn die automatische Vergrößerung aktiviert ist, zeigt das Datendiagramm auch den im Aggregat verfügbaren Speicherplatz an. Das Datendiagramm zeigt den effektiven Speicherplatz an, der von Daten im Volume verwendet werden kann. Dabei kann es sich um einen der folgenden Werte handeln:

- Tatsächliche Datenkapazität des Datenträgers unter den folgenden Bedingungen:
  - Autogrow ist deaktiviert.
  - Das Volume mit aktivierter Autogrow-Funktion hat die maximale Größe erreicht.
  - Das Autogrow-fähige Thick-Provisioning-Volume kann nicht weiter wachsen.
- Datenkapazität des Volumes unter Berücksichtigung der maximalen Volumegröße (für Thin Provisioning-Volumes und für Thick Provisioning-Volumes, wenn das Aggregat Platz für das Erreichen der maximalen Volumegröße bietet)
- Datenkapazität des Volumes nach Berücksichtigung der nächstmöglichen Autogrow-Größe (für Thick Provisioning-Volumes mit einem Autogrow-Prozentschwellenwert)

◦ Diagramm „Snapshot-Kopien“

Dieses Diagramm wird nur angezeigt, wenn die verwendete Snapshot-Kapazität oder die Snapshot-Reserve nicht Null ist.

Beide Diagramme zeigen die Kapazität an, um die die Snapshot-Kapazität die Snapshot-Reserve übersteigt, wenn die verwendete Snapshot-Kapazität die Snapshot-Reserve übersteigt.

- **Kapazität logisch**

Zeigt die logischen Speicherplatzeigenschaften des Datenträgers an. Der logische Speicherplatz gibt die tatsächliche Größe der auf der Festplatte gespeicherten Daten an, ohne die Einsparungen durch die Verwendung von ONTAP Speichereffizienztechnologien zu berücksichtigen.

◦ Logische Speicherplatzberichte

Zeigt an, ob für das Volume die logische Speicherplatzberichterstattung konfiguriert ist. Der Wert kann „Aktiviert“, „Deaktiviert“ oder „Nicht zutreffend“ sein. Für Volumes auf älteren Versionen von ONTAP oder auf Volumes, die die logische Speicherplatzberichterstattung nicht unterstützen, wird „Nicht zutreffend“ angezeigt.

◦ Gebraucht

Zeigt die Menge des logischen Speicherplatzes an, der von Daten im Volume verwendet wird, sowie den Prozentsatz des verwendeten logischen Speicherplatzes basierend auf der gesamten Datenkapazität.

◦ Durchsetzung des logischen Speicherplatzes

Zeigt an, ob die Durchsetzung des logischen Speicherplatzes für Thin Provisioning-Volumes konfiguriert ist. Wenn die Option auf „Aktiviert“ eingestellt ist, kann die logisch verwendete Größe des Datenträgers nicht größer sein als die aktuell eingestellte physische Datenträgergröße.

- **Automatisches Wachstum**

Zeigt an, ob das Volume automatisch vergrößert wird, wenn der Speicherplatz erschöpft ist.

- **Platzgarantie**

  Zeigt die FlexVol volume -Einstellungssteuerung an, wenn ein Volume freie Blöcke aus einem Aggregat entfernt. Diese Blöcke stehen dann garantiert für Schreibvorgänge in Dateien im Volume zur Verfügung. Die Speicherplatzgarantie kann auf einen der folgenden Werte eingestellt werden:

  - Keine

    Für das Volume ist keine Speicherplatzgarantie konfiguriert.

  - Datei

    Die volle Größe spärlich geschriebener Dateien (z. B. LUNs) ist garantiert.

  - Volumen

    Die volle Größe des Volumens ist garantiert.

  - Teilweise

    Das FlexCache -Volume reserviert Speicherplatz basierend auf seiner Größe. Wenn die Größe des FlexCache Volumes 100 MB oder mehr beträgt, wird die Mindestspeicherplatzgarantie standardmäßig auf 100 MB festgelegt. Wenn die Größe des FlexCache Volumes weniger als 100 MB beträgt, wird die Mindestspeicherplatzgarantie auf die Größe des FlexCache Volumes festgelegt. Wenn die Größe des FlexCache Volumes später vergrößert wird, wird die Mindestspeicherplatzgarantie nicht erhöht.

  Die Speicherplatzgarantie ist teilweise, wenn das Volume vom Typ „Datencache“ ist.

- **Details (physisch)**

  Zeigt die physikalischen Eigenschaften des Datenträgers an.

- **Gesamtkapazität**

  Zeigt die gesamte physische Kapazität des Datenträgers an.

- **Datenkapazität**

  Zeigt die Menge des vom Volume verwendeten physischen Speicherplatzes (genutzte Kapazität) und die Menge des physischen Speicherplatzes an, der im Volume noch verfügbar ist (freie Kapazität). Diese Werte werden auch als Prozentsatz der gesamten körperlichen Leistungsfähigkeit angezeigt.

  Wenn das Ereignis „Gefährdeter Speicherplatz für Thin-Provisioned-Volume“ für Thin-Provisioned-Volumes generiert wird, wird die vom Volume verwendete Speicherplatzmenge (verwendete Kapazität) und die Speicherplatzmenge angezeigt, die im Volume verfügbar ist, aber aufgrund von Problemen mit der Gesamtkapazität nicht verwendet werden kann (unverwendbare Kapazität).

- **Schnappschuss-Reserve**

  Zeigt die von den Snapshot-Kopien verwendete Speicherplatzmenge (genutzte Kapazität) und die für Snapshot-Kopien verfügbare Speicherplatzmenge (freie Kapazität) im Volume an. Diese Werte werden auch als Prozentsatz der gesamten Snapshot-Reserve angezeigt.

  Wenn das Ereignis „Speicherplatz im Thin-Provisioning-Volume gefährdet“ für Thin-Provisioning-Volumes generiert wird, wird die von den Snapshot-Kopien verwendete Speicherplatzmenge (verwendete Kapazität)

und die Speicherplatzmenge angezeigt, die im Volume verfügbar ist, aber aufgrund von Problemen mit der Gesamtkapazität nicht zum Erstellen von Snapshot-Kopien verwendet werden kann (unbrauchbare Kapazität).

- **Lautstärkeschwellenwerte**

  Zeigt die folgenden Schwellenwerte für die Volume-Kapazität an:

  - Fast volle Schwelle

    Gibt den Prozentsatz an, bei dem ein Volume fast voll ist.

  - Voller Schwellenwert

    Gibt den Prozentsatz an, bei dem ein Volume voll ist.

- **Weitere Details**

  - Maximale Größe automatisch vergrößern

    Zeigt die maximale Größe an, bis zu der das Volume automatisch wachsen kann. Der Standardwert beträgt 120 % der Volumegröße bei der Erstellung. Dieses Feld wird nur angezeigt, wenn die automatische Vergrößerung für das Volume aktiviert ist.

  - Qtree-Kontingent – Zugesicherte Kapazität

    Zeigt den in den Kontingenten reservierten Speicherplatz an.

  - Überbelegte Kapazität des Qtree-Kontingents

    Zeigt die Menge an Speicherplatz an, die verwendet werden kann, bevor das System das Ereignis „Volume Qtree Quota Overcommitted“ generiert.

  - Teilreserve

    Steuert die Größe der Überschreibreserve. Standardmäßig ist die Teilreserve auf 100 eingestellt. Dies bedeutet, dass 100 Prozent des erforderlichen reservierten Speicherplatzes reserviert sind, sodass die Objekte vollständig vor Überschreibungen geschützt sind. Wenn die Teilreserve weniger als 100 Prozent beträgt, wird der reservierte Speicherplatz für alle reservierten Dateien in diesem Volume auf den Prozentsatz der Teilreserve reduziert.

  - Momentaufnahme der täglichen 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.

    Im Feld „Snapshot-Tage bis zur Vollendung“ wird der Wert „Nicht zutreffend“ angezeigt, wenn die Wachstumsrate der Snapshot-Kopien im Volume null oder negativ ist oder wenn nicht genügend Daten zum Berechnen der Wachstumsrate vorhanden sind.

  - Automatisches Löschen von Schnappschüssen

Gibt an, 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 zu den Snapshot-Kopien im Volume an.

Die Anzahl der Snapshot-Kopien im Volume wird als Link angezeigt. Durch Klicken auf den Link wird das Dialogfeld „Snapshot-Kopien auf einem Volume“ geöffnet, in dem Details zu den Snapshot-Kopien angezeigt werden.

Die Anzahl der Snapshot-Kopien wird etwa stündlich aktualisiert. Die Liste der Snapshot-Kopien wird jedoch aktualisiert, wenn 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 beim Klicken auf das Symbol aufgelistet werden.

- **Lautstärke verschieben**

Zeigt den Status des aktuellen oder des letzten Volume-Verschiebevorgangs an, der auf dem Volume ausgeführt wurde, sowie weitere Details, z. B. die aktuelle Phase des laufenden Volume-Verschiebevorgangs, Quellaggregat, Zielaggregat, Startzeit, Endzeit und geschätzte Endzeit.

Zeigt außerdem die Anzahl der Volume-Verschiebungsvorgänge an, die für das ausgewählte Volume ausgeführt wurden. Weitere Informationen zu den Volume-Verschiebungsvorgängen können Sie anzeigen, indem Sie auf den Link **Volume-Verschiebungsverlauf** klicken.

Registerkarte „Konfiguration“

Auf der Registerkarte „Konfiguration“ werden Details zum ausgewählten Volume angezeigt, z. B. die Exportrichtlinie, der RAID-Typ, die Kapazität und die mit der Speichereffizienz verbundenen Funktionen des Volumes:

- **Überblick**

◦ Vollständiger Name

Zeigt den vollständigen Namen des Datenträgers 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, wenn das Volume auf einem FabricPool-fähigen Aggregat bereitgestellt wird. Die Richtlinie kann „Keine“, „Nur Snapshot“, „Backup“, „Auto“ oder „Alle“ sein.

◦ Speicher-VM

Zeigt den Namen der SVM an, die das Volume enthält.

◦ Kreuzungspfad

Zeigt den Status des Pfads an, der aktiv oder inaktiv sein kann. Außerdem wird der Pfad in der SVM angezeigt, in dem das Volume eingebunden ist. Sie können auf den Link **Verlauf** klicken, um die letzten fünf Änderungen am Kreuzungspfad anzuzeigen.

- Exportrichtlinie

  Zeigt den Namen der Exportrichtlinie an, die für das Volume erstellt wird. Sie können auf den Link klicken, um Details zu den Exportrichtlinien, Authentifizierungsprotokollen und dem aktivierten Zugriff auf die Volumes anzuzeigen, die zur SVM gehören.

- Stil

  Zeigt den Lautstärkestil an. Der Volume-Stil kann FlexVol oder FlexGroup sein.

- Typ

  Zeigt den Typ des ausgewählten Volumes an. Der Datenträgertyp kann „Lesen/Schreiben“, „Lastverteilung“, „Datenschutz“, „Datencache“ oder „Temporär“ sein.

- RAID-Typ

  Zeigt den RAID-Typ des ausgewählten Volumes an. Der RAID-Typ kann RAID0, RAID4, RAID-DP oder RAID-TEC sein.

  > Für FlexGroup -Volumes werden möglicherweise mehrere RAID-Typen angezeigt, da sich die einzelnen Volumes für FlexGroups auf Aggregaten unterschiedlicher Typen befinden können.

- SnapLock -Typ

  Zeigt den SnapLock -Typ des Aggregats an, das das Volume enthält.

- SnapLock -Ablauf

  Zeigt das Ablaufdatum des SnapLock -Volumes an.

- **Kapazität**
  - Thin Provisioning

    Zeigt an, ob Thin Provisioning für das Volume konfiguriert ist.

  - Automatisches Wachstum

    Zeigt an, ob das flexible Volumen innerhalb eines Aggregats automatisch wächst.

  - Automatisches Löschen von Schnappschüssen

    Gibt an, 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 Kontingente 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

  Gibt an, ob der auf einem Volume aktivierte Deduplizierungsvorgang ein manueller, geplanter oder richtlinienbasierter Vorgang ist. Wenn der Modus auf „Geplant“ eingestellt ist, wird der Betriebszeitplan angezeigt, und wenn der Modus auf „Richtlinie“ eingestellt ist, wird der Richtlinienname angezeigt.

- Deduplizierungstyp

  Gibt den Typ des Deduplizierungsvorgangs an, der auf dem Volume ausgeführt wird. Wenn sich das Volume in einer SnapVault -Beziehung befindet, wird der Typ SnapVault angezeigt. Für alle anderen Volumes wird der Typ als „Regulär“ angezeigt.

- Richtlinie zur Speichereffizienz

  Gibt den Namen der Speichereffizienzrichtlinie an, die diesem Volume über Unified Manager zugewiesen wurde. Diese Richtlinie kann die Komprimierungs- und Deduplizierungseinstellungen steuern.

- **Schutz**
  - Snapshot-Kopien

    Gibt an, ob automatische Snapshot-Kopien aktiviert oder deaktiviert sind.

Registerkarte „Schutz“

Auf der Registerkarte „Schutz“ werden Schutzdetails zum ausgewählten Volume angezeigt, z. B. Verzögerungsinformationen, Beziehungstyp und Topologie der Beziehung.

- **Zusammenfassung**

  Zeigt Eigenschaften der Schutzbeziehungen (SnapMirror, SnapVault oder Storage VM DR) für ein ausgewähltes Volume an. Für alle anderen Beziehungstypen wird nur die Eigenschaft „Beziehungstyp“ angezeigt. Wenn ein primäres Volume ausgewählt ist, werden nur die verwalteten und lokalen Snapshot-Kopierrichtlinien angezeigt. Zu den für SnapMirror und SnapVault -Beziehungen angezeigten Eigenschaften gehören die folgenden:

  - Quellvolumen

    Zeigt den Namen der Quelle des ausgewählten Volumes an, wenn das ausgewählte Volume ein Ziel ist.

  - Verzögerungsstatus

    Zeigt den Update- oder Übertragungsverzögerungsstatus für eine Schutzbeziehung an. Der Status kann „Fehler“, „Warnung“ oder „Kritisch“ sein.

    Der Verzögerungsstatus ist für synchrone Beziehungen nicht anwendbar.

◦ Verzögerungsdauer

Zeigt die Zeit an, um die die Daten auf dem Spiegel hinter der Quelle zurückliegen.

◦ Letztes erfolgreiches Update

Zeigt Datum und Uhrzeit des letzten erfolgreichen Schutzupdates an.

Das letzte erfolgreiche Update ist für synchrone Beziehungen nicht anwendbar.

◦ Speicherdienstmitarbeiter

Zeigt entweder „Ja“ oder „Nein“ an, um anzugeben, ob das Volume zu einem Speicherdienst gehört und von diesem verwaltet wird.

◦ Versionsflexible Replikation

Zeigt entweder „Ja“, „Ja mit Sicherungsoption“ oder „Keine“ an. „Ja“ bedeutet, dass die SnapMirror Replikation auch dann möglich ist, wenn auf Quell- und Zielvolumes unterschiedliche Versionen der ONTAP -Software ausgeführt werden. „Ja mit Sicherungsoption“ bedeutet die Implementierung des SnapMirror Schutzes mit der Möglichkeit, mehrere Versionen von Sicherungskopien auf dem Ziel aufzubewahren. „Keine“ bedeutet, dass die Version Flexible Replication nicht aktiviert ist.

◦ Beziehungsfähigkeit

Gibt die für die Schutzbeziehung verfügbaren ONTAP Funktionen an.

◦ Schutzdienst

Zeigt den Namen des Schutzdienstes an, wenn die Beziehung von einer Schutzpartneranwendung 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 „Nicht initialisiert“, „SnapMirrored“ oder „Abgebrochen“ 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 ein Übertragungsabbruchvorgang ausgeführt, der möglicherweise die Entfernung des Prüfpunkts umfasst.

- Überprüfung

  Das Zielvolume wird einer Diagnoseprüfung unterzogen und es findet keine Übertragung statt.

- Finalisieren

  SnapMirror Übertragungen sind aktiviert. Das Volume befindet sich derzeit in der Nachübertragungsphase für inkrementelle SnapVault Übertragungen.

- Leerlauf

  Übertragungen sind aktiviert und es findet keine Übertragung statt.

- Synchron

  Die Daten in den beiden Volumes in der synchronen Beziehung werden synchronisiert.

- Nicht synchron

  Die Daten im Zielvolume werden nicht mit dem Quellvolume synchronisiert.

- Vorbereitung

  SnapMirror Übertragungen sind aktiviert. Das Volume befindet sich derzeit in der Vorübertragungsphase für inkrementelle SnapVault Übertragungen.

- In der Warteschlange

  SnapMirror Übertragungen sind aktiviert. Es sind keine Überweisungen im Gange.

- Ruhezustand

  SnapMirror -Übertragungen sind deaktiviert. Es ist keine Übertragung im Gange.

- Stilllegung

  Eine SnapMirror -Übertragung ist im Gange. Weitere Übertragungen sind deaktiviert.

- Übertragen

  SnapMirror Übertragungen sind aktiviert und eine Übertragung ist im Gange.

- Übergang

  Die asynchrone Datenübertragung vom Quell- zum Zieldatenträger ist abgeschlossen und der Übergang zum synchronen Betrieb hat begonnen.

- Warten

  Eine SnapMirror Übertragung wurde eingeleitet, aber einige zugehörige Aufgaben warten darauf, in die Warteschlange gestellt zu werden.

◦ Max. Übertragungsrate

Zeigt die maximale Übertragungsrate für die Beziehung an. Die maximale Übertragungsrate kann ein numerischer Wert in Kilobyte pro Sekunde (Kbps), Megabyte pro Sekunde (Mbps), Gigabyte pro Sekunde (Gbps) oder Terabyte pro Sekunde (Tbps) sein. Wenn „Keine Begrenzung“ angezeigt wird, ist die Basisübertragung zwischen Beziehungen unbegrenzt.

◦ SnapMirror -Richtlinie

Zeigt die Schutzrichtlinie für das Volume an. DPDefault gibt die standardmäßige asynchrone Spiegelschutzrichtlinie an, XDPDefault gibt die standardmäßige asynchrone Vault-Richtlinie an und DPSyncDefault gibt die standardmäßige asynchrone MirrorVault-Richtlinie an. StrictSync gibt die standardmäßige synchrone strikte Schutzrichtlinie an und Sync gibt die standardmäßige synchrone Richtlinie an. Sie können auf den Richtliniennamen klicken, um die mit dieser Richtlinie verknüpften Details anzuzeigen, einschließlich der folgenden Informationen:

- Übertragungspriorität
- Zugriffszeiteinstellung ignorieren
- Versuchslimit
- Kommentare
- SnapMirror -Etiketten
- Aufbewahrungseinstellungen
- Tatsächliche Snapshot-Kopien
- Snapshot-Kopien aufbewahren
- Schwellenwert für die Aufbewahrungswarnung
- Snapshot-Kopien ohne Aufbewahrungseinstellungen. In einer kaskadierenden SnapVault -Beziehung, bei der die Quelle ein Datenschutz-Volume (DP) ist, gilt nur die Regel „sm_created“.

◦ Aktualisierungszeitplan

Zeigt den der Beziehung zugewiesenen SnapMirror Zeitplan an. Wenn Sie den Cursor über das Informationssymbol bewegen, werden die Zeitplandetails angezeigt.

◦ Lokale Snapshot-Richtlinie

Zeigt die Snapshot-Kopierrichtlinie für das Volume an. Die Richtlinie ist „Standard“, „Keine“ oder ein beliebiger Name, der einer benutzerdefinierten Richtlinie zugewiesen wird.

◦ Geschützt durch

Zeigt den für das ausgewählte Volume verwendeten Schutztyp an. Wenn ein Volume beispielsweise durch Consistency Group- und SnapMirror Volume-Beziehungen geschützt ist, werden in diesem Feld sowohl SnapMirror als auch Consistency Group angezeigt. Dieses Feld enthält auch einen Link, der Sie zur Seite „Beziehungen“ weiterleitet, um den einheitlichen Beziehungsstatus anzuzeigen. Die Verknüpfung ist nur auf Bestandteilsbeziehungen anwendbar.

◦ Konsistenzgruppe

Für 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 Zusammenhang stehen. Das ausgewählte Volume wird durch einen dunkelgrauen Rahmen angezeigt und Linien zwischen Volumes in der Topologie zeigen den Schutzbeziehungstyp 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 fettgedruckte Linien geben eine asynchrone Spiegelbeziehung an, eine einfache fettgedruckte

Linie gibt eine asynchrone Vault-Beziehung an, doppelte einfache Linien geben eine asynchrone MirrorVault-Beziehung an und eine fettgedruckte und eine nicht fettgedruckte Linie geben eine synchrone Beziehung an. Die folgende Tabelle gibt an, ob es sich bei der synchronen Beziehung um StrictSync oder Sync handelt.

Wenn Sie mit der rechten Maustaste auf ein Volume klicken, wird ein Menü angezeigt, in dem Sie entweder das Volume schützen oder Daten darauf wiederherstellen können. Wenn Sie mit der rechten Maustaste auf eine Beziehung klicken, wird ein Menü angezeigt, in dem Sie eine Beziehung bearbeiten, abbrechen, stilllegen, unterbrechen, entfernen oder fortsetzen können.

In den folgenden Fällen werden die Menüs nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn sich das Volume in einer synchronen Schutzbeziehung befindet
- Wenn die Volume-ID unbekannt ist, beispielsweise wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde, können Sie durch Klicken auf ein anderes Volume in der Topologie Informationen zu diesem Volume auswählen und anzeigen. Ein Fragezeichen ( ) in der oberen linken Ecke eines Volumes zeigt an, dass das Volume entweder fehlt oder noch nicht erkannt wurde. Es kann auch darauf hinweisen, dass die Kapazitätsinformationen fehlen. Wenn Sie den Cursor über das Fragezeichen bewegen, werden zusätzliche Informationen angezeigt, darunter auch Vorschläge für Abhilfemaßnahmen.

Die Topologie zeigt Informationen zu Volumekapazität, Verzögerung, Snapshot-Kopien und der letzten erfolgreichen Datenübertragung an, wenn sie einer der mehreren gängigen Topologievorlagen entspricht. Wenn eine Topologie nicht einer dieser Vorlagen entspricht, werden Informationen zur Volumeverzögerung und zur letzten erfolgreichen Datenübertragung in einer Beziehungstabelle unter der Topologie angezeigt. In diesem Fall zeigt die hervorgehobene Zeile in der Tabelle das ausgewählte Volume an und in der Topologieansicht zeigen fette Linien mit einem blauen Punkt die Beziehung zwischen dem ausgewählten Volume und seinem Quellvolume an.

Topologieansichten enthalten die folgenden Informationen:

- Kapazität

  Zeigt die Gesamtkapazität an, die vom Volume verwendet wird. Wenn Sie den Cursor über einem Volume in der Topologie positionieren, werden im Dialogfeld „Aktuelle Schwellenwerteinstellungen“ die aktuellen Warn- und kritischen Schwellenwerteinstellungen für dieses Volume angezeigt. Sie können die Schwellenwerteinstellungen auch bearbeiten, indem Sie im Dialogfeld „Aktuelle Schwellenwerteinstellungen“ auf den Link **Schwellenwerte bearbeiten** klicken. Wenn Sie das Kontrollkästchen **Kapazität** 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 Kontrollkästchens **Lag** werden alle Verzögerungsinformationen für alle Volumes in der Topologie ausgeblendet. Wenn das Kontrollkästchen **Lag** abgeblendet ist, werden die Lag-Informationen für das ausgewählte Volume in der Beziehungstabelle unter der Topologie angezeigt, sowie die Lag-Informationen für alle zugehörigen Volumes.

- Schnappschuss

  Zeigt die Anzahl der für ein Volume verfügbaren Snapshot-Kopien an. Durch Deaktivieren des

Kontrollkästchens **Snapshot** werden alle Snapshot-Kopierinformationen für alle Volumes in der Topologie ausgeblendet. Klicken Sie auf das Symbol zum Kopieren eines Snapshots ( ) zeigt die Snapshot-Kopienliste für ein Volume an. Die neben dem Symbol angezeigte Anzahl der Snapshot-Kopien wird etwa stündlich aktualisiert. Die Liste der Snapshot-Kopien wird jedoch aktualisiert, wenn 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 beim Klicken auf das Symbol aufgelistet werden.

- Letzte erfolgreiche Übertragung

  Zeigt Betrag, Dauer, Uhrzeit und Datum der letzten erfolgreichen Datenübertragung an. Wenn das Kontrollkästchen **Letzte erfolgreiche Übertragung** abgeblendet ist, werden die Informationen zur letzten erfolgreichen Übertragung für das ausgewählte Volume in der Beziehungstabelle unter 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 -Schutzbeziehungen für das ausgewählte Volume an. Es stehen drei Verlaufsdiagramme zur Verfügung: Verzögerungsdauer eingehender Beziehungen, Dauer eingehender Beziehungsübertragungen und Größe eingehender Beziehungsübertragungen. Verlaufsinformationen werden nur angezeigt, wenn Sie ein Zielvolume auswählen. Wenn Sie ein primäres Volume auswählen, sind die Diagramme leer und die Meldung „Keine Daten gefunden“ wird angezeigt. Wenn die Volumes durch synchrone Consistency Group- und SnapMirror -Beziehungen geschützt sind, werden keine Informationen zur Übertragungsdauer und Übertragungsgröße der Beziehung angezeigt.

  Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Verlaufsbereich auswählen. Sie können auch Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Mithilfe von Verlaufsdiagrammen können Sie Trends erkennen: Wenn beispielsweise große Datenmengen zur gleichen Tages- oder Wochenzeit übertragen werden oder wenn der Schwellenwert für Verzögerungswarnungen oder Verzögerungsfehler ständig überschritten wird, können Sie entsprechende Maßnahmen ergreifen. Darüber hinaus können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie gerade anzeigen.

In den Schutzverlaufsdiagrammen werden die folgenden Informationen angezeigt:

- **Dauer der Beziehungsverzögerung**

  Zeigt je nach ausgewähltem Zeitraum Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Tage, Monate oder Jahre auf der horizontalen Achse (x) an. Der obere Wert auf der y-Achse gibt die maximale Verzögerungsdauer an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. Die horizontale orange Linie im Diagramm stellt den Schwellenwert für den Verzögerungsfehler dar und die horizontale gelbe Linie stellt den Schwellenwert für die Verzögerungswarnung dar. Wenn Sie den Cursor über diese Linien bewegen, wird die Schwellenwerteinstellung angezeigt. Die horizontale blaue Linie stellt die Verzögerungsdauer dar. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen gewünschten Bereich bewegen.

- **Dauer der Beziehungsübertragung**

  Zeigt je nach ausgewähltem Zeitraum Sekunden, Minuten oder Stunden auf der vertikalen Achse (y) und Tage, Monate oder Jahre auf der horizontalen Achse (x) an. Der obere Wert auf der y-Achse gibt die maximale Übertragungsdauer an, die in dem auf der x-Achse dargestellten Zeitraum erreicht wurde. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den gewünschten Bereich bewegen.

Dieses Diagramm ist für Datenträger in synchronen Schutzbeziehungen nicht verfügbar.

- **Beziehung übertragene Größe**

  Zeigt je nach Übertragungsgröße Bytes, Kilobytes, Megabytes usw. auf der vertikalen Achse (y) an und zeigt je nach ausgewähltem Zeitraum Tage, Monate oder Jahre auf der horizontalen Achse (x) an. Der obere Wert auf der y-Achse gibt die maximale Übertragungsgröße an, die in dem auf der x-Achse angezeigten Zeitraum erreicht wurde. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen gewünschten Bereich bewegen.

  Dieses Diagramm ist für Datenträger in synchronen Schutzbeziehungen nicht verfügbar.

Geschichtsbereich

Im Bereich „Verlauf“ werden Diagramme angezeigt, die Informationen zur Kapazität und den Speicherplatzreservierungen des ausgewählten Volumes liefern. Darüber hinaus können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie gerade anzeigen.

Wenn die Daten oder der Zustand des Datenträgers über einen bestimmten Zeitraum unverändert bleiben, sind die Diagramme möglicherweise leer und die Meldung „Keine Daten gefunden“ wird angezeigt.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Verlaufsbereich auswählen. Sie können auch Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Mithilfe von Verlaufsdiagrammen können Sie Trends erkennen. Wenn beispielsweise die Datenträgernutzung ständig den Schwellenwert „Fast voll“ überschreitet, können Sie entsprechende Maßnahmen ergreifen.

Verlaufsdiagramme zeigen die folgenden Informationen an:

- **Verwendete Volumenkapazität**

  Zeigt die verwendete Kapazität des Datenträgers und den Trend der Datenträgerkapazitätsnutzung basierend auf dem Nutzungsverlauf als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der vertikalen Achse (y) 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 bewegen. 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 Volumenkapazität im Vergleich zum Gesamtvolumen**

  Zeigt den Trend der Nutzung der Volume-Kapazität basierend auf dem Nutzungsverlauf sowie die genutzte Kapazität, die Gesamtkapazität und Details zu den Speicherplatzeinsparungen durch Deduplizierung und Komprimierung 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. Sie können die Details für bestimmte Punkte im Diagramm anzeigen, indem Sie den Cursor über einen bestimmten Bereich bewegen. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Trend der genutzten Kapazität“ klicken, wird die Diagrammlinie „Trend der genutzten Kapazität“ ausgeblendet.

- **Genutzte Volumenkapazität (%)**

  Zeigt die genutzte Kapazität des Datenträgers und den Trend der Nutzung der Datenträgerkapazität basierend auf dem Nutzungsverlauf als Liniendiagramm in Prozent auf der vertikalen Achse (y) 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 bewegen. 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.

- **Genutzte Snapshot-Kapazität (%)**

  Zeigt die Snapshot-Reserve und den Snapshot-Warnschwellenwert als Liniendiagramme und die von den Snapshot-Kopien verwendete Kapazität als Flächendiagramm in Prozent auf der vertikalen (y) Achse an. 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 Cursor über einen bestimmten Bereich bewegen. 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 „Snapshot Reserve“ ausgeblendet.

Ereignisliste

In der Ereignisliste werden Details zu neuen und bestätigten Ereignissen angezeigt:

- **Schwere**

  Zeigt den Schweregrad des Ereignisses an.

- **Ereignis**

  Zeigt den Ereignisnamen an.

- **Ausgelöste Zeit**

  Zeigt die Zeit an, die seit der Generierung des Ereignisses vergangen ist. Wenn die verstrichene Zeit mehr als eine Woche beträgt, wird der Zeitstempel angezeigt, wann das Ereignis generiert wurde.

Bereich „Zugehörige Anmerkungen“

Im Bereich „Zugehörige Anmerkungen“ können Sie Anmerkungsdetails anzeigen, die mit dem ausgewählten Datenträger verknüpft sind. Zu den Details gehören der Anmerkungsname und die Anmerkungswerte, die auf das Volume angewendet werden. Sie können manuelle Anmerkungen auch aus dem Bereich „Verwandte Anmerkungen“ 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 in Zusammenhang stehen:

- **Virtuelle Speichermaschine**

  Zeigt die Kapazität und den Integritätsstatus der SVM an, die das ausgewählte Volume enthält.

- **Aggregat**

  Zeigt die Kapazität und den Integritätsstatus des Aggregats an, das das ausgewählte Volume enthält. Bei FlexGroup -Volumes wird die Anzahl der Aggregate aufgelistet, aus denen die FlexGroup besteht.

- **Volumina im Aggregat**

  Zeigt die Anzahl und Kapazität aller Volumes an, die zum übergeordneten Aggregat des ausgewählten Volumes gehören. Außerdem wird der Integritätsstatus der Volumes basierend auf dem höchsten Schweregrad angezeigt. Wenn ein Aggregat beispielsweise zehn Volumes enthält, von denen fünf den Status „Warnung“ und die restlichen fünf den Status „Kritisch“ anzeigen, 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, und die Kapazität der Qtrees mit Kontingent, die das ausgewählte Volume enthält. Die Kapazität der Qtrees mit Quota wird im Verhältnis zur Datenkapazität des Volumes angezeigt. Der Gesundheitszustand der Qtrees wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn ein Volume beispielsweise zehn Qtrees hat, fünf mit dem Status „Warnung“ und die restlichen fünf mit dem Status „Kritisch“, dann 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 Integritätsstatus der LUNs wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad.

- **Benutzer- und Gruppenkontingente**

  Zeigt die Anzahl und den Status der Benutzer- und Benutzergruppenkontingente an, die dem Volume und seinen Qtrees zugeordnet sind.

- * FlexClone -Volumes*

  Zeigt die Anzahl und Kapazität aller geklonten Volumes des ausgewählten Volumes an. Die Anzahl und Kapazität werden nur angezeigt, wenn das ausgewählte Volume geklonte Volumes enthält.

- **Übergeordnetes Volume**

  Zeigt den Namen und die Kapazität des übergeordneten Volumes eines ausgewählten FlexClone -Volumes an. Das übergeordnete Volume wird nur angezeigt, wenn das ausgewählte Volume ein FlexClone -Volume ist.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ können Sie die Liste der mit dem ausgewählten Volume verknüpften Gruppen anzeigen.

Bereich „Zugehörige Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnungen anzeigen, die für das ausgewählte Volume erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link „Warnung hinzufügen“ klicken, oder eine vorhandene Warnung bearbeiten, indem Sie auf den Warnungsnamen klicken.

Seite mit Speicher-VM-/Integritätsdetails

Auf der Seite „Storage VM / Health Details“ können Sie ausführliche Informationen zur ausgewählten Storage VM anzeigen, beispielsweise deren Integrität, Kapazität, Konfiguration, Datenrichtlinien, logische Schnittstellen (LIFs), LUNs, Qtrees, Benutzer, Benutzergruppenkontingente und Schutzdetails. Sie können auch Informationen zu den zugehörigen Objekten und zugehörigen Warnungen für die Speicher-VM anzeigen.

Sie können nur die Datenspeicher-VM überwachen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für die ausgewählte Speicher-VM ausführen:

- **Zur Leistungsansicht wechseln**

  Ermöglicht Ihnen die Navigation zur Seite mit den Storage-VM-/Leistungsdetails.

- **Aktionen**
  - Benachrichtigung hinzufügen

    Ermöglicht Ihnen, der ausgewählten Speicher-VM eine Warnung hinzuzufügen.

  - Kommentieren

    Ermöglicht Ihnen, die ausgewählte Speicher-VM mit Anmerkungen zu versehen.

- **Speicher-VMs anzeigen**

  Ermöglicht Ihnen die Navigation zur Ansicht „Integrität: Alle Speicher-VMs“.

Registerkarte „Integrität“

Auf der Registerkarte „Integrität“ werden detaillierte Informationen zur Datenverfügbarkeit, Datenkapazität und zu Schutzproblemen verschiedener Objekte wie Volumes, Aggregaten, NAS-LIFs, SAN-LIFs, LUNs, Protokollen, Diensten, NFS-Freigaben und CIFS-Freigaben angezeigt.

Sie können auf das Diagramm eines Objekts klicken, um die gefilterte Objektliste anzuzeigen. Sie können beispielsweise auf das Volume-Kapazitätsdiagramm klicken, das Warnungen anzeigt, um die Liste der Volumes anzuzeigen, bei denen Kapazitätsprobleme mit dem Schweregrad „Warnung“ vorliegen.

- **Verfügbarkeitsprobleme**

  Zeigt die Gesamtzahl der Objekte als Diagramm an, einschließlich der Objekte mit Verfügbarkeitsproblemen und der Objekte ohne Verfügbarkeitsprobleme. Die Farben im Diagramm stellen die unterschiedlichen Schweregrade der Probleme dar. Die Informationen unter dem Diagramm enthalten Details zu Verfügbarkeitsproblemen, die die Verfügbarkeit von Daten in der Speicher-VM beeinträchtigen

können oder bereits beeinträchtigt haben. Beispielsweise werden Informationen zu den ausgefallenen NAS-LIFs und SAN-LIFs sowie zu den offline geschalteten Volumes angezeigt.

Sie können auch Informationen zu den zugehörigen Protokollen und Diensten anzeigen, die derzeit ausgeführt werden, sowie die Anzahl und den Status der NFS- und CIFS-Freigaben.

- **Kapazitätsprobleme**

  Zeigt die Gesamtzahl der Objekte als Diagramm an, einschließlich der Objekte mit Kapazitätsproblemen und der Objekte ohne kapazitätsbezogene Probleme. Die Farben im Diagramm stellen die unterschiedlichen Schweregrade der Probleme dar. Die Informationen unter dem Diagramm enthalten Einzelheiten zu Kapazitätsproblemen, die sich auf die Datenkapazität in der Speicher-VM auswirken können oder bereits ausgewirkt haben. Beispielsweise werden Informationen zu Aggregaten angezeigt, bei denen die Wahrscheinlichkeit einer Überschreitung der festgelegten Schwellenwerte besteht.

- **Schutzprobleme**

  Bietet einen schnellen Überblick über den schutzbezogenen Zustand der Speicher-VM, indem in einem Felddialogfeld die Gesamtzahl der Beziehungen angezeigt wird, einschließlich der Beziehungen mit Schutzproblemen und der Beziehungen ohne schutzbezogene Probleme. Sie können auch den Status der Speicher-VM-DR-Beziehung für die ausgewählte Speicher-VM anzeigen. Die Ereignisse der Speicher-VM-DR-Beziehungen werden hier angezeigt. Durch Klicken auf die Ereignisse gelangen Sie zur Seite mit den Ereignisdetails. Wenn ungeschützte Volumes vorhanden sind, gelangen Sie durch Klicken auf den Link zur Ansicht „Integrität: Alle Volumes“, wo Sie eine gefilterte Liste der ungeschützten Volumes auf der Speicher-VM anzeigen können. Die Farben im Diagramm stellen die unterschiedlichen Schweregrade der Probleme dar. Durch Klicken auf ein Diagramm gelangen Sie zur Ansicht „Beziehung: Alle Beziehungen“, in der Sie eine gefilterte Liste mit Details zu Schutzbeziehungen anzeigen können. Die Informationen unter dem Diagramm enthalten Einzelheiten zu Schutzproblemen, die den Schutz der Daten in der Speicher-VM beeinträchtigen können oder bereits beeinträchtigt haben. Beispielsweise werden Informationen zu Volumes angezeigt, deren Snapshot-Kopierreserve fast voll ist, oder zu Verzögerungsproblemen bei der SnapMirror Beziehung.

Registerkarte „Kapazität“

Auf der Registerkarte „Kapazität“ werden detaillierte Informationen zur Datenkapazität der ausgewählten SVM angezeigt.

Für eine Storage-VM mit FlexVol volume oder FlexGroup -Volume werden folgende Informationen angezeigt:

- **Kapazität**

  Im Bereich „Kapazität“ werden Details zur verwendeten und verfügbaren Kapazität angezeigt, die allen Volumes zugewiesen wurde:

  - Gesamtkapazität

    Zeigt die Gesamtkapazität der Storage-VM an.

  - Gebraucht

    Zeigt den von Daten belegten Speicherplatz in den Volumes an, die zur Storage-VM gehören.

  - Garantiert verfügbar

    Zeigt den garantiert verfügbaren Speicherplatz für Daten an, der für Volumes in der Storage-VM

verfügbar ist.

- Nicht garantiert

  Zeigt den verbleibenden verfügbaren Speicherplatz für Daten an, der Thin Provisioning-Volumes in der Storage-VM zugewiesen ist.

- **Volumes mit Kapazitätsproblemen**

  Die Liste „Volumes mit Kapazitätsproblemen“ zeigt in tabellarischer Form Details zu den Volumes mit Kapazitätsproblemen an:

  - Status

    Zeigt an, dass das Volume ein kapazitätsbezogenes Problem mit einem angegebenen Schweregrad aufweist.

    Sie können den Zeiger über den Status bewegen, um weitere Informationen zu dem bzw. den für das Volume generierten kapazitätsbezogenen Ereignissen anzuzeigen.

    Wenn der Status des Volumes durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum der Ereignisauslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Über die Schaltfläche **Details anzeigen** können Sie weitere Informationen zur Veranstaltung anzeigen.

    Wenn der Status des Volumes durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu jedem dieser Ereignisse anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

    > ⓘ Ein Volume kann mehrere Ereignisse mit demselben oder unterschiedlichen Schweregrad aufweisen. Es wird jedoch nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Volume zwei Ereignisse mit den Schweregraden „Fehler“ und „Warnung“ aufweist, wird nur der Schweregrad „Fehler“ angezeigt.

  - Volumen

    Zeigt den Namen des Volumes an.

  - Verwendete Datenkapazität

    Zeigt als Diagramm Informationen zur Volume-Kapazitätsnutzung (in Prozent) an.

  - Tage bis zur vollständigen

    Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor das Volume seine volle Kapazität erreicht.

  - Thin Provisioning

    Zeigt an, ob für das ausgewählte Volume eine Speicherplatzgarantie festgelegt ist. Gültige Werte sind Ja und Nein.

- Aggregate

  Zeigt bei FlexVol -Volumes den Namen des Aggregats an, das das Volume enthält. Zeigt für FlexGroup -Volumes die Anzahl der Aggregate an, die in der FlexGroup verwendet werden.

Registerkarte „Konfiguration“

Auf der Registerkarte „Konfiguration“ werden Konfigurationsdetails zur ausgewählten Speicher-VM angezeigt, z. B. ihr Cluster, ihr Stammvolume, der Typ der darin enthaltenen Volumes (FlexVol Volumes), Richtlinien und der auf der Speicher-VM erstellte Schutz:

- **Überblick**
  - Cluster

    Zeigt den Namen des Clusters an, zu dem die Speicher-VM gehört.

  - Zulässiger Datenträgertyp

    Zeigt den Typ der Volumes an, die in der Speicher-VM erstellt werden können. Der Typ kann FlexVol oder FlexVol/ FlexGroup sein.

  - Stammvolumen

    Zeigt den Namen des Stammvolumes der Speicher-VM an.

  - Erlaubte Protokolle

    Zeigt die Art der Protokolle an, die auf der Speicher-VM konfiguriert werden können. Zeigt außerdem an, ob ein Protokoll aktiv ist ( ), runter ( ) oder ist nicht konfiguriert ( ).

- **Datennetzwerkschnittstellen**
  - NAS

    Zeigt die Anzahl der NAS-Schnittstellen an, die mit der Speicher-VM verknüpft sind. Zeigt außerdem an, ob die Schnittstellen aktiv sind ( ) oder nach unten ( ).

  - SAN

    Zeigt die Anzahl der SAN-Schnittstellen an, die mit der Speicher-VM verknüpft sind. Zeigt außerdem an, ob die Schnittstellen aktiv sind ( ) oder nach unten ( ).

  - FC-NVMe

    Zeigt die Anzahl der FC-NVMe-Schnittstellen an, die mit der Storage-VM verknüpft sind. Zeigt außerdem an, ob die Schnittstellen aktiv sind ( ) oder nach unten ( ).

- **Verwaltungsnetzwerkschnittstellen**
  - Verfügbarkeit

    Zeigt die Anzahl der Verwaltungsschnittstellen an, die mit der Storage-VM verknüpft sind. Zeigt außerdem an, ob die Verwaltungsschnittstellen aktiv sind ( ) oder nach unten ( ).

- **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 eine einzelne Richtlinie erstellt wird, oder die Anzahl der Exportrichtlinien, wenn mehrere Richtlinien erstellt werden.

- **Schutz**
  - Speicher-VM-DR

    Zeigt an, ob die ausgewählte Speicher-VM geschützt, Ziel- oder ungeschützt ist, und den Namen des Ziels, auf dem die Speicher-VM geschützt ist. Wenn die ausgewählte Speicher-VM das Ziel ist, werden die Details der Quell-Speicher-VM angezeigt. Im Falle einer Fan-Out-Aufteilung zeigt dieses Feld die Gesamtzahl der Ziel-Speicher-VMs an, auf denen die Speicher-VM geschützt ist. Über den Zähllink gelangen Sie zum Beziehungsraster der Speicher-VM, gefiltert nach der Quell-Speicher-VM.

  - Geschützte Volumes

    Zeigt die Anzahl der geschützten Volumes auf der ausgewählten Speicher-VM im Verhältnis zur Gesamtzahl der Volumes an. Wenn Sie eine Ziel-Speicher-VM anzeigen, gilt der Nummernlink für die Zielvolumes der ausgewählten Speicher-VM.

  - Ungeschützte Volumes

    Zeigt die Anzahl der ungeschützten Volumes auf der ausgewählten Speicher-VM an.

- **Dienstleistungen**
  - Typ

    Zeigt den Diensttyp an, der auf der Speicher-VM konfiguriert ist. Der Typ kann Domain Name System (DNS) oder Network Information Service (NIS) sein.

  - Status

    Zeigt den Status des Dienstes an, der Aktiv sein kann ( ), Runter ( ) oder Nicht konfiguriert ( ).

  - Domänenname

    Zeigt die vollqualifizierten Domänennamen (FQDNs) des DNS-Servers für die DNS-Dienste oder des NIS-Servers für die NIS-Dienste 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 die aktive IP-Adresse des NIS-Servers angezeigt. Wenn der NIS-Server deaktiviert ist, wird die Liste aller IP-Adressen angezeigt.

Registerkarte „Netzwerkschnittstellen“

Auf der Registerkarte „Netzwerkschnittstellen“ werden Details zu den Datennetzwerkschnittstellen (LIFs) angezeigt, die auf der ausgewählten Speicher-VM erstellt werden:

- **Netzwerkschnittstelle**

  Zeigt den Namen der Schnittstelle an, die auf der ausgewählten Speicher-VM erstellt wird.

- **Betriebsstatus**

  Zeigt den Betriebsstatus der Schnittstelle an, der Aktiv sein kann ( ), Runter ( ) oder Unbekannt ( ). Der Betriebsstatus einer Schnittstelle wird durch den Status ihrer physischen Ports bestimmt.

- **Verwaltungsstatus**

  Zeigt den Verwaltungsstatus der Schnittstelle an, der Aktiv sein kann ( ), Runter ( ) oder Unbekannt ( ). Der Verwaltungsstatus einer Schnittstelle wird vom Speicheradministrator gesteuert, um Änderungen an der Konfiguration vorzunehmen oder zu Wartungszwecken. Der Verwaltungsstatus kann vom Betriebsstatus abweichen. Wenn der Verwaltungsstatus einer Schnittstelle jedoch „Down“ lautet, ist der Betriebsstatus standardmäßig „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, z. B. CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe und FlexCache.

- **Rolle**

  Zeigt die Schnittstellenrolle an. Die Rollen können Daten oder Management sein.

- **Heimathafen**

  Zeigt den physischen Port an, mit dem die Schnittstelle ursprünglich verknüpft war.

- **Aktueller Hafen**

  Zeigt den physischen Port an, mit dem die Schnittstelle derzeit verknüpft ist. Wenn die Schnittstelle migriert wird, kann der aktuelle Port vom Home-Port abweichen.

- **Port-Set**

  Zeigt den Portsatz an, dem die Schnittstelle zugeordnet ist.

- **Failover-Richtlinie**

  Zeigt die Failover-Richtlinie an, die für die Schnittstelle konfiguriert ist. Für NFS-, CIFS- und FlexCache -Schnittstellen ist die Standard-Failover-Richtlinie „Next Available“ (Nächste verfügbare Option). Die Failover-Richtlinie gilt nicht für FC- und iSCSI-Schnittstellen.

- **Routing-Gruppen**

  Zeigt den Namen der Routinggruppe an. Weitere Informationen zu den Routen und dem Ziel-Gateway können Sie anzeigen, indem Sie auf den Namen der Routinggruppe klicken.

  Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt und daher wird für diese Cluster eine leere Spalte angezeigt.

- **Failover-Gruppe**

  Zeigt den Namen der Failover-Gruppe an.

Registerkarte „Qtrees“

Auf der Registerkarte „Qtrees“ werden Details zu Qtrees und ihren Kontingenten angezeigt. Sie können auf die Schaltfläche **Schwellenwerte bearbeiten** klicken, wenn Sie die Integritätsschwellenwerteinstellungen für die Qtree-Kapazität für einen oder mehrere Qtrees bearbeiten möchten.

Verwenden Sie die Schaltfläche **Exportieren**, um eine Datei mit durch Kommas getrennten Werten (.csv) zu erstellen, die die Details aller überwachten Qtrees enthält. Beim Exportieren in eine CSV-Datei können Sie wählen, ob Sie einen Qtrees-Bericht für die aktuelle Speicher-VM, für alle Speicher-VMs im aktuellen Cluster oder für alle Speicher-VMs für alle Cluster in Ihrem Rechenzentrum erstellen möchten. 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 ( ).

  Sie können den Zeiger über das Statussymbol bewegen, um weitere Informationen zu dem oder den für den Qtree generierten Ereignissen anzuzeigen.

  Wenn der Status des Qtree durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum der Ereignisauslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Mit **Details anzeigen** können Sie weitere Informationen zur Veranstaltung anzeigen.

  Wenn der Status des Qtree durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu jedem dieser Ereignisse anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch **Alle Ereignisse anzeigen** verwenden, um die Liste der generierten Ereignisse anzuzeigen.

  > Ein Qtree kann mehrere Ereignisse mit derselben oder 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.

- **Virtuelle Speichermaschine**

  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 Datenträgers an, der den Qtree enthält.

  Sie können den Zeiger über den Datenträgernamen bewegen, um weitere Informationen zum Datenträger anzuzeigen.

- **Kontingent festgelegt**

  Gibt an, ob im Qtree ein Kontingent aktiviert oder deaktiviert ist.

- **Kontingenttyp**

  Gibt an, ob das Kontingent für einen Benutzer, eine Benutzergruppe oder einen Qtree gilt. Erscheint nur in der exportierten CSV-Datei.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Für jeden Benutzer und jede Benutzergruppe gibt es mehrere Zeilen. Wenn der Kontingenttyp „qtree“ ist oder das Kontingent nicht festgelegt ist, ist die Spalte leer. Erscheint nur in der exportierten CSV-Datei.

- **Datenträgernutzung %**

  Zeigt den Prozentsatz des belegten Speicherplatzes an. Wenn ein Festplattenlimit festgelegt ist, basiert dieser Wert auf dem Festplattenlimit. Wenn das Kontingent ohne festes Festplattenlimit festgelegt wird, basiert der Wert auf dem Datenspeicherplatz des Volumes. Wenn das Kontingent nicht festgelegt ist oder die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind, wird auf der Rasterseite „Nicht zutreffend“ angezeigt und das Feld in den CSV-Exportdaten ist leer.

- **Festplattenlimit**

  Zeigt die maximale Menge an Speicherplatz an, die dem Qtree zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht ist und keine weiteren Schreibvorgänge auf die Festplatte mehr zulässig sind. Der Wert wird unter den folgenden Bedingungen als „Unbegrenzt“ angezeigt: wenn das Kontingent ohne Festplattenlimit festgelegt ist, wenn das Kontingent nicht festgelegt ist oder wenn die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind.

- **Festplatten-Softlimit**

  Zeigt die Menge an Speicherplatz an, die dem Qtree zugewiesen wird, bevor ein Warnereignis generiert wird. Der Wert wird unter den folgenden Bedingungen als „Unbegrenzt“ angezeigt: wenn das Kontingent ohne weiche Festplattenbegrenzung festgelegt ist, wenn das Kontingent nicht festgelegt ist oder wenn die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind. Standardmäßig ist diese Spalte ausgeblendet.

- **Festplattenschwelle**

  Zeigt den für den Speicherplatz festgelegten Schwellenwert an. Der Wert wird unter den folgenden Bedingungen als „Unbegrenzt“ angezeigt: wenn das Kontingent ohne Festplattenschwellenwert festgelegt ist, wenn das Kontingent nicht festgelegt ist oder wenn die 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 harte Dateilimit festgelegt ist,

basiert dieser Wert auf dem harten Dateilimit. Wenn das Kontingent ohne feste Dateibeschränkung festgelegt ist, wird kein Wert angezeigt. Wenn das Kontingent nicht festgelegt ist oder die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind, wird auf der Rasterseite „Nicht zutreffend“ angezeigt und das Feld in den CSV-Exportdaten ist leer.

- **Datei-Hartlimit**

  Zeigt die feste Grenze für die Anzahl der in den Qtrees zulässigen Dateien an. Der Wert wird unter den folgenden Bedingungen als „Unbegrenzt“ angezeigt: wenn das Kontingent ohne harte Dateibeschränkung festgelegt ist, wenn das Kontingent nicht festgelegt ist oder wenn die Kontingente auf dem Volume, zu dem der Qtree gehört, deaktiviert sind.

- **Datei-Softlimit**

  Zeigt das Soft-Limit für die Anzahl der in den Qtrees zulässigen Dateien an. Der Wert wird unter den folgenden Bedingungen als „Unbegrenzt“ angezeigt: wenn das Kontingent ohne weiche Dateibegrenzung festgelegt ist, wenn das Kontingent nicht festgelegt ist oder wenn die Kontingente auf dem Datenträger, zu dem der Qtree gehört, deaktiviert sind. Standardmäßig ist diese Spalte ausgeblendet.

Registerkarte „Benutzer- und Gruppenkontingente“

Zeigt Details zu den Benutzer- und Benutzergruppenkontingenten für die ausgewählte Speicher-VM an. Sie können Informationen wie den Status des Kontingents, den Namen des Benutzers oder der Benutzergruppe, die für die Datenträger und Dateien festgelegten weichen und harten Grenzwerte, die Menge des verwendeten Speicherplatzes und die Anzahl der Dateien sowie den Datenträgerschwellenwert anzeigen. Sie können auch die einem Benutzer oder einer Benutzergruppe zugeordnete E-Mail-Adresse ändern.

- **Befehlsschaltfläche „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. Sie können die E-Mail-Adresse 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 über dasselbe Kontingent verfügen, werden die Namen der Benutzer als durch Kommas getrennte Werte angezeigt. Außerdem wird die Standardregel nicht zum Generieren der E-Mail-Adresse verwendet. Daher müssen Sie die erforderliche E-Mail-Adresse angeben, damit Benachrichtigungen gesendet werden können.

- **Befehlsschaltfläche „E-Mail-Regeln konfigurieren“**

  Ermöglicht Ihnen das Erstellen oder Ändern von Regeln zum Generieren einer E-Mail-Adresse für die Benutzer- oder Benutzergruppenkontingente, die auf der Speicher-VM konfiguriert sind. Bei einer Quotenüberschreitung 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 ( ).

  Sie können den Zeiger über das Statussymbol bewegen, um weitere Informationen zu dem oder den für das Kontingent generierten Ereignissen anzuzeigen.

  Wenn der Status des Kontingents durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum der Ereignisauslösung, den Namen des

Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Mit **Details anzeigen** können Sie weitere Informationen zur Veranstaltung anzeigen.

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, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu jedem dieser Ereignisse anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch **Alle Ereignisse anzeigen** verwenden, um die Liste der generierten Ereignisse anzuzeigen.

Ein Kontingent kann mehrere Ereignisse mit demselben oder unterschiedlichen Schweregrad enthalten. Es wird jedoch nur der höchste Schweregrad angezeigt. Wenn beispielsweise ein Kontingent zwei Ereignisse mit den Schweregraden „Fehler“ und „Warnung“ aufweist, wird nur der Schweregrad „Fehler“ angezeigt.

- **Benutzer oder Gruppe**

  Zeigt den Namen des Benutzers oder der Benutzergruppe an. Wenn mehrere Benutzer über dasselbe Kontingent verfügen, werden die Namen der Benutzer als durch Kommas getrennte Werte angezeigt.

  Der Wert wird als „Unbekannt“ angezeigt, wenn ONTAP aufgrund von SecD-Fehlern keinen gültigen Benutzernamen bereitstellt.

- **Typ**

  Gibt an, ob das Kontingent für einen Benutzer oder eine Benutzergruppe gilt.

- **Volume oder Qtree**

  Zeigt den Namen des Volumes oder Qtree an, auf dem das Benutzer- oder Benutzergruppenkontingent angegeben ist.

  Sie können den Zeiger über den Namen des Volumes oder Qtree bewegen, um weitere Informationen zum Volume oder Qtree anzuzeigen.

- **Datenträgernutzung %**

  Zeigt den Prozentsatz des belegten Speicherplatzes an. Der Wert wird als „Nicht zutreffend“ angezeigt, wenn das Kontingent ohne feste Festplattenbegrenzung festgelegt ist.

- **Festplattenlimit**

  Zeigt die maximale Menge an Speicherplatz an, die für das Kontingent zugewiesen ist. Unified Manager generiert ein kritisches Ereignis, wenn dieses Limit erreicht ist und keine weiteren Schreibvorgänge auf die Festplatte mehr zulässig sind. Der Wert wird als „Unbegrenzt“ angezeigt, wenn das Kontingent ohne feste Festplattenbegrenzung festgelegt ist.

- **Festplatten-Softlimit**

  Zeigt die Menge an Speicherplatz an, die dem Kontingent zugewiesen ist, bevor ein Warnereignis generiert wird. Der Wert wird als „Unbegrenzt“ angezeigt, wenn das Kontingent ohne weiche Festplattenbegrenzung festgelegt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Festplattenschwelle**

Zeigt den für den Speicherplatz festgelegten Schwellenwert an. Der Wert wird als „Unbegrenzt“ angezeigt, wenn das Kontingent ohne Festplattenschwellenwert festgelegt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Verwendete Dateien %**

  Zeigt den Prozentsatz der im Qtree verwendeten Dateien an. Der Wert wird als „Nicht zutreffend“ angezeigt, wenn das Kontingent ohne harte Dateibeschränkung festgelegt ist.

- **Datei-Hartlimit**

  Zeigt die feste Grenze für die Anzahl der im Kontingent zulässigen Dateien an. Der Wert wird als „Unbegrenzt“ angezeigt, wenn das Kontingent ohne feste Dateibeschränkung festgelegt ist.

- **Datei-Softlimit**

  Zeigt das Soft-Limit für die Anzahl der im Kontingent zulässigen Dateien an. Der Wert wird als „Unbegrenzt“ angezeigt, wenn das Kontingent ohne weiche Dateibeschränkung festgelegt ist. Standardmäßig ist diese Spalte ausgeblendet.

- **E-Mail-Adresse**

  Zeigt die E-Mail-Adresse des Benutzers oder der Benutzergruppe an, an die Benachrichtigungen gesendet werden, wenn es zu einer Quotenüberschreitung kommt.

Registerkarte „NFS-Freigaben“

Auf der Registerkarte „NFS-Freigaben“ werden Informationen zu NFS-Freigaben angezeigt, z. B. deren Status, der mit dem Volume verknüpfte Pfad (FlexGroup Volumes oder FlexVol -Volumes), Zugriffsebenen von Clients auf die NFS-Freigaben und die für die exportierten Volumes definierte Exportrichtlinie. NFS-Freigaben werden unter folgenden Bedingungen nicht angezeigt: wenn das Volume nicht gemountet ist oder wenn die mit der Exportrichtlinie für das Volume verknüpften Protokolle keine NFS-Freigaben enthalten.

- **Status**

  Zeigt den aktuellen Status der NFS-Freigaben an. Der Status kann Fehler ( ) oder Normal ( ).

- **Kreuzungspfad**

  Zeigt den Pfad an, in dem das Volume eingebunden ist. Wenn eine explizite NFS-Exportrichtlinie auf einen Qtree angewendet wird, zeigt die Spalte den Pfad des Volumes an, über das auf den Qtree zugegriffen werden kann.

- **Kreuzungspfad aktiv**

  Zeigt an, ob der Pfad zum Zugriff auf das bereitgestellte Volume aktiv oder inaktiv ist.

- **Volume oder Qtree**

  Zeigt den Namen des Volumes oder Qtree an, auf das die NFS-Exportrichtlinie angewendet wird. Wenn eine NFS-Exportrichtlinie auf einen Qtree im Volume angewendet wird, zeigt die Spalte sowohl den Namen des Volumes als auch den des Qtree an.

  Über den Link können Sie sich Details zum Objekt auf der jeweiligen Detailseite anzeigen lassen. Wenn es sich bei dem Objekt um einen Qtree handelt, werden Links sowohl für den Qtree als auch für das Volume

angezeigt.

- **Volumenstatus**

  Zeigt den Status des Volumes an, das exportiert wird. Der Status kann „Offline“, „Online“, „Eingeschränkt“ oder „Gemischt“ sein.

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

  - Online

    Lese- und Schreibzugriff auf das Volume ist erlaubt.

  - Eingeschränkt

    Eingeschränkte Vorgänge, wie etwa die Rekonstruktion der Parität, sind zulässig, der Datenzugriff ist jedoch nicht gestattet.

  - Gemischt

    Die Bestandteile eines FlexGroup -Volumes befinden sich nicht alle im gleichen Zustand.

- **Sicherheitsstil**

  Zeigt die Zugriffsberechtigung für die zu exportierenden Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder Mixed sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume verfügen über UNIX-Berechtigungen.

  - Einheitlich

    Dateien und Verzeichnisse im Volume haben einen einheitlichen Sicherheitsstil.

  - NTFS (CIFS-Clients)

    Dateien und Verzeichnisse im 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 oktalen Zeichenfolgenformat an, das für die exportierten Datenträger festgelegt ist. Es ähnelt den Berechtigungsbits im UNIX-Stil.

- **Exportrichtlinie**

  Zeigt die Regeln an, die die Zugriffsberechtigung für exportierte Volumes definieren. Sie können auf den Link klicken, um Details zu den mit der Exportrichtlinie verknüpften Regeln anzuzeigen, z. B. zu den Authentifizierungsprotokollen und der Zugriffsberechtigung.

Registerkarte „SMB-Freigaben“

Zeigt Informationen zu den SMB-Freigaben auf der ausgewählten Speicher-VM an. Sie können Informationen wie den Status der SMB-Freigabe, den Freigabenamen, den mit der Speicher-VM verknüpften Pfad, den Status des Verbindungspfads der Freigabe, das enthaltene Objekt, den Status des enthaltenden Volumes, die Sicherheitsdaten der Freigabe und die für die Freigabe definierten Exportrichtlinien anzeigen. Sie können auch feststellen, ob ein äquivalenter NFS-Pfad für die SMB-Freigabe vorhanden ist.

Freigaben in Ordnern werden auf der Registerkarte „SMB-Freigaben“ nicht angezeigt.

- **Befehlsschaltfläche „Benutzerzuordnung anzeigen“**

  Öffnet das Dialogfeld „Benutzerzuordnung“.

  Sie können die Details der Benutzerzuordnung für die Speicher-VM anzeigen.

- **ACL-Befehlsschaltfläche anzeigen**

  Öffnet das Dialogfeld „Zugriffskontrolle“ für die Freigabe.

  Sie können Benutzer- und Berechtigungsdetails für die ausgewählte Freigabe anzeigen.

- **Status**

  Zeigt den aktuellen Status der Freigabe an. Der Status kann Normal ( ) oder Fehler ( ).

- **Freigabename**

  Zeigt den Namen der SMB-Freigabe an.

- **Weg**

  Zeigt den Verbindungspfad an, auf dem die Freigabe erstellt wird.

- **Kreuzungspfad aktiv**

  Zeigt an, ob der Pfad zum Zugriff auf die Freigabe aktiv oder inaktiv ist.

- **Enthaltendes Objekt**

  Zeigt den Namen des enthaltenen Objekts an, zu dem die Freigabe gehört. Das enthaltene Objekt kann ein Volume oder ein Qtree sein.

  Durch Klicken auf den Link können Sie Details zum enthaltenen Objekt auf der jeweiligen Detailseite anzeigen. Wenn das enthaltene Objekt ein Qtree ist, werden Links sowohl für den Qtree als auch für das Volume angezeigt.

- **Volumenstatus**

  Zeigt den Status des Volumes an, das exportiert wird. Der Status kann „Offline“, „Online“, „Eingeschränkt“ oder „Gemischt“ sein.

  - Offline

    Lese- oder Schreibzugriff auf das Volume ist nicht zulässig.

- Online

  Lese- und Schreibzugriff auf das Volume ist erlaubt.

- Eingeschränkt

  Eingeschränkte Vorgänge, wie etwa die Rekonstruktion der Parität, sind zulässig, der Datenzugriff ist jedoch nicht gestattet.

- Gemischt

  Die Bestandteile eines FlexGroup -Volumes befinden sich nicht alle im gleichen Zustand.

- **Sicherheit**

  Zeigt die Zugriffsberechtigung für die zu exportierenden Volumes an. Der Sicherheitsstil kann UNIX, Unified, NTFS oder Mixed sein.

  - UNIX (NFS-Clients)

    Dateien und Verzeichnisse im Volume verfügen über UNIX-Berechtigungen.

  - Einheitlich

    Dateien und Verzeichnisse im Volume haben einen einheitlichen Sicherheitsstil.

  - NTFS (CIFS-Clients)

    Dateien und Verzeichnisse im 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 Speicher-VM keine Exportrichtlinie angegeben ist, wird der Wert als „Nicht aktiviert“ angezeigt.

  Sie können auf den Link klicken, um Details zu den mit der Exportrichtlinie verknüpften Regeln anzuzeigen, z. B. Zugriffsprotokolle und Berechtigungen. Der Link ist deaktiviert, wenn die Exportrichtlinie für die ausgewählte Speicher-VM deaktiviert ist.

- **NFS-Äquivalent**

  Gibt an, ob es für die Freigabe ein NFS-Äquivalent gibt.

Registerkarte „SAN“

Zeigt Details zu LUNs, Initiatorgruppen und Initiatoren für die ausgewählte Speicher-VM an. Standardmäßig wird die LUN-Ansicht angezeigt. Sie können Details zu den Initiatorgruppen auf der Registerkarte „Initiatorgruppen“ und Details zu Initiatoren auf der Registerkarte „Initiatoren“ anzeigen.

- **Registerkarte „LUNs“**

Zeigt Details zu den LUNs an, die zur ausgewählten Speicher-VM gehören. Sie können Informationen wie den LUN-Namen, den LUN-Status (online oder offline), den Namen des Dateisystems (Volume oder Qtree), das die LUN enthält, den Typ des Host-Betriebssystems, die Gesamtdatenkapazität und die Seriennummer der LUN anzeigen. Die Spalte „LUN-Leistung“ enthält einen Link zur Seite mit den LUN-/Leistungsdetails.

Sie können auch Informationen darüber anzeigen, ob Thin Provisioning auf der LUN aktiviert ist und ob die LUN einer Initiatorgruppe zugeordnet ist. Wenn es einem Initiator zugeordnet ist, können Sie die Initiatorgruppen und Initiatoren anzeigen, die der ausgewählten LUN zugeordnet sind.

- **Registerkarte „Initiatorgruppen“**

  Zeigt Details zu Initiatorgruppen an. Sie können Details wie den Namen der Initiatorgruppe, den Zugriffsstatus, den Typ des Hostbetriebssystems, das von allen Initiatoren in der Gruppe verwendet wird, und das unterstützte Protokoll anzeigen. Wenn Sie auf den Link in der Spalte „Zugriffsstatus“ klicken, können Sie den aktuellen Zugriffsstatus der Initiatorgruppe anzeigen.

  - **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.

    Sie können anzeigen, ob Initiatorgruppen allen Schnittstellen oder bestimmten Schnittstellen über einen Portsatz zugeordnet sind. Wenn Sie in der Spalte „Zugeordnete Schnittstellen“ auf den Zähllink klicken, werden entweder alle Schnittstellen oder bestimmte Schnittstellen für einen Portsatz angezeigt. Schnittstellen, die über das Zielportal abgebildet werden, werden nicht angezeigt. Es wird die Gesamtzahl der Initiatoren und LUNs angezeigt, die einer Initiatorgruppe zugeordnet sind.

  Sie können auch die LUNs und Initiatoren anzeigen, die der ausgewählten Initiatorgruppe zugeordnet sind.

- **Registerkarte „Initiatoren“**

  Zeigt den Namen und Typ des Initiators und die Gesamtzahl der diesem Initiator zugeordneten Initiatorgruppen für die ausgewählte Speicher-VM an.

```
initiator groups that are mapped to the selected initiator group.
```

Bereich „Zugehörige Anmerkungen“

Im Bereich „Verwandte Anmerkungen“ können Sie die Anmerkungsdetails anzeigen, die mit der ausgewählten Speicher-VM verknüpft sind. Zu den Details gehören der Annotation-Name und die Annotation-Werte, die auf die Speicher-VM angewendet werden. Sie können manuelle Anmerkungen auch aus dem Bereich „Verwandte Anmerkungen“ entfernen.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie die Cluster, Aggregate und Volumes anzeigen, die mit der Speicher-VM in Zusammenhang stehen:

- **Cluster**

  Zeigt den Integritätsstatus des Clusters an, zu dem die Speicher-VM gehört.

- **Aggregate**

  Zeigt die Anzahl der Aggregate an, die zur ausgewählten Speicher-VM gehören. Der Integritätsstatus der Aggregate wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn eine Speicher-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 Speicher-VM zugewiesen sind. Der Integritätsstatus der Aggregate wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad.

- **Bände**

  Zeigt die Anzahl und Kapazität der Volumes an, die zur ausgewählten Speicher-VM gehören. Der Integritätsstatus der Volumes wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn in der Speicher-VM FlexGroup -Volumes vorhanden sind, umfasst die Zählung auch FlexGroups, nicht jedoch FlexGroup Bestandteile.

Bereich „Verwandte Gruppen“

Im Bereich „Verwandte Gruppen“ können Sie die Liste der Gruppen anzeigen, die mit der ausgewählten Speicher-VM verknüpft sind.

Bereich „Zugehörige Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnungen anzeigen, die für die ausgewählte Speicher-VM erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link **Warnung hinzufügen** klicken, oder eine vorhandene Warnung bearbeiten, indem Sie auf den Warnungsnamen klicken.

Cluster-/Integritätsdetailseite

Die Seite „Cluster-/Integritätsdetails“ bietet ausführliche Informationen zu einem ausgewählten Cluster, z. B. Integrität, Kapazität und Konfigurationsdetails. Sie können auch Informationen zu den Netzwerkschnittstellen (LIFs), Knoten, Datenträgern, zugehörigen Geräten und zugehörigen Warnungen für den Cluster anzeigen.

Der Status neben dem Clusternamen, z. B. (Gut), stellt den Kommunikationsstatus dar, d. h., ob Unified Manager mit dem Cluster kommunizieren kann. Es stellt nicht den Failover-Status oder den Gesamtstatus des Clusters dar.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für den ausgewählten Cluster ausführen:

- **Zur Leistungsansicht wechseln**

  Ermöglicht Ihnen die Navigation zur Seite mit den Cluster-/Leistungsdetails.

- **Aktionen**

  - Alarm hinzufügen: Öffnet das Dialogfeld „Alarm hinzufügen“, in dem Sie dem ausgewählten Cluster einen Alarm hinzufügen können.
  - Neu erkennen: Leitet eine manuelle Aktualisierung des Clusters ein, wodurch Unified Manager aktuelle Änderungen am Cluster erkennen kann.

    Wenn Unified Manager mit OnCommand Workflow Automation gekoppelt ist, werden beim Wiedererkennungsvorgang auch zwischengespeicherte Daten von WFA erneut abgerufen, sofern vorhanden.

  Nachdem der Neuerkennungsvorgang gestartet wurde, wird ein Link zu den zugehörigen Auftragsdetails angezeigt, um die Verfolgung des Auftragsstatus zu ermöglichen.

  - Kommentieren: Ermöglicht Ihnen, den ausgewählten Cluster mit Anmerkungen zu versehen.

- **Cluster anzeigen**

  Ermöglicht Ihnen die Navigation zur Ansicht „Integrität: Alle Cluster“.

Registerkarte „Integrität“

Zeigt detaillierte Informationen zu Problemen mit der Datenverfügbarkeit und Datenkapazität verschiedener Clusterobjekte wie Knoten, SVMs und Aggregaten an. Verfügbarkeitsprobleme hängen mit der Datenbereitstellungskapazität der Clusterobjekte zusammen. Kapazitätsprobleme hängen mit der Datenspeicherkapazität der Clusterobjekte zusammen.

Sie können auf das Diagramm eines Objekts klicken, um eine gefilterte Liste der Objekte anzuzeigen. Sie können beispielsweise auf das SVM-Kapazitätsdiagramm klicken, das Warnungen anzeigt, um eine gefilterte Liste von SVMs anzuzeigen. Diese Liste enthält SVMs mit Volumes oder Qtrees, die Kapazitätsprobleme mit dem Schweregrad „Warnung“ aufweisen. Sie können auch auf das SVM-Verfügbarkeitsdiagramm klicken, das Warnungen anzeigt, um die Liste der SVMs anzuzeigen, bei denen Verfügbarkeitsprobleme mit dem Schweregrad „Warnung“ vorliegen.

Verfügbarkeitsprobleme

Zeigt grafisch die Gesamtzahl der Objekte an, einschließlich der Objekte mit Verfügbarkeitsproblemen und der Objekte ohne Verfügbarkeitsprobleme. Die Farben im Diagramm stellen die unterschiedlichen Schweregrade der Probleme dar. Die Informationen unter dem Diagramm enthalten Einzelheiten zu Verfügbarkeitsproblemen, die die Verfügbarkeit von Daten im Cluster beeinträchtigen können oder bereits beeinträchtigt haben. Beispielsweise werden Informationen zu ausgefallenen Festplatten-Shelves und offline geschalteten Aggregaten angezeigt.

> Die für das SFO-Balkendiagramm angezeigten Daten basieren auf dem HA-Status der Knoten. Die für alle anderen Balkendiagramme angezeigten Daten werden basierend auf den generierten Ereignissen berechnet.

Kapazitätsprobleme

Zeigt grafisch die Gesamtzahl der Objekte an, einschließlich der Objekte mit Kapazitätsproblemen und der

Objekte ohne kapazitätsbezogene Probleme. Die Farben im Diagramm stellen die unterschiedlichen Schweregrade der Probleme dar. Die Informationen unter dem Diagramm liefern Details zu Kapazitätsproblemen, die sich auf die Datenkapazität im Cluster auswirken können oder bereits ausgewirkt haben. Beispielsweise werden Informationen zu Aggregaten angezeigt, bei denen die Wahrscheinlichkeit einer Überschreitung der festgelegten Schwellenwerte besteht.

Registerkarte „Kapazität“

Zeigt detaillierte Informationen zur Kapazität des ausgewählten Clusters an.

Kapazität

Zeigt das Datenkapazitätsdiagramm zur genutzten und verfügbaren Kapazität aller zugewiesenen Aggregate an:

- Verwendeter logischer Speicherplatz

  Die tatsächliche Größe der Daten, die auf allen Aggregaten dieses Clusters gespeichert werden, ohne Berücksichtigung der Einsparungen durch die Verwendung von ONTAP Speichereffizienztechnologien. Snapshot-Kopien sind hiervon nicht umfasst.

- Datenreduktion

  Zeigt das Verhältnis ohne Snapshot-Kopien und mit zwei signifikanten Ziffern an, beispielsweise 1,8 zu 1. Dieses Verhältnis basiert auf den konfigurierten ONTAP Speichereffizienzeinstellungen.

- Gebraucht

  Die physische Kapazität, die von Daten auf allen Aggregaten verwendet wird. Darin ist die Kapazität nicht enthalten, die für Parität, Größenanpassung und Reservierung verwendet wird.

- Verfügbar

  Zeigt die für Daten verfügbare Kapazität an.

- Ersatzteile

  Zeigt die verfügbare Speicherkapazität aller Ersatzfestplatten an.

- Bereitgestellt

  Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

Details

Zeigt detaillierte Informationen zur genutzten und verfügbaren Kapazität an. Die Berechnung schließt die Stammaggregatdaten aus.

- Gesamtkapazität

  Zeigt die Gesamtkapazität des Clusters an. Darin ist die für die Parität zugewiesene Kapazität nicht enthalten.

- Gebraucht

Zeigt die von Daten verwendete Kapazität an. Darin ist die Kapazität nicht enthalten, die für Parität, Größenanpassung und Reservierung verwendet wird.

- Verfügbar

  Zeigt die für Daten verfügbare Kapazität an.

- Bereitgestellt

  Zeigt die Kapazität an, die für alle zugrunde liegenden Volumes bereitgestellt wird.

- Ersatzteile

  Zeigt die verfügbare Speicherkapazität aller Ersatzfestplatten an.

Cloud-Ebene

Zeigt die insgesamt verwendete Cloud-Tier-Kapazität und die für jede verbundene Cloud-Tier verwendete Kapazität für FabricPool-fähige Aggregate im Cluster an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

Aufschlüsselung der physischen Kapazität nach Festplattentyp

Im Bereich „Aufschlüsselung der physischen Kapazität nach Datenträgertyp“ werden ausführliche Informationen zur Datenträgerkapazität der verschiedenen Datenträgertypen im Cluster angezeigt. Durch Klicken auf den Datenträgertyp können Sie auf der Registerkarte „Datenträger“ weitere Informationen zum Datenträgertyp anzeigen.

- Gesamtnutzkapazität

  Zeigt die verfügbare Kapazität und die freie Kapazität der Datenträger an.

- Festplatte

  Zeigt die genutzte und die verfügbare Kapazität aller HDD-Datenträger im Cluster grafisch an. Die gepunktete Linie stellt die freie Kapazität der Datenträger in der Festplatte dar.

- Blitz
  - SSD-Daten

    Zeigt die genutzte und die verfügbare Kapazität der SSD-Datenträger im Cluster grafisch an.

  - SSD-Cache

    Zeigt grafisch die speicherbare Kapazität der SSD-Cache-Festplatten im Cluster an.

  - SSD-Ersatz

    Zeigt die freie Kapazität der SSD-, Daten- und Cache-Festplatten im Cluster grafisch an.

- Nicht zugewiesene Datenträger

  Zeigt die Anzahl nicht zugewiesener Festplatten im Cluster an.

Liste der Aggregate mit Kapazitätsproblemen

Zeigt in tabellarischer Form Details zur genutzten und verfügbaren Kapazität der Aggregate an, bei denen Kapazitätsrisikoprobleme vorliegen.

- Status

  Zeigt an, dass das Aggregat ein kapazitätsbezogenes Problem einer bestimmten Schwere aufweist.

  Sie können den Zeiger über den Status bewegen, um weitere Informationen zu dem Ereignis oder den für das Aggregat generierten Ereignissen anzuzeigen.

  Wenn der Status des Aggregats durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum der Ereignisauslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Sie können auf die Schaltfläche **Details anzeigen** klicken, um weitere Informationen zum Ereignis anzuzeigen.

  Wenn der Status des Aggregats durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu jedem dieser Ereignisse anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

  > Ein Aggregat kann mehrere kapazitätsbezogene Ereignisse mit demselben oder unterschiedlichen Schweregrad 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.

- Verwendete Datenkapazität

  Zeigt grafisch Informationen zur Gesamtkapazitätsnutzung (in Prozent) an.

- Tage bis zur vollständigen

  Zeigt die geschätzte Anzahl der verbleibenden Tage an, bevor das Aggregat seine volle Kapazität erreicht.

Registerkarte „Konfiguration“

Zeigt Details zum ausgewählten Cluster an, z. B. IP-Adresse, Kontakt und Standort:

Clusterübersicht

- Verwaltungsschnittstelle

  Zeigt das Cluster-Management-LIF an, das Unified Manager zum Herstellen einer Verbindung mit dem Cluster verwendet. Außerdem wird der Betriebszustand der Schnittstelle angezeigt.

- Hostname oder IP-Adresse

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Cluster-Management-LIF an, das Unified

Manager für die Verbindung mit dem Cluster verwendet.

- FQDN

  Zeigt den vollqualifizierten Domänennamen (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 früheste ONTAP Version angezeigt.

- Kontakt

  Zeigt Details zum 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 Remote-Cluster

Bietet Details zum Remote-Cluster in einer MetroCluster -Konfiguration. Diese Informationen werden nur für MetroCluster -Konfigurationen angezeigt.

- Cluster

  Zeigt den Namen des Remote-Clusters an. Sie können auf den Clusternamen klicken, um zur Detailseite des Clusters zu navigieren.

- 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 -Übersicht

Bietet Details zum lokalen Cluster in einer MetroCluster over FC- oder MetroCluster over IP-Konfiguration. Diese Informationen werden nur für MetroCluster über FC- oder IP-Konfigurationen angezeigt.

- Typ

  Zeigt an, ob der MetroCluster -Typ zwei oder vier Knoten hat. Für MetroCluster über IP werden nur vier Knoten unterstützt.

- Konfiguration

  Zeigt die MetroCluster -Konfiguration über FC und IP an, die die folgenden Werte haben kann:

Für FC

- Stretch-Konfiguration mit SAS-Kabeln
- Stretch-Konfiguration mit FC-SAS-Brücke
- Fabric-Konfiguration mit FC-Switches

> Für einen 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 für den lokalen Cluster ein automatisierter ungeplanter Switchover aktiviert ist. Standardmäßig ist AUSO für alle Cluster in einer MetroCluster -Konfiguration mit zwei Knoten in Unified Manager aktiviert. Sie können die AUSO-Einstellung über die Befehlszeilenschnittstelle ändern. Dies wird nur für MetroCluster über 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 aktiven Knoten an ( ) oder nach unten ( ) im Cluster.

- 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 auf zwei Knoten ONTAP 9.6 und auf einem Knoten ONTAP 9.3 ausgeführt wird.

Virtuelle Speichermaschinen

- Verfügbarkeit

  Zeigt die Anzahl der aktiven SVMs an ( ) oder nach unten ( ) im Cluster.

Netzwerkschnittstellen

- Verfügbarkeit

  Zeigt die Anzahl der aktiven Nicht-Daten-LIFs an ( ) oder nach unten ( ) im Cluster.

- 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 lizenzierten Datenprotokolle an, die für den Cluster aktiviert sind. Zu den Datenprotokollen gehören iSCSI, CIFS, NFS, NVMe und FC/FCoE.

Schutz

- Mediatoren

  Zeigt an, ob der Cluster Mediatoren unterstützt und den Konnektivitätsstatus des Mediators. Es zeigt an, ob der Mediator konfiguriert ist, und wenn ja, wird der Status der Mediatoren angezeigt.

  - Nicht zutreffend

    Wird angezeigt, wenn der Cluster keine Mediatoren unterstützt.

  - Nicht konfiguriert

    Wird angezeigt, wenn der Cluster Mediatoren unterstützt, der Mediator jedoch nicht konfiguriert ist.

  - IP-Adresse

    Wird angezeigt, wenn der Cluster Mediatoren unterstützt und der Mediator konfiguriert ist. Der Mediatorstatus wird durch die Farbe angezeigt. Die Farbe Grün zeigt an, dass der Mediatorstatus erreichbar ist. Die Farbe Rot zeigt an, dass der Mediatorstatus nicht erreichbar ist.

Cloud-Ebenen

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) aufgelistet.

Registerkarte „MetroCluster -Konnektivität“

Zeigt die Probleme und den Verbindungsstatus der Clusterkomponenten in der MetroCluster -over-FC -Konfiguration an. Ein Cluster wird in einem roten Kästchen angezeigt, wenn der Disaster Recovery-Partner des Clusters Probleme hat.

Die Registerkarte „MetroCluster -Konnektivität“ wird nur für Cluster angezeigt, die sich in einer MetroCluster über-FC-Konfiguration befinden.

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 Zähllink einer Komponente klicken. Wenn Sie beispielsweise auf den Zähllink des Knotens im Cluster klicken, wird die Knotenregisterkarte auf der Detailseite des Clusters angezeigt. Wenn Sie auf den Link „Zählen“ der Datenträger im Remote-Cluster klicken, wird die Registerkarte „Datenträger“ auf der Detailseite des Remote-Clusters angezeigt.

Wenn Sie bei der Verwaltung einer MetroCluster Konfiguration mit acht Knoten auf den Link „Zählen“ der Komponente „Disk Shelves“ klicken, werden nur die lokalen Shelves des Standard-HA-Paares angezeigt. Außerdem gibt es keine Möglichkeit, die lokalen Regale auf dem anderen HA-Paar anzuzeigen.

Sie können den Zeiger über die Komponenten bewegen, um im Falle eines Problems die Details und den Konnektivitätsstatus der Cluster anzuzeigen und weitere Informationen zu dem oder den für das Problem generierten Ereignissen anzuzeigen.

Wenn der Status des Konnektivitätsproblems zwischen Komponenten durch ein einzelnes Ereignis bestimmt wird, können Sie Informationen wie den Ereignisnamen, die Uhrzeit und das Datum der Ereignisauslösung, den Namen des Administrators, dem das Ereignis zugewiesen ist, und die Ursache des Ereignisses anzeigen. Über die Schaltfläche „Details anzeigen“ erhalten Sie weitere Informationen zum Ereignis.

Wenn der Status des Konnektivitätsproblems zwischen Komponenten durch mehrere Ereignisse mit demselben Schweregrad bestimmt wird, werden die drei wichtigsten Ereignisse mit Informationen wie dem Ereignisnamen, der Uhrzeit und dem Datum, an dem die Ereignisse ausgelöst wurden, und dem Namen des Administrators angezeigt, dem das Ereignis zugewiesen ist. Sie können weitere Details zu jedem dieser Ereignisse anzeigen, indem Sie auf den Ereignisnamen klicken. Sie können auch auf den Link **Alle Ereignisse anzeigen** klicken, um die Liste der generierten Ereignisse anzuzeigen.

Registerkarte „MetroCluster -Replikation“

Zeigt den Status der Daten an, die in einer MetroCluster over-FC-Konfiguration repliziert werden. Sie können die Registerkarte „MetroCluster -Replikation“ verwenden, um den Datenschutz sicherzustellen, indem Sie die Daten synchron mit den bereits per Peering verbundenen Clustern spiegeln. Ein Cluster wird in einem roten Kästchen angezeigt, wenn der Disaster Recovery-Partner des Clusters Probleme hat.

Die Registerkarte „MetroCluster -Replikation“ wird nur für Cluster angezeigt, die sich in einer MetroCluster über-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 einsehen. Dies hilft dabei, die Probleme zu identifizieren, die beim Spiegeln von Metadaten und Daten auftreten können.

Auf der Registerkarte „MetroCluster -Replikation“ bietet der lokale Cluster die detaillierte grafische Darstellung des ausgewählten Clusters und der MetroCluster Partner bezieht sich auf den Remote-Cluster.

Registerkarte „Netzwerkschnittstellen“

Zeigt Details zu allen Nicht-Daten-LIFs an, die auf dem ausgewählten Cluster erstellt werden.

Netzwerkschnittstelle

Zeigt den Namen des LIF an, das auf dem ausgewählten Cluster erstellt wird.

Betriebsstatus

Zeigt den Betriebsstatus der Schnittstelle an, der Aktiv sein kann ( ), Runter ( ) oder Unbekannt ( ). Der Betriebsstatus einer Netzwerkschnittstelle wird durch den Status ihrer physischen Ports bestimmt.

Verwaltungsstatus

Zeigt den Verwaltungsstatus der Schnittstelle an, der Aktiv sein kann ( ), Runter ( ) oder Unbekannt ( ). Sie können den Verwaltungsstatus einer Schnittstelle steuern, wenn Sie Änderungen an der Konfiguration vornehmen oder während der Wartung. Der Verwaltungsstatus kann vom Betriebsstatus abweichen. Wenn der Verwaltungsstatus eines LIF jedoch „Down“ lautet, ist der Betriebsstatus standardmäßig „Down“.

IP-Adresse

Zeigt die IP-Adresse der Schnittstelle an.

Rolle

Zeigt die Rolle der Schnittstelle an. Mögliche Rollen sind Cluster-Management-LIFs, Node-Management-LIFs, Cluster-LIFs und Intercluster-LIFs.

Heimathafen

Zeigt den physischen Port an, mit dem die Schnittstelle ursprünglich verknüpft war.

Aktueller Port

Zeigt den physischen Port an, mit dem die Schnittstelle derzeit verknüpft ist. Nach der LIF-Migration kann der aktuelle Port vom Home-Port abweichen.

Failover-Richtlinie

Zeigt die Failover-Richtlinie an, die für die Schnittstelle konfiguriert ist.

Routinggruppen

Zeigt den Namen der Routinggruppe an. Weitere Informationen zu den Routen und dem Ziel-Gateway können Sie anzeigen, indem Sie auf den Namen der Routinggruppe klicken.

Routinggruppen werden für ONTAP 8.3 oder höher nicht unterstützt und daher wird für diese Cluster eine leere Spalte angezeigt.

Failover-Gruppe

Zeigt den Namen der Failover-Gruppe an.

Registerkarte „Knoten“

Zeigt Informationen zu Knoten im ausgewählten Cluster an. Sie können detaillierte Informationen zu den HA-Paaren, Festplatten-Shelves und Ports anzeigen:

HA-Details

Bietet eine bildliche Darstellung des HA-Status und des Integritätsstatus der Knoten im HA-Paar. Der Integritätsstatus des Knotens wird durch die folgenden Farben angezeigt:

- **Grün**

  Der Knoten ist in einem funktionsfähigen Zustand.

- **Gelb**

  Der Knoten hat den Partnerknoten übernommen oder der Knoten hat mit Umweltproblemen zu kämpfen.

- **Rot**

  Der Knoten ist ausgefallen.

Sie können Informationen zur Verfügbarkeit des HA-Paares anzeigen und die erforderlichen Maßnahmen ergreifen, um Risiken zu vermeiden. Beispielsweise wird im Falle einer möglichen Übernahmeoperation die folgende Meldung angezeigt: Speicher-Failover möglich.

Sie können eine Liste der Ereignisse im Zusammenhang mit dem HA-Paar und seiner Umgebung anzeigen, z. B. Lüfter, Netzteile, NVRAM Batterie, Flash-Karten, Serviceprozessor und Konnektivität von Festplattenregalen. Sie können auch den Zeitpunkt anzeigen, zu dem die Ereignisse ausgelöst wurden.

Sie können weitere knotenbezogene Informationen anzeigen, beispielsweise die Modellnummer.

Wenn Cluster mit einem einzigen Knoten vorhanden sind, können Sie auch Details zu den Knoten anzeigen.

Festplattenregale

Zeigt Informationen zu den Festplatten-Shelves im HA-Paar an.

Sie können auch die für die Festplatten-Shelves und die Umgebungskomponenten generierten Ereignisse sowie den Zeitpunkt der Auslösung der Ereignisse anzeigen.

- **Regal-ID**

  Zeigt die ID des Shelfs an, in dem sich die Festplatte befindet.

- **Komponentenstatus**

  Zeigt Umgebungsdetails der Festplattenregale an, z. B. Netzteile, Lüfter, Temperatursensoren, Stromsensoren, Festplattenkonnektivität und Spannungssensoren. Die Umgebungsdetails werden als Symbole in den folgenden Farben angezeigt:

  - **Grün**

    Die Umweltkomponenten funktionieren ordnungsgemäß.

  - **Grau**

    Zu den Umweltkomponenten liegen keine Daten vor.

  - **Rot**

Einige der Umweltkomponenten sind ausgefallen.

- **Zustand**

  Zeigt den Status des Festplattenregals an. Die möglichen Zustände sind „Offline“, „Online“, „Kein Status“, „Initialisierung erforderlich“, „Fehlt“ und „Unbekannt“.

- **Modell**

  Zeigt die Modellnummer des Festplattenregals an.

- **Lokales Festplattenregal**

  Gibt an, ob sich das Festplattenregal auf dem lokalen Cluster oder dem Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster -Konfiguration angezeigt.

- **Eindeutige ID**

  Zeigt die eindeutige Kennung des Festplatten-Shelfs an.

- **Firmware-Version**

  Zeigt die Firmware-Version des Festplatten-Shelfs an.

Häfen

Zeigt Informationen zu den zugehörigen FC-, FCoE- und Ethernet-Ports an. Sie können Details zu den Ports und den zugehörigen LIFs anzeigen, indem Sie auf die Portsymbole klicken.

Sie können auch die für die Ports generierten Ereignisse anzeigen.

Sie können die folgenden Portdetails anzeigen:

- Port-ID

  Zeigt den Namen des Ports an. Die Portnamen können beispielsweise e0M, e0a und e0b sein.

- Rolle

  Zeigt die Rolle des Ports an. Die möglichen Rollen sind Cluster, Daten, Intercluster, Knotenverwaltung und Undefiniert.

- Typ

  Zeigt das für den Port verwendete Protokoll der physischen Schicht 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. Die möglichen Zustände sind „Up“, „Down“, „Link Not Connected“ oder „Unknown“ ( ).

  Sie können die portbezogenen Ereignisse in der Ereignisliste anzeigen. Sie können auch die zugehörigen LIF-Details anzeigen, z. B. LIF-Name, Betriebsstatus, IP-Adresse oder WWPN, Protokolle, Name der mit dem LIF verknüpften SVM, aktueller Port, Failover-Richtlinie und Failover-Gruppe.

Registerkarte „Datenträger“

Zeigt Details zu den Datenträgern im ausgewählten Cluster an. Sie können datenträgerbezogene Informationen anzeigen, beispielsweise die Anzahl der verwendeten Datenträger, Ersatzdatenträger, defekten Datenträger und nicht zugewiesenen Datenträger. Sie können auch andere Details wie den Datenträgernamen, den Datenträgertyp und den Besitzerknoten des Datenträgers anzeigen.

Zusammenfassung des Datenträgerpools

Zeigt die Anzahl der Datenträger an, die nach effektiven Typen (FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN und VMDISK) kategorisiert sind, sowie den Status der Datenträger. Sie können auch andere Details anzeigen, beispielsweise die Anzahl der Aggregate, gemeinsam genutzten Datenträger, Ersatzdatenträger, defekten Datenträger, nicht zugewiesenen Datenträger und nicht unterstützten Datenträger. Wenn Sie auf den Link zur Anzahl der effektiven Datenträgertypen klicken, werden Datenträger des ausgewählten Status und des effektiven Typs angezeigt. Wenn Sie beispielsweise auf den Zähllink für den Datenträgerstatus „Defekt“ und den effektiven Typ „SAS“ klicken, werden alle Datenträger mit dem Datenträgerstatus „Defekt“ und dem effektiven Typ „SAS“ angezeigt.

Scheibe

Zeigt den Namen der Festplatte an.

RAID-Gruppen

Zeigt den Namen der RAID-Gruppe an.

Besitzerknoten

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: Aggregiert, Gemeinsam genutzt, Ersatz, Defekt, Nicht zugewiesen, Nicht unterstützt oder Unbekannt. Standardmäßig ist diese Spalte so sortiert, dass die Zustände in der folgenden Reihenfolge angezeigt werden: Defekt, Nicht zugewiesen, Nicht unterstützt, Ersatz, Aggregiert und Gemeinsam genutzt.

Lokale Festplatte

Zeigt entweder „Ja“ oder „Nein“ an, um anzugeben, ob sich die Festplatte im lokalen Cluster oder im Remote-Cluster befindet. Diese Spalte wird nur für Cluster in einer MetroCluster -Konfiguration angezeigt.

Position

Zeigt die Position der Festplatte basierend auf ihrem Containertyp an: beispielsweise Kopie, Daten oder Parität. Standardmäßig ist diese Spalte ausgeblendet.

Betroffene Aggregate

Zeigt die Anzahl der Aggregate an, die aufgrund der ausgefallenen Festplatte betroffen sind. Sie können den Zeiger über den Zähllink bewegen, um die betroffenen Aggregate anzuzeigen, und dann auf den Aggregatnamen klicken, um Details des Aggregats anzuzeigen. Sie können auch auf die Gesamtanzahl klicken, um die Liste der betroffenen Aggregate in der Ansicht „Integrität: Alle Aggregate“ anzuzeigen.

In den folgenden Fällen wird in dieser Spalte kein Wert angezeigt:

- Für defekte Festplatten, wenn ein Cluster mit solchen Festplatten zu Unified Manager hinzugefügt wird
- Wenn keine Festplatten ausgefallen sind

Speicherpool

Zeigt den Namen des Speicherpools an, zu dem die SSD gehört. Sie können den Zeiger über den Namen des Speicherpools bewegen, um Details zum Speicherpool anzuzeigen.

Speicherkapazität

Zeigt die zur Nutzung verfügbare Festplattenkapazität an.

Rohkapazität

Zeigt die Kapazität der unformatierten Rohfestplatte vor der Größenanpassung und RAID-Konfiguration an. Standardmäßig ist diese Spalte ausgeblendet.

Typ

Zeigt die Festplattentypen an: beispielsweise ATA, SATA, FCAL oder VMDISK.

Effektiver Typ

Zeigt den von ONTAP zugewiesenen Festplattentyp an.

Bestimmte ONTAP Festplattentypen werden zum Erstellen und Hinzufügen zu Aggregaten sowie zur Ersatzteilverwaltung als gleichwertig angesehen. ONTAP weist jedem Festplattentyp einen effektiven Festplattentyp zu.

Verbrauchte Ersatzblöcke %

Zeigt die in der SSD-Festplatte verbrauchten Ersatzblöcke in Prozent an. Diese Spalte ist für andere Datenträger als SSD-Datenträger leer.

Nennlebensdauer %

Zeigt eine Schätzung der verwendeten SSD-Lebensdauer in Prozent an, basierend auf der tatsächlichen SSD-Nutzung und der Vorhersage des Herstellers zur SSD-Lebensdauer. Ein Wert größer als 99 zeigt an, dass die geschätzte Lebensdauer aufgebraucht ist, weist aber möglicherweise nicht auf einen SSD-Fehler hin. Wenn der Wert unbekannt ist, wird die Festplatte weggelassen.

Firmware

Zeigt die Firmware-Version der Festplatte an.

Drehzahl

Zeigt die Umdrehungen pro Minute (RPM) der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

Modell

Zeigt die Modellnummer der Festplatte an. Standardmäßig ist diese Spalte ausgeblendet.

Verkäufer

Zeigt den Namen des Festplattenherstellers an. Standardmäßig ist diese Spalte ausgeblendet.

Regal-ID

Zeigt die ID des Shelfs an, in dem sich die Festplatte befindet.

Einschub

Zeigt die ID des Schachts an, in dem sich die Festplatte befindet.

Bereich „Zugehörige Anmerkungen“

Ermöglicht Ihnen, die mit dem ausgewählten Cluster verknüpften Anmerkungsdetails anzuzeigen. Zu den Details gehören der Annotation-Name und die Annotation-Werte, die auf den Cluster angewendet werden. Sie können manuelle Anmerkungen auch aus dem Bereich „Verwandte Anmerkungen“ entfernen.

Bereich „Verwandte Geräte“

Ermöglicht Ihnen, Gerätedetails anzuzeigen, die mit dem ausgewählten Cluster verknüpft sind.

Die Details umfassen Eigenschaften des mit dem Cluster verbundenen Geräts, wie Gerätetyp, Größe, Anzahl und Integritätsstatus. Sie können auf den Zähllink klicken, um weitere Analysen zu diesem bestimmten Gerät durchzuführen.

Sie können den Bereich „MetroCluster -Partner“ verwenden, um die Anzahl und auch Details zum Remote MetroCluster -Partner sowie den zugehörigen Clusterkomponenten wie Knoten, Aggregaten und SVMs abzurufen. 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 ihnen navigieren, die mit dem Cluster in Zusammenhang stehen:

MetroCluster Partner

Zeigt den Integritätsstatus des MetroCluster Partners an. Über den Zähllink können Sie weiter navigieren und Informationen zum Zustand und zur Kapazität der Clusterkomponenten erhalten.

Nodes

Zeigt die Anzahl, Kapazität und den Integritätsstatus der Knoten an, die zum ausgewählten Cluster gehören. Die Kapazität gibt die gesamte nutzbare Kapazität im Verhältnis zur verfügbaren Kapazität an.

Virtuelle Speichermaschinen

Zeigt die Anzahl der SVMs an, die zum ausgewählten Cluster gehören.

Aggregate

Zeigt die Anzahl, Kapazität und den Integritätsstatus der Aggregate an, die zum ausgewählten Cluster gehören.

Bereich „Verwandte Gruppen“

Ermöglicht Ihnen, die Liste der Gruppen anzuzeigen, die den ausgewählten Cluster enthalten.

Bereich „Zugehörige Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnungen für den ausgewählten Cluster anzeigen. Sie können auch 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 „Bände“" "Anzeigen der Clusterliste und Details"

Seite mit Aggregat-/Gesundheitsdetails

Auf der Seite „Aggregat-/Integritätsdetails“ können Sie ausführliche Informationen zum ausgewählten Aggregat anzeigen, beispielsweise Kapazität, Datenträgerinformationen, Konfigurationsdetails und generierte Ereignisse. Sie können auch Informationen zu den zugehörigen Objekten und zugehörigen Warnungen für dieses Aggregat anzeigen.

Befehlsschaltflächen

Beim Überwachen eines FabricPool-fähigen Aggregats sind die zugesagten und überzugesagten Werte auf dieser Seite nur für die lokale Kapazität bzw. die Kapazität der Leistungsebene relevant. Die Menge des in der Cloud-Ebene verfügbaren Speicherplatzes spiegelt sich nicht in den überbelegten Werten wider. Ebenso sind die aggregierten Schwellenwerte nur für die lokale Leistungsebene relevant.

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben für das ausgewählte Aggregat ausführen:

- **Zur Leistungsansicht wechseln**

  Ermöglicht Ihnen die Navigation zur Seite mit den Gesamt-/Leistungsdetails.

- **Aktionen**
  - Benachrichtigung hinzufügen

    Ermöglicht Ihnen, dem ausgewählten Aggregat eine Warnung hinzuzufügen.

  - Schwellenwerte bearbeiten

    Ermöglicht Ihnen, die Schwellenwerteinstellungen für das ausgewählte Aggregat zu ändern.

- **Aggregate anzeigen**

  Ermöglicht Ihnen die Navigation zur Ansicht „Integrität: Alle Aggregate“.

Registerkarte „Kapazität“

Auf der Registerkarte „Kapazität“ werden ausführliche Informationen zum ausgewählten Aggregat angezeigt, beispielsweise dessen Kapazität, Schwellenwerte und tägliche Wachstumsrate.

Standardmäßig werden für Root-Aggregate keine Kapazitätsereignisse generiert. Außerdem sind die von Unified Manager verwendeten Schwellenwerte nicht auf Knotenstammaggregate anwendbar. 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 Knotenstammaggregat angewendet.

- **Kapazität**

  Zeigt das Datenkapazitätsdiagramm und das Snapshot-Kopiendiagramm an, die Kapazitätsdetails zum Aggregat anzeigen:

  - Verwendeter logischer Speicherplatz

    Die tatsächliche Größe der auf dem Aggregat gespeicherten Daten ohne Berücksichtigung der Einsparungen durch den Einsatz von ONTAP Speichereffizienztechnologien.

  - Gebraucht

    Die von den Daten insgesamt genutzte physische Kapazität.

  - Überlastet

    Wenn der Speicherplatz im Aggregat überbelegt ist, wird im Diagramm eine Markierung mit dem überbelegten Betrag angezeigt.

  - Warnung

    Zeigt eine gepunktete Linie an der Stelle an, an der der Warnschwellenwert festgelegt ist. Dies bedeutet, dass der Speicherplatz im Aggregat fast voll ist. Wenn dieser Schwellenwert überschritten wird, wird das Ereignis „Speicherplatz fast voll“ generiert.

  - Fehler

    Zeigt eine durchgezogene Linie an der Stelle an, an der der Fehlerschwellenwert festgelegt ist. Dies bedeutet, dass der Speicherplatz im Aggregat voll ist. Wenn dieser Schwellenwert überschritten wird, wird das Ereignis „Speicherplatz voll“ generiert.

  - Diagramm „Snapshot-Kopien“

    Dieses Diagramm wird nur angezeigt, wenn die verwendete Snapshot-Kapazität oder die Snapshot-Reserve nicht Null ist.

  Beide Diagramme zeigen die Kapazität an, um die die Snapshot-Kapazität die Snapshot-Reserve übersteigt, wenn die verwendete Snapshot-Kapazität die Snapshot-Reserve übersteigt.

- **Cloud-Ebene**

Zeigt den von Daten in der Cloud-Ebene für FabricPool-fähige Aggregate verwendeten Speicherplatz an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein.

Wenn die Cloud-Ebene auf einen anderen Cloud-Anbieter gespiegelt wird (die „Spiegelebene“), werden hier beide Cloud-Ebenen angezeigt.

- **Details**

  Zeigt detaillierte Informationen zur Kapazität an.

  - Gesamtkapazität

    Zeigt die Gesamtkapazität im Aggregat an.

  - Datenkapazität

    Zeigt die vom Aggregat verwendete Speicherplatzmenge (genutzte Kapazität) und die Menge des im Aggregat verfügbaren Speicherplatzes (freie Kapazität) an.

  - Schnappschuss-Reserve

    Zeigt die verwendete und freie Snapshot-Kapazität des Aggregats an.

  - Überbelegte Kapazität

    Zeigt die gesamte Überbelegung an. Durch die Überbelegung von Aggregaten können Sie mehr Speicher bereitstellen, als tatsächlich von einem bestimmten Aggregat verfügbar ist, solange nicht der gesamte Speicher derzeit verwendet wird. Wenn Thin Provisioning verwendet wird, kann die Gesamtgröße der Volumes im Aggregat die Gesamtkapazität des Aggregats überschreiten.

    Wenn Sie Ihr Aggregat überlastet haben, müssen Sie den verfügbaren Speicherplatz sorgfältig überwachen und bei Bedarf Speicher hinzufügen, um Schreibfehler aufgrund von Speicherplatzmangel zu vermeiden.

  - Cloud-Ebene

    Zeigt den von Daten in der Cloud-Ebene für FabricPool-fähige Aggregate verwendeten Speicherplatz an. Ein FabricPool kann entweder lizenziert oder nicht lizenziert sein. Wenn die Cloud-Ebene auf einen anderen Cloud-Anbieter (die Spiegelebene) gespiegelt wird, werden hier beide Cloud-Ebenen angezeigt.

  - Gesamter Cache-Speicherplatz

    Zeigt den Gesamtspeicherplatz der Solid-State-Laufwerke (SSDs) oder Zuordnungseinheiten an, die einem Flash Pool-Aggregat hinzugefügt werden. Wenn Sie Flash Pool für ein Aggregat aktiviert, aber keine SSDs hinzugefügt haben, wird der Cache-Speicherplatz als 0 KB angezeigt.

    Dieses Feld ist ausgeblendet, wenn Flash Pool für ein Aggregat deaktiviert ist.

  - Aggregierte Schwellenwerte

    Zeigt die folgenden Schwellenwerte für die Gesamtkapazität an:

    - Fast volle Schwelle

Gibt den Prozentsatz an, bei dem ein Aggregat fast voll ist.

- Voller Schwellenwert

  Gibt den Prozentsatz an, bei dem ein Aggregat voll ist.

- Fast überbelegter Schwellenwert

  Gibt den Prozentsatz an, bei dem ein Aggregat nahezu überlastet ist.

- Überbelegter Schwellenwert

  Gibt den Prozentsatz an, bei dem ein Aggregat überbelegt ist.

◦ Weitere Details: Tägliche Wachstumsrate

Zeigt den im Aggregat verwendeten Speicherplatz an, wenn die Änderungsrate zwischen den letzten beiden Stichproben 24 Stunden lang anhält.

Wenn ein Aggregat beispielsweise um 14:00 Uhr 10 GB und um 18:00 Uhr 12 GB Speicherplatz verwendet, beträgt die tägliche Wachstumsrate (GB) für dieses Aggregat 2 GB.

◦ Volumen verschieben

Zeigt die Anzahl der Volume-Verschiebungsvorgänge an, die derzeit ausgeführt werden:

- Ausgehende Volumen

  Zeigt die Anzahl und Kapazität der Volumes an, die aus dem Aggregat verschoben werden.

Sie können auf den Link klicken, um weitere Details anzuzeigen, z. B. den Volumenamen, das Aggregat, in das das Volume verschoben wird, den Status des Volumeverschiebungsvorgangs und die voraussichtliche Endzeit.

- Volumen in

  Zeigt die Anzahl und die verbleibende Kapazität der Volumes an, die in das Aggregat verschoben werden.

Sie können auf den Link klicken, um weitere Details anzuzeigen, z. B. den Volumenamen, das Aggregat, aus dem das Volume verschoben wird, den Status des Volumeverschiebungsvorgangs und die voraussichtliche Endzeit.

◦ Geschätzte genutzte Kapazität nach der Volumeverschiebung

Zeigt die geschätzte Menge des verwendeten Speicherplatzes (als Prozentsatz und in KB, MB, GB usw.) insgesamt an, nachdem die Volume-Verschiebungsvorgänge abgeschlossen sind.

- **Kapazitätsübersicht - Volumen**

Zeigt Diagramme an, die Informationen zur Kapazität der im Aggregat enthaltenen Volumes liefern. Es wird die vom Volume verwendete Speicherplatzmenge (genutzte Kapazität) und die Menge des verfügbaren Speicherplatzes (freie Kapazität) im Volume angezeigt. Wenn das Ereignis „Gefährdeter Speicherplatz für Thin-Provisioned-Volume“ für Thin-Provisioned-Volumes generiert wird, wird die vom Volume verwendete Speicherplatzmenge (verwendete Kapazität) und die Speicherplatzmenge angezeigt, die im Volume verfügbar ist, aber aufgrund von Problemen mit der Gesamtkapazität nicht verwendet werden kann

(unverwendbare Kapazität).

Sie können das Diagramm, das Sie anzeigen möchten, aus den Dropdown-Listen auswählen. Sie können die im Diagramm angezeigten Daten sortieren, um Details wie die verwendete Größe, die bereitgestellte Größe, die verfügbare Kapazität, die schnellste tägliche Wachstumsrate und die langsamste Wachstumsrate anzuzeigen. Sie können die Daten basierend auf den Storage Virtual Machines (SVMs) filtern, die die Volumes im Aggregat enthalten. Sie können auch Details zu Thin Provisioning-Volumes anzeigen. Sie können die Details bestimmter Punkte im Diagramm anzeigen, indem Sie den Cursor über den gewünschten Bereich bewegen. Standardmäßig zeigt das Diagramm die 30 wichtigsten gefilterten Volumina im Aggregat an.

Registerkarte „Datenträgerinformationen“

Zeigt detaillierte Informationen zu den Festplatten im ausgewählten Aggregat an, einschließlich RAID-Typ und -Größe sowie den Typ der im Aggregat verwendeten Festplatten. Die Registerkarte zeigt auch grafisch die RAID-Gruppen und die verwendeten Festplattentypen (z. B. SAS, ATA, FCAL, SSD oder VMDISK) an. Sie können weitere Informationen anzeigen, beispielsweise den Schacht, das Regal und die Rotationsgeschwindigkeit der Festplatte, indem Sie den Cursor über die Paritätsfestplatten und Datenfestplatten bewegen.

- **Daten**

  Zeigt grafisch Details zu dedizierten Datenträgern, gemeinsam genutzten Datenträgern oder beidem an. Wenn die Datenträger gemeinsam genutzte Datenträger enthalten, werden grafische Details der gemeinsam genutzten Datenträger angezeigt. Wenn die Datenträger dedizierte und gemeinsam genutzte Datenträger enthalten, werden grafische Details sowohl der dedizierten 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 maximale Anzahl der in der RAID-Gruppe zulässigen Festplatten an.

    - Gruppen

      Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

  - **Verwendete Datenträger**
    - Effektiver Typ

      Zeigt die Typen der Datenträger (z. B. ATA, SATA, FCAL, SSD oder VMDISK) im Aggregat an.

    - Datenträger

      Zeigt die Anzahl und Kapazität der Datenträger an, die einem Aggregat zugewiesen sind. Datenträgerdetails werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Datenträger enthält.

        - Paritätsfestplatten

          Zeigt die Anzahl und Kapazität der Paritätsfestplatten an, die einem Aggregat zugewiesen sind. Paritätsdatenträgerdetails werden nicht angezeigt, wenn das Aggregat nur gemeinsam genutzte Datenträger enthält.

        - Gemeinsam genutzte Datenträger

          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 gemeinsam genutzte Datenträger enthält.

    - **Ersatzdisketten**

      Zeigt den effektiven Datenträgertyp, die Anzahl und die Kapazität der Ersatzdatenträger an, die für den Knoten im ausgewählten Aggregat verfügbar sind.

      Wenn ein Aggregat per Failover auf den Partnerknoten umgeschaltet wird, zeigt Unified Manager nicht alle Ersatzfestplatten an, die mit dem Aggregat kompatibel sind.

- **SSD-Cache**

  Bietet Details zu dedizierten Cache-SSD-Festplatten und gemeinsam genutzten Cache-SSD-Festplatten.

  Die folgenden Details für die dedizierten Cache-SSD-Festplatten werden angezeigt:

    - **RAID-Details**
        - Typ

          Zeigt den RAID-Typ an (RAID0, RAID4, RAID-DP oder RAID-TEC).

        - Gruppengröße

          Zeigt die maximale Anzahl der in der RAID-Gruppe zulässigen Festplatten an.

        - Gruppen

          Zeigt die Anzahl der RAID-Gruppen im Aggregat an.

    - **Verwendete Datenträger**
        - Effektiver Typ

          Gibt an, dass die für den Cache im Aggregat verwendeten Datenträger vom Typ SSD sind.

        - Datenträger

          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.

◦ **Ersatzdisketten**

Zeigt den effektiven Datenträgertyp, die Anzahl und die Kapazität der Ersatzdatenträger an, die für den Knoten im ausgewählten Aggregat für den Cache verfügbar sind.

Wenn ein Aggregat per Failover auf den Partnerknoten umgeschaltet wird, zeigt Unified Manager nicht alle Ersatzfestplatten an, die mit dem Aggregat kompatibel sind.

Bietet die folgenden Details zum gemeinsam genutzten Cache:

◦ **Speicherpool**

Zeigt den Namen des Speicherpools an. Sie können den Zeiger über den Namen des Speicherpools bewegen, um die folgenden Details anzuzeigen:

- Status

  Zeigt den Status des Speicherpools an, der fehlerfrei oder fehlerhaft sein kann.

- Gesamtzuweisungen

  Zeigt die gesamten Zuordnungseinheiten und die Größe im Speicherpool an.

- Größe der Zuordnungseinheit

  Zeigt die Mindestmenge an Speicherplatz im Speicherpool an, die einem Aggregat zugewiesen werden kann.

- Festplatten

  Zeigt die Anzahl der zum Erstellen des Speicherpools verwendeten Datenträger an. Wenn die Datenträgeranzahl in der Spalte „Speicherpool“ und die Anzahl der Datenträger, die auf der Registerkarte „Datenträgerinformationen“ für diesen Speicherpool angezeigt werden, nicht übereinstimmen, weist dies darauf hin, dass ein oder mehrere Datenträger defekt sind und der Speicherpool nicht fehlerfrei ist.

- Verwendete Zuordnung

  Zeigt die Anzahl und Größe der von den Aggregaten verwendeten Zuordnungseinheiten an. Sie können auf den Aggregatnamen klicken, um die Aggregatdetails anzuzeigen.

- Verfügbare Zuteilung

  Zeigt die Anzahl und Größe der für die Knoten verfügbaren Zuordnungseinheiten an. Sie können auf den Knotennamen klicken, um die Gesamtdetails anzuzeigen.

◦ **Zugewiesener Cache**

Zeigt die Größe der vom Aggregat verwendeten Zuordnungseinheiten an.

◦ **Zuordnungseinheiten**

Zeigt die Anzahl der vom Aggregat verwendeten Zuordnungseinheiten an.

◦ **Festplatten**

Zeigt die Anzahl der im Speicherpool enthaltenen Datenträger an.

- **Details**
  - Speicherpool

    Zeigt die Anzahl der Speicherpools an.

  - Gesamtgröße

    Zeigt die Gesamtgröße der Speicherpools an.

- **Cloud-Ebene**

  Zeigt den Namen der Cloud-Ebene an, wenn Sie ein FabricPool-fähiges Aggregat konfiguriert haben, und zeigt den insgesamt verwendeten Speicherplatz an. Wenn die Cloud-Ebene auf einen anderen Cloud-Anbieter (die Spiegelebene) gespiegelt wird, werden hier die Details für beide Cloud-Ebenen angezeigt.

Registerkarte „Konfiguration“

Auf der Registerkarte „Konfiguration“ werden Details zum ausgewählten Aggregat angezeigt, z. B. Clusterknoten, Blocktyp, RAID-Typ, RAID-Größe und 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-Ebene**

  Wenn es sich um ein FabricPool-fähiges Aggregat handelt, werden die Details für die Cloud-Ebene angezeigt. Einige Felder sind je nach Speicheranbieter unterschiedlich. Wenn die Cloud-Ebene auf einen anderen Cloud-Anbieter gespiegelt wird (die „Spiegelebene“), werden hier beide Cloud-Ebenen angezeigt.

  - Anbieter

Zeigt den Namen des Speicheranbieters an, z. B. 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 der Cloud-Ebene an.

- Hafen

  Der Port, der für die Kommunikation mit dem Cloud-Anbieter verwendet wird.

- 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.

Geschichtsbereich

Im Bereich „Verlauf“ werden Diagramme angezeigt, die Informationen zur Kapazität des ausgewählten Aggregats liefern. Darüber hinaus können Sie auf die Schaltfläche **Exportieren** klicken, um einen Bericht im CSV-Format für das Diagramm zu erstellen, das Sie gerade anzeigen.

Sie können einen Diagrammtyp aus der Dropdown-Liste oben im Verlaufsbereich auswählen. Sie können auch Details für einen bestimmten Zeitraum anzeigen, indem Sie entweder 1 Woche, 1 Monat oder 1 Jahr auswählen. Mithilfe von Verlaufsdiagrammen können Sie Trends erkennen: Wenn beispielsweise die Gesamtnutzung ständig den Schwellenwert „Fast voll“ überschreitet, können Sie entsprechende Maßnahmen ergreifen.

Verlaufsdiagramme zeigen die folgenden Informationen an:

- **Genutzte Gesamtkapazität (%)**

  Zeigt die genutzte Kapazität im Aggregat und den Trend zur Nutzung der Aggregatkapazität basierend auf dem Nutzungsverlauf 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 bewegen. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Kapazitätsnutzung“ klicken, wird die Diagrammlinie „Kapazitätsnutzung“ ausgeblendet.

- **Genutzte Gesamtkapazität im Vergleich zur Gesamtkapazität**

  Zeigt den Trend der Nutzung der Gesamtkapazität basierend auf dem Nutzungsverlauf sowie die genutzte Kapazität und die Gesamtkapazität als Liniendiagramme in Byte, Kilobyte, Megabyte usw. auf der

vertikalen Achse (y) 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 bewegen. Sie können ein Liniendiagramm ausblenden oder anzeigen, indem Sie auf die entsprechende Legende klicken. Wenn Sie beispielsweise auf die Legende „Trend der genutzten Kapazität“ klicken, wird die Diagrammlinie „Trend der genutzten Kapazität“ ausgeblendet.

- **Genutzte Gesamtkapazität (%) vs. zugesagte Kapazität (%)**

  Zeigt den Trend der Nutzung der Gesamtkapazität basierend auf dem Nutzungsverlauf sowie den zugesicherten 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 bewegen. 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

In der Ereignisliste werden Details zu neuen und bestätigten Ereignissen angezeigt:

- **Schwere**

  Zeigt den Schweregrad des Ereignisses an.

- **Ereignis**

  Zeigt den Ereignisnamen an.

- **Ausgelöste Zeit**

  Zeigt die Zeit an, die seit der Generierung des Ereignisses vergangen ist. Wenn die verstrichene Zeit mehr als eine Woche beträgt, wird der Zeitstempel für die Generierung des Ereignisses angezeigt.

Bereich „Verwandte Geräte“

Im Bereich „Verwandte Geräte“ können Sie die Clusterknoten, Volumes und Datenträger anzeigen, die mit dem Aggregat in Zusammenhang stehen:

- **Knoten**

  Zeigt die Kapazität und den Integritätsstatus des Knotens an, der das Aggregat enthält. Die Kapazität gibt die gesamte nutzbare Kapazität im Verhältnis zur verfügbaren Kapazität an.

- **Aggregate im Knoten**

  Zeigt die Anzahl und Kapazität aller Aggregate im Clusterknoten an, der das ausgewählte Aggregat enthält. Der Integritätsstatus der Aggregate wird ebenfalls angezeigt, basierend auf dem höchsten Schweregrad. Wenn ein Clusterknoten beispielsweise zehn Aggregate enthält, von denen fünf den Status „Warnung“ und die restlichen fünf den Status „Kritisch“ anzeigen, wird der Status „Kritisch“ angezeigt.

- **Bände**

  Zeigt die Anzahl und Kapazität der FlexVol -Volumes und FlexGroup -Volumes insgesamt an; die Zahl umfasst keine FlexGroup -Bestandteile. Außerdem wird der Integritätsstatus der Volumes basierend auf

dem höchsten Schweregrad angezeigt.

- **Ressourcenpool**

  Zeigt die mit dem Aggregat verbundenen Ressourcenpools an.

- **Festplatten**

  Zeigt die Anzahl der Festplatten im ausgewählten Aggregat an.

Bereich „Zugehörige Warnungen“

Im Bereich „Verwandte Warnungen“ können Sie die Liste der Warnungen anzeigen, die für das ausgewählte Aggregat erstellt wurden. Sie können auch eine Warnung hinzufügen, indem Sie auf den Link „Warnung hinzufügen“ klicken, oder eine vorhandene Warnung bearbeiten, indem Sie auf den Warnungsnamen klicken.

Verwandte Informationen

"Anzeigen von Speicherpooldetails"

Schützen und Wiederherstellen von Daten

Erstellen, Überwachen und Beheben von Problemen mit Schutzbeziehungen

Mit Unified Manager können Sie Schutzbeziehungen erstellen, den Spiegelschutz und den Backup-Vault-Schutz von auf verwalteten Clustern gespeicherten Daten überwachen und Fehler beheben sowie Daten wiederherstellen, wenn diese überschrieben wurden oder verloren gegangen sind.

Arten des SnapMirror Schutzes

Abhängig von der Bereitstellung Ihrer Datenspeichertopologie können Sie mit Unified Manager mehrere Arten von SnapMirror Schutzbeziehungen konfigurieren. Alle Varianten des SnapMirror Schutzes bieten Failover-Disaster-Recovery-Schutz, unterscheiden sich jedoch hinsichtlich Leistung, Versionsflexibilität und Schutz mehrerer Sicherungskopien.

Traditionelle SnapMirror Asynchrone Schutzbeziehungen

Der traditionelle asynchrone SnapMirror Schutz bietet einen Blockreplikationsspiegelschutz zwischen Quell- und Zielvolumes.

In herkömmlichen SnapMirror -Beziehungen werden Spiegelvorgänge schneller ausgeführt als in alternativen SnapMirror -Beziehungen, da der Spiegelvorgang auf Blockreplikation basiert. Der herkömmliche SnapMirror Schutz erfordert jedoch, dass das Zielvolume unter derselben oder einer späteren Nebenversion der ONTAP -Software wie das Quellvolume innerhalb derselben Hauptversion ausgeführt wird (z. B. Version 8.x bis 8.x oder 9.x bis 9.x). Die Replikation von einer 9.1-Quelle zu einem 9.0-Ziel wird nicht unterstützt, da auf dem Ziel eine frühere Hauptversion ausgeführt wird.

SnapMirror Asynchroner Schutz mit versionsflexibler Replikation

Der asynchrone SnapMirror Schutz mit versionsflexibler Replikation bietet logischen Replikationsspiegelschutz zwischen Quell- und Zielvolumes, selbst wenn diese Volumes unter unterschiedlichen Versionen der ONTAP 8.3-Software 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 Spiegelvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror -Beziehungen.

Aufgrund der langsameren Ausführung ist SnapMirror mit versionsflexiblem Replikationsschutz unter folgenden Umständen nicht für die Implementierung geeignet:

- Das Quellobjekt enthält mehr als 10 Millionen zu schützende Dateien.
- Das Recovery Point Objective für die geschützten Daten beträgt zwei Stunden oder weniger. (Das heißt, das Ziel muss immer gespiegelte, wiederherstellbare Daten enthalten, die nicht älter als die Daten an der Quelle sind.)

In beiden aufgeführten Fällen ist die schnellere, auf Blockreplikation basierende Ausführung des standardmäßigen SnapMirror Schutzes erforderlich.

SnapMirror Asynchroner Schutz mit versionsflexibler Replikations- und Backup-Option

Der asynchrone Schutz von SnapMirror mit versionsflexibler Replikations- und Sicherungsoption bietet Spiegelschutz zwischen Quell- und Zielvolumes und die Möglichkeit, mehrere Kopien der gespiegelten Daten am Ziel zu speichern.

Der Speicheradministrator kann angeben, welche Snapshot-Kopien von der Quelle zum Ziel gespiegelt werden, und kann auch angeben, wie lange diese Kopien am Ziel aufbewahrt werden, selbst wenn sie an der Quelle gelöscht werden.

In SnapMirror -Beziehungen mit versionsflexibler Replikations- und Sicherungsoption werden Spiegelvorgänge nicht so schnell ausgeführt wie in herkömmlichen SnapMirror -Beziehungen.

SnapMirror Unified Replication (Spiegel und Tresor)

Mit der einheitlichen Replikation von SnapMirror können Sie die Notfallwiederherstellung und Archivierung auf demselben Zielvolume konfigurieren. Wie bei SnapMirror führt der einheitliche Datenschutz beim ersten Aufruf eine Basisübertragung durch. Bei einer Basisübertragung unter der standardmäßigen einheitlichen Datenschutzrichtlinie „MirrorAndVault“ wird eine Snapshot-Kopie des Quellvolumes erstellt und anschließend diese Kopie und die darin referenzierten Datenblöcke auf das Zielvolume übertragen. Wie SnapVault umfasst der einheitliche Datenschutz keine älteren Snapshot-Kopien in der Basislinie.

SnapMirror Synchroner Schutz mit strikter Synchronisierung

Der SnapMirror Synchronous-Schutz mit „strikter“ Synchronisierung stellt sicher, dass die primären und sekundären Volumes immer eine echte Kopie voneinander sind. Wenn beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replikationsfehler auftritt, wird die Client-E/A zum primären Volume unterbrochen.

SnapMirror Synchroner Schutz mit regelmäßiger Synchronisierung

Der synchrone SnapMirror -Schutz mit „normaler“ Synchronisierung erfordert nicht, dass das primäre und das sekundäre Volume immer eine echte Kopie voneinander sind. Dadurch wird die Verfügbarkeit des primären Volumes sichergestellt. Wenn beim Versuch, Daten auf das sekundäre Volume zu schreiben, ein Replikationsfehler auftritt, sind das primäre und das sekundäre Volume nicht mehr synchron und die Client-E/A wird auf dem primären Volume fortgesetzt.

Die Schaltflächen „Wiederherstellen“ und „Beziehungsvorgang“ sind nicht verfügbar, wenn synchrone Schutzbeziehungen über die Ansicht „Integrität: Alle Volumes“ oder die Seite „Volume-/Integritätsdetails“ überwacht werden.

SnapMirror aktive Synchronisierung

Die SnapMirror Active Sync-Funktion ist mit ONTAP 9.8 und höher verfügbar und Sie können sie zum Schutz von Anwendungen mit LUNs verwenden, sodass Anwendungen transparent ausfallen und die Geschäftskontinuität im Katastrophenfall gewährleistet ist.

Es ermöglicht Ihnen, die synchronen SnapMirror -Beziehungen für Konsistenzgruppen (CGs) zu erkennen und zu überwachen, die auf Clustern und virtuellen Speichermaschinen von 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 Anwendungen mit iSCSI- oder FCP-LUNs.

Wenn Sie die durch die SnapMirror Active Sync-Beziehung geschützten Volumes und LUNs anzeigen, erhalten

Sie eine einheitliche Ansicht für Schutzbeziehungen, Konsistenzgruppen im Volume-Inventar, die Anzeige der Schutztopologie für Konsistenzgruppenbeziehungen und die Anzeige historischer Daten für Konsistenzgruppenbeziehungen bis zu einem Jahr. Sie können den Bericht auch herunterladen. Sie können auch die Zusammenfassung der Konsistenzgruppenbeziehungen anzeigen, Support für Konsistenzgruppenbeziehungen suchen und Informationen zu Volumes erhalten, die durch die Konsistenzgruppe geschützt sind.

Auf der Seite „Beziehungen“ können Sie auch den Schutz der Quell- und Zielspeicherobjekte und ihrer Beziehungen, die durch die Konsistenzgruppe geschützt sind, sortieren, filtern und erweitern.

Weitere Informationen zu SnapMirror Active Sync finden Sie unter"ONTAP 9-Dokumentation für Snapmirror Active Sync (früher SM-BC)" .

Einrichten von Schutzbeziehungen im Unified Manager

Um mit Unified Manager und OnCommand Workflow Automation SnapMirror und SnapVault -Beziehungen zum Schutz Ihrer Daten einzurichten, müssen Sie mehrere Schritte ausführen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Peer-Beziehungen zwischen zwei Clustern oder zwei virtuellen Speichermaschinen (SVMs) eingerichtet haben.
- OnCommand Workflow Automation muss in Unified Manager integriert werden:
  - "Einrichten der OnCommand Workflow Automation".
  - "Überprüfen des Unified Manager-Datenquellen-Cachings in der Workflow-Automatisierung".

Schritte

1. Führen Sie je nach Art der Schutzbeziehung, die Sie erstellen möchten, einen der folgenden Schritte aus:
   - "Erstellen einer SnapMirror Schutzbeziehung".
   - "Erstellen einer SnapVault -Schutzbeziehung".
2. Wenn Sie eine Richtlinie für die Beziehung erstellen möchten, führen Sie je nach dem von Ihnen erstellten Beziehungstyp einen der folgenden Schritte aus:
   - "Erstellen einer SnapVault -Richtlinie".
   - "Erstellen einer SnapMirror -Richtlinie".
3. "Erstellen Sie einen SnapMirror oder SnapVault -Zeitplan".

Konfigurieren Sie eine Verbindung zwischen Workflow Automation und Unified Manager

Sie können eine sichere Verbindung zwischen OnCommand Workflow Automation (WFA) und Unified Manager konfigurieren. Durch die Verbindung mit Workflow Automation können Sie Schutzfunktionen wie SnapMirror und SnapVault -Konfigurationsworkflows sowie Befehle zum Verwalten von SnapMirror Beziehungen verwenden.

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. Sie müssen dieses Paket also nicht wie bisher aus dem NetAppStorage Automation Store herunterladen und separat auf Ihrem WFA-Server installieren. "WFA-Paket zur Verwaltung von ONTAP"

- Sie müssen den Namen des Datenbankbenutzers haben, den Sie in Unified Manager erstellt haben, um WFA- und Unified Manager-Verbindungen zu unterstützen.

  Diesem Datenbankbenutzer muss die Benutzerrolle „Integrationsschema“ zugewiesen worden sein.

- Ihnen muss in der Workflow-Automatisierung entweder die Administratorrolle oder die Architektrolle zugewiesen sein.
- Sie müssen über die Hostadresse, die Portnummer 443, den Benutzernamen und das Kennwort für die Einrichtung der Workflow-Automatisierung verfügen.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Workflow-Automatisierung**.
2. Wählen Sie im Bereich **Datenbankbenutzer** der **Seite „Workflow-Automatisierung“** den Namen aus und geben Sie das Kennwort für den Datenbankbenutzer ein, den Sie zur Unterstützung von Unified Manager- und Workflow-Automatisierungsverbindungen erstellt haben.
3. Geben Sie im Bereich **Anmeldeinformationen für die Workflow-Automatisierung** der Seite den Hostnamen oder die IP-Adresse (IPv4 oder IPv6) sowie den Benutzernamen und das Kennwort für die Einrichtung der Workflow-Automatisierung ein.

   Sie müssen den Unified Manager-Serverport (Port 443) verwenden.

4. Klicken Sie auf **Speichern**.
5. Wenn Sie ein selbstsigniertes Zertifikat verwenden, klicken Sie auf **Ja**, um das Sicherheitszertifikat zu autorisieren.

   Die Seite „Workflow-Automatisierung“ wird angezeigt.

6. Klicken Sie auf **Ja**, um die Web-Benutzeroberfläche neu zu laden und die Workflow-Automatisierungsfunktionen hinzuzufügen.

Verwandte Informationen

"NetApp -Dokumentation: OnCommand Workflow Automation (aktuelle Versionen)"

Überprüfen Sie das Caching der Unified Manager-Datenquelle in der Workflow-Automatisierung

Sie können feststellen, ob das Datenquellen-Caching von Unified Manager ordnungsgemäß funktioniert, indem Sie überprüfen, ob die Datenquellenerfassung in der Workflow-Automatisierung erfolgreich war. Sie können dies tun, wenn Sie die Workflow-Automatisierung mit Unified Manager integrieren, um sicherzustellen, dass die Workflow-Automatisierungsfunktion nach der Integration verfügbar ist.

Bevor Sie beginnen

Um diese Aufgabe ausführen zu können, muss Ihnen in der Workflow-Automatisierung entweder die

Administratorrolle oder die Architektrolle zugewiesen sein.

Schritte

1. Wählen Sie in der Benutzeroberfläche der Workflow-Automatisierung **Ausführung** > **Datenquellen** aus.
2. Klicken Sie mit der rechten Maustaste auf den Namen der Unified Manager-Datenquelle und wählen Sie dann **Jetzt abrufen**.
3. Überprüfen Sie, ob die Erfassung fehlerfrei verläuft.

   Damit die Workflow-Automatisierungsintegration mit Unified Manager erfolgreich ist, müssen Erfassungsfehler behoben werden.

Was passiert, wenn OnCommand Workflow Automation neu installiert oder aktualisiert wird?

Bevor Sie OnCommand Workflow Automation neu installieren oder aktualisieren, müssen Sie zunächst die Verbindung zwischen OnCommand Workflow Automation und Unified Manager entfernen und sicherstellen, dass alle derzeit ausgeführten oder geplanten Jobs von OnCommand Workflow Automation gestoppt werden.

Sie müssen Unified Manager auch manuell aus OnCommand Workflow Automation löschen.

Nachdem Sie OnCommand Workflow Automation neu installiert oder aktualisiert haben, müssen Sie die Verbindung mit Unified Manager erneut einrichten.

Entfernen Sie das OnCommand Workflow Automation -Setup aus Unified Manager

Sie können das OnCommand Workflow Automation -Setup aus Unified Manager entfernen, wenn Sie Workflow Automation nicht mehr verwenden möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich im linken Setup-Menü auf **Allgemein** > **Workflow-Automatisierung**.
2. Klicken Sie auf der Seite **Workflow-Automatisierung** auf **Setup entfernen**.

Führen Sie ein Failover und Failback für die Schutzbeziehung durch

Wenn ein Quellvolume in Ihrer Schutzbeziehung aufgrund eines Hardwarefehlers oder einer Katastrophe deaktiviert wird, können Sie die Schutzbeziehungsfunktionen in Unified Manager verwenden, um das Schutzziel lese-/schreibzugänglich zu machen und ein Failover auf dieses Volume durchzuführen, bis die Quelle wieder online ist. Anschließend können Sie ein Failback auf die ursprüngliche Quelle durchführen, wenn diese wieder zur Bereitstellung von Daten verfügbar ist.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die OnCommand Workflow Automation eingerichtet haben, um diesen Vorgang auszuführen.

Schritte

1. "Brechen Sie die SnapMirror Beziehung".

   Sie müssen die Beziehung trennen, bevor Sie das Ziel von einem Datenschutzvolume in ein Lese-/Schreibvolume konvertieren und bevor Sie die Beziehung umkehren können.

2. "Umkehren des Schutzverhältnisses".

   Wenn das ursprüngliche Quellvolume wieder verfügbar ist, können Sie die ursprüngliche Schutzbeziehung durch Wiederherstellen des Quellvolumes wiederherstellen. Bevor Sie die Quelle wiederherstellen können, müssen Sie sie mit den Daten synchronisieren, die in das frühere Ziel geschrieben wurden. Mit dem umgekehrten Resynchronisierungsvorgang 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 Basis-Snapshot-Kopie erstellt.

   Die umgekehrte Beziehung ähnelt einer kaskadierten Beziehung:

3. "Brechen Sie die umgekehrte SnapMirror Beziehung".

   Wenn das ursprüngliche Quellvolume neu synchronisiert ist und wieder Daten bereitstellen kann, verwenden Sie den Unterbrechungsvorgang, um die umgekehrte Beziehung aufzuheben.

4. "Entfernen Sie die Beziehung".

   Wenn die umgekehrte Beziehung nicht mehr benötigt wird, sollten Sie diese Beziehung entfernen, bevor Sie die ursprüngliche Beziehung wiederherstellen.

5. "Resynchronisieren Sie die Beziehung".

   Verwenden Sie den Neusynchronisierungsvorgang, um Daten von der Quelle zum Ziel zu synchronisieren und die ursprüngliche Beziehung wiederherzustellen.

Unterbrechen Sie eine SnapMirror -Beziehung von der Seite mit den Volume-/Integritätsdetails

Sie können eine Schutzbeziehung auf der Seite „Volume-/Integritätsdetails“ unterbrechen und Datenübertragungen zwischen einem Quell- und einem Zielvolume in einer SnapMirror -Beziehung stoppen. Sie können eine Beziehung unterbrechen, wenn Sie Daten migrieren, eine Notfallwiederherstellung durchführen oder Anwendungen testen möchten. Das Zielvolume wird in ein Lese-/Schreibvolume geändert. Sie können eine SnapVault -Beziehung nicht unterbrechen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Schritte

1. Wählen Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** aus der Topologie die SnapMirror -Beziehung aus, die Sie trennen möchten.
2. Klicken Sie mit der rechten Maustaste auf das Ziel und wählen Sie im Menü **Unterbrechen** aus.

   Das Dialogfeld „Beziehung auflösen“ wird angezeigt.

3. Klicken Sie auf **Weiter**, um die Beziehung zu beenden.
4. Überprüfen Sie in der Topologie, ob die Beziehung unterbrochen ist.

Umgekehrte Schutzbeziehungen von der Seite „Volume-/Integritätsdetails“

Wenn das Quellvolume in Ihrer Schutzbeziehung durch einen Notfall deaktiviert wird, können Sie das Zielvolume zum Bereitstellen von Daten verwenden, indem Sie es in einen Lese-/Schreibzugriff konvertieren, während Sie die Quelle reparieren oder ersetzen. Wenn die Quelle wieder zum Empfangen von Daten verfügbar ist, können Sie den umgekehrten Resynchronisierungsvorgang verwenden, um die Beziehung in umgekehrter Richtung herzustellen und die Daten auf der Quelle mit den Daten auf dem Lese-/Schreibziel zu synchronisieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.
- Bei der Beziehung darf es sich nicht um eine SnapVault -Beziehung handeln.
- Es muss bereits ein Schutzverhältnis bestehen.
- Das Schutzverhältnis muss aufgelöst werden.
- Sowohl die Quelle als auch das Ziel müssen online sein.
- Die Quelle darf nicht das Ziel eines anderen Datensicherungsvolumes sein.
- Wenn Sie diese Aufgabe ausführen, werden Daten auf der Quelle gelöscht, die neuer sind als die Daten auf der gemeinsamen Snapshot-Kopie.
- Für die umgekehrte Resynchronisierungsbeziehung werden dieselben Richtlinien und Zeitpläne erstellt wie für die ursprüngliche Schutzbeziehung.

  Wenn keine Richtlinien und Zeitpläne vorhanden sind, werden sie erstellt.

Schritte

1. Suchen Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** in der Topologie die SnapMirror -Beziehung, bei der Sie Quelle und Ziel umkehren möchten, und klicken Sie mit der rechten Maustaste darauf.
2. Wählen Sie im Menü „Reverse Resync“ aus.

   Das Dialogfeld „Umgekehrte Neusynchronisierung“ wird angezeigt.

3. Überprüfen Sie, ob die im Dialogfeld **Reverse Resync** angezeigte Beziehung diejenige ist, für die Sie den umgekehrten Resynchronisierungsvorgang durchführen möchten, und klicken Sie dann auf **Senden**.

   Das Dialogfeld „Reverse Resync“ wird geschlossen und oben auf der Seite mit den Volume-/Integritätsdetails wird ein Job-Link angezeigt.

4. **Optional:** Klicken Sie auf der Detailseite **Volume/Integrität** auf **Jobs anzeigen**, um den Status jedes umgekehrten Resynchronisierungsjobs zu verfolgen.

   Es wird eine gefilterte Liste mit Jobs angezeigt.

5. **Optional:** Klicken Sie in Ihrem Browser auf den Pfeil **Zurück**, um zur Detailseite **Volumen/Gesundheit** zurückzukehren.

   Der umgekehrte Resynchronisierungsvorgang ist abgeschlossen, wenn alle Jobaufgaben erfolgreich abgeschlossen wurden.

Entfernen einer Schutzbeziehung von der Seite „Volume-/Integritätsdetails“

Sie können eine Schutzbeziehung entfernen, um eine bestehende Beziehung zwischen der ausgewählten Quelle und dem ausgewählten 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

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Schritte

1. Wählen Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** aus der Topologie die SnapMirror -Beziehung aus, die Sie entfernen möchten.
2. Klicken Sie mit der rechten Maustaste auf den Namen des Ziels und wählen Sie im Menü **Entfernen**.

   Das Dialogfeld „Beziehung entfernen“ wird angezeigt.

3. Klicken Sie auf **Weiter**, um die Beziehung zu entfernen.

   Die Beziehung wird von der Seite mit den Volumen-/Gesundheitsdetails entfernt.

Synchronisieren Sie Schutzbeziehungen über die Seite „Volume-/Integritätsdetails“ erneut.

Sie können Daten einer SnapMirror oder SnapVault -Beziehung neu synchronisieren, die unterbrochen wurde und bei der das Ziel anschließend zum Lesen/Schreiben freigegeben wurde, sodass die Daten auf der Quelle mit den Daten auf dem Ziel übereinstimmen. Sie können die Synchronisierung auch dann erneut durchführen, wenn eine erforderliche gemeinsame Snapshot-Kopie auf dem Quellvolume gelöscht wird und dadurch SnapMirror oder SnapVault -Updates fehlschlagen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Suchen Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** in der Topologie die Schutzbeziehung, die Sie neu synchronisieren möchten, und klicken Sie mit der rechten Maustaste darauf.
2. Wählen Sie im Menü **Neu synchronisieren**.

   Alternativ können Sie im Menü **Aktionen** die Option **Beziehung** > **Neu synchronisieren** auswählen, um die Beziehung, deren Details Sie gerade anzeigen, neu zu synchronisieren.

Das Dialogfeld „Neu synchronisieren“ wird angezeigt.

3. Wählen Sie auf der Registerkarte **Resynchronisierungsoptionen** eine Übertragungspriorität und die maximale Übertragungsrate aus.
4. Klicken Sie auf **Quell-Snapshot-Kopien** und dann in der Spalte **Snapshot-Kopie** auf **Standard**.

   Das Dialogfeld „Quell-Snapshot-Kopie auswählen“ wird angezeigt.

5. Wenn Sie eine vorhandene Snapshot-Kopie angeben möchten, anstatt die Standard-Snapshot-Kopie zu übertragen, klicken Sie auf **Vorhandene Snapshot-Kopie** und wählen Sie eine Snapshot-Kopie aus der Liste aus.
6. Klicken Sie auf **Senden**.

   Sie kehren zum Dialogfeld „Neu synchronisieren“ zurück.

7. Wenn Sie mehr als eine Quelle zur Neusynchronisierung ausgewählt haben, klicken Sie auf **Standard** für die nächste Quelle, für die Sie eine vorhandene Snapshot-Kopie angeben möchten.
8. Klicken Sie auf **Senden**, um den Neusynchronisierungsauftrag zu starten.

   Der Resynchronisierungsauftrag wird gestartet, Sie werden zur Seite mit den Volume-/Integritätsdetails zurückgeleitet und oben auf der Seite wird ein Auftragslink angezeigt.

9. **Optional:** Klicken Sie auf der Seite **Volume-/Integritätsdetails** auf **Jobs anzeigen**, um den Status jedes Resynchronisierungsjobs zu verfolgen.

   Es wird eine gefilterte Liste mit Jobs angezeigt.

10. **Optional:** Klicken Sie in Ihrem Browser auf den Pfeil **Zurück**, um zur Detailseite **Volumen/Gesundheit** zurückzukehren.

    Der Neusynchronisierungsauftrag ist abgeschlossen, wenn alle Auftragsaufgaben erfolgreich abgeschlossen wurden.

Beheben eines Schutzauftragsfehlers

Dieser Workflow bietet ein Beispiel dafür, wie Sie einen Schutzauftragsfehler über das Unified Manager-Dashboard identifizieren und beheben können.

Bevor Sie beginnen

Da für einige Aufgaben in diesem Workflow eine Anmeldung mit der Administratorrolle erforderlich ist, müssen Sie mit den für die Verwendung verschiedener Funktionen erforderlichen Rollen vertraut sein.

In diesem Szenario greifen Sie auf die Dashboard-Seite zu, um zu sehen, ob es Probleme mit Ihren Schutzaufträgen gibt. Im Bereich „Schutzvorfall“ stellen Sie fest, dass ein Vorfall „Job beendet“ vorliegt, der den Fehler „Schutzauftrag fehlgeschlagen“ auf einem Volume anzeigt. Sie untersuchen diesen Fehler, um die mögliche Ursache und mögliche Lösung zu ermitteln.

Schritte

1. Klicken Sie im Bereich „Schutzvorfälle“ des Dashboard-Bereichs „Ungelöste Vorfälle und Risiken“ auf das Ereignis „Schutzauftrag fehlgeschlagen“.

Der verlinkte Text zur Veranstaltung hat die Form `object_name:/object_name - Error Name` , wie zum Beispiel `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed.`

Die Seite mit den Ereignisdetails für den fehlgeschlagenen Schutzauftrag wird angezeigt.

2. Überprüfen Sie die Fehlermeldung im Feld „Ursache“ des Bereichs „Zusammenfassung“, um das Problem zu ermitteln und mögliche Korrekturmaßnahmen zu bewerten.

   Sehen"Identifizieren des Problems und Ausführen von Korrekturmaßnahmen für einen fehlgeschlagenen Schutzauftrag" .

Identifizieren Sie das Problem und führen Sie Korrekturmaßnahmen für einen fehlgeschlagenen Schutzjob durch

Sie überprüfen die Fehlermeldung zum Auftragsfehler im Feld „Ursache“ auf der Seite „Ereignisdetails“ und stellen fest, dass der Auftrag aufgrund eines Snapshot-Kopierfehlers fehlgeschlagen ist. Anschließend fahren Sie mit der Seite mit den Volumen-/Gesundheitsdetails fort, um weitere Informationen zu erhalten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ verfügen.

Die im Feld „Ursache“ auf der Seite „Ereignisdetails“ angegebene Fehlermeldung enthält den folgenden Text zum fehlgeschlagenen Auftrag:

```
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 die folgenden Informationen:

- Ein Sicherungs- oder Spiegelungsauftrag wurde nicht erfolgreich abgeschlossen.

  Der Auftrag beinhaltete eine Schutzbeziehung zwischen dem Quellvolume `cluster2_src_vol2` auf dem virtuellen Server `cluster2_src_svm` und das Zielvolumen `managed_svc2_vol3` auf dem virtuellen Server mit dem Namen `cluster3_dst_svm` .

- Ein Snapshot-Kopierauftrag ist fehlgeschlagen für `0426cluster2_src_vol2snap` auf dem Quellvolume `cluster2_src_svm:/cluster2_src_vol2` .

In diesem Szenario können Sie die Ursache und mögliche Korrekturmaßnahmen für den Auftragsfehler ermitteln. Um den Fehler zu beheben, müssen Sie jedoch entweder auf die Web-Benutzeroberfläche des System Managers oder auf die ONTAP CLI-Befehle zugreifen.

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 vorliegt.

   Optional könnten Sie am Ende der Fehlermeldung auf den Link **Jobdetails** klicken, für die Zwecke dieses Szenarios möchten wir dies jedoch nicht tun.

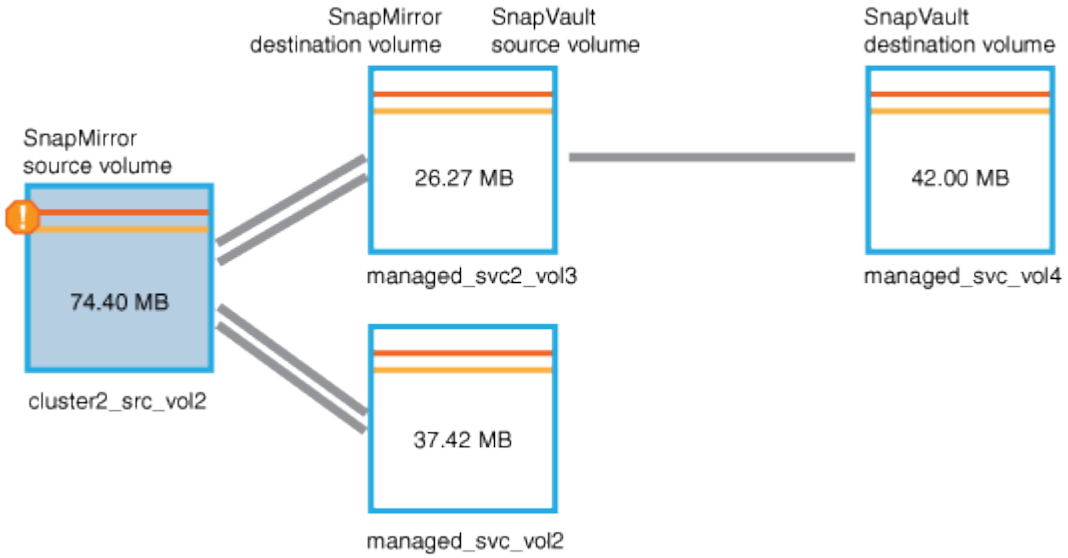
2. Sie entscheiden, dass Sie versuchen möchten, das Ereignis zu beheben, und gehen daher wie folgt vor:
   a. Klicken Sie auf die Schaltfläche **Zuweisen an** und wählen Sie **Mich** aus dem Menü.
   b. Klicken Sie auf die Schaltfläche **Bestätigen**, damit Sie keine weiteren Warnmeldungen mehr erhalten, wenn für das Ereignis Warnmeldungen festgelegt wurden.
   c. Optional können Sie auch Notizen zur Veranstaltung hinzufügen.
3. Klicken Sie im Bereich **Zusammenfassung** auf das Feld **Quelle**, um Details zum Quellvolume anzuzeigen.

   Das Feld **Quelle** enthält den Namen des Quellobjekts: in diesem Fall das Volume, auf dem der Snapshot-Kopierauftrag geplant war.

   Die Seite mit den Volumen-/Gesundheitsdetails wird angezeigt für `cluster2_src_vol2` , zeigt den Inhalt der Registerkarte „Schutz“.

4. Wenn Sie sich das Schutztopologiediagramm ansehen, sehen Sie ein Fehlersymbol, das mit dem ersten Volume in der Topologie verknüpft ist, bei dem es sich um das Quellvolume für die SnapMirror -Beziehung handelt.

   Sie sehen auch die horizontalen Balken im Symbol des Quellvolumes, die die für dieses Volume festgelegten Warn- und Fehlerschwellenwerte anzeigen.



5. Sie platzieren den Cursor über dem Fehlersymbol, um das Popup-Dialogfeld mit den Schwellenwerteinstellungen anzuzeigen. Sie sehen, dass das Volume den Fehlerschwellenwert überschritten hat, was auf ein Kapazitätsproblem hinweist.
6. Klicken Sie auf die Registerkarte **Kapazität**.

   Kapazitätsinformationen zum Volumen `cluster2_src_vol2` angezeigt.

7. Im Bereich **Kapazität** sehen Sie, dass im Balkendiagramm ein Fehlersymbol angezeigt wird, das wiederum

darauf hinweist, dass die Volume-Kapazität den für das Volume festgelegten Schwellenwert überschritten hat.

8. Unter dem Kapazitätsdiagramm sehen Sie, dass die automatische Volumevergrößerung deaktiviert und eine Volume-Speicherplatzgarantie festgelegt wurde.

   Sie könnten sich dafür entscheiden, die automatische Vergrößerung zu aktivieren, aber für die Zwecke dieses Szenarios entscheiden Sie sich, weitere Untersuchungen durchzuführen, bevor Sie eine Entscheidung darüber treffen, wie das Kapazitätsproblem gelöst werden soll.

9. Sie scrollen nach unten zur Liste **Ereignisse** und sehen, dass die Ereignisse „Schutzauftrag fehlgeschlagen“, „Volumen in Tagen bis zur Volllast“ und „Volumenspeicher voll“ generiert wurden.
10. Klicken Sie in der Liste **Ereignisse** 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 „Volumenspeicher voll“ für das Quellvolume angezeigt.

11. Im Bereich **Zusammenfassung** lesen Sie das Feld Ursache für das Ereignis: `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Unter dem Bereich „Zusammenfassung“ werden die vorgeschlagenen Korrekturmaßnahmen angezeigt.

    Die vorgeschlagenen Korrekturmaßnahmen werden nur für einige Ereignisse angezeigt, daher wird dieser Bereich nicht für alle Ereignistypen angezeigt.

    Sie klicken sich durch die Liste der vorgeschlagenen Aktionen, die Sie zur Behebung des Ereignisses „Vollspeicherplatz voll“ durchführen können:

    - Aktivieren Sie die automatische Vergrößerung auf diesem Volume.
    - Ändern Sie die Größe des Volumes.
    - Aktivieren und führen Sie die Deduplizierung auf diesem Volume aus.
    - Aktivieren und führen Sie die Komprimierung auf diesem Datenträger aus.

13. Sie entscheiden sich, die automatische Vergrößerung auf dem Volume zu aktivieren. Dazu müssen Sie jedoch den verfügbaren freien Speicherplatz auf dem übergeordneten Aggregat und die aktuelle Volume-Wachstumsrate ermitteln:
    a. Schauen Sie sich das übergeordnete Aggregat an. `cluster2_src_aggr1` , 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 Volumevergrößerung zu ermöglichen.

    b. Sehen Sie sich oben auf der Seite das Symbol an, das auf einen kritischen Vorfall hinweist, und lesen Sie den Text unter dem Symbol.

       Sie stellen fest: „Tage bis zur Vollendung: Weniger als ein Tag | Tägliche Wachstumsrate: 5,4 %“.

14. Gehen Sie zum System Manager oder greifen Sie auf die ONTAP CLI zu, um die `volume autogrow` Option.

Notieren Sie sich die Namen des Volumes und des Aggregats, damit Sie sie beim Aktivieren der automatischen Vergrößerung zur Hand haben.

15. Kehren Sie nach der Lösung des Kapazitätsproblems zur Detailseite des Unified Manager-Ereignisses zurück und markieren Sie das Ereignis als gelöst.

Beheben von Verzögerungsproblemen

Dieser Arbeitsablauf bietet ein Beispiel dafür, wie Sie ein Verzögerungsproblem lösen können. In diesem Szenario greifen Sie als Administrator oder Operator auf die Unified ManagerDashboard-Seite zu, um zu sehen, ob es Probleme mit Ihren Schutzbeziehungen gibt, und um gegebenenfalls Lösungen zu finden.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Auf der Dashboard-Seite sehen Sie sich den Bereich „Ungelöste Vorfälle und Risiken“ an und sehen im Schutzbereich unter „Schutzrisiken“ einen SnapMirror -Verzögerungsfehler.

Schritte

1. Suchen Sie im Bereich **Schutz** auf der Seite **Dashboard** nach dem Fehler „SnapMirror -Beziehungsverzögerung“ und klicken Sie darauf.

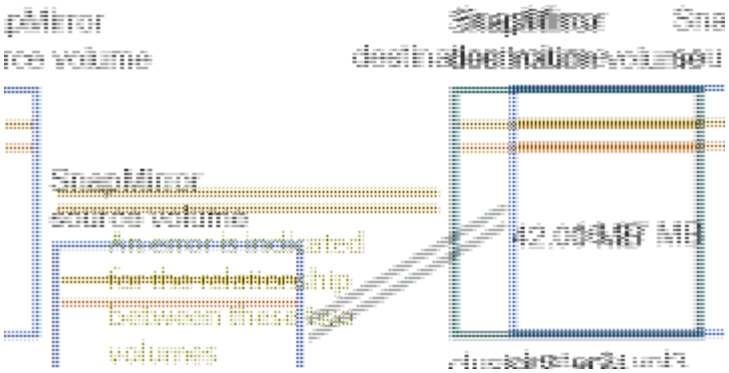
   Die Seite mit den Ereignisdetails für das Verzögerungsfehlerereignis wird angezeigt.

2. Auf der Detailseite **Ereignis** können Sie eine oder mehrere der folgenden Aufgaben ausführen:
   - Überprüfen Sie die Fehlermeldung im Feld „Ursache“ des Bereichs „Zusammenfassung“, um festzustellen, ob Korrekturmaßnahmen vorgeschlagen werden.
   - Klicken Sie im Feld „Quelle“ des Bereichs „Zusammenfassung“ auf den Objektnamen (in diesem Fall ein Volume), um Details zum Volume zu erhalten.
   - Suchen Sie nach Notizen, die möglicherweise zu diesem Ereignis hinzugefügt wurden.
   - Fügen Sie dem Ereignis eine Notiz hinzu.
   - Weisen Sie das Ereignis einem bestimmten Benutzer zu.
   - Bestätigen oder beheben Sie das Ereignis.
3. In diesem Szenario klicken Sie auf den Objektnamen (in diesem Fall ein Volume) im Feld „Quelle“ des Bereichs „Zusammenfassung“, um Details zum Volume zu erhalten.

   Die Registerkarte „Schutz“ der Seite „Volume-/Integritätsdetails“ wird angezeigt.

4. Im Reiter **Schutz** sehen Sie sich das Topologiediagramm an.

   Sie stellen fest, dass das Volume mit dem Verzögerungsfehler das letzte Volume in einer SnapMirror Kaskade mit drei Volumes ist. Das von Ihnen ausgewählte Volume ist dunkelgrau umrandet und eine doppelte orange Linie vom Quellvolume weist auf einen SnapMirror Beziehungsfehler hin.



5. Klicken Sie auf jedes der Volumes in der SnapMirror Kaskade.

   Wenn Sie die einzelnen Volumes auswählen, ändern sich die Schutzinformationen in den Bereichen „Zusammenfassung“, „Topologie“, „Verlauf“, „Ereignisse“, „Verwandte Geräte“ und „Verwandte Warnungen“, um Details anzuzeigen, die für das ausgewählte Volume relevant sind.

6. Sie sehen sich den Bereich **Zusammenfassung** an und positionieren den Cursor über dem Informationssymbol im Feld **Aktualisierungsplan** für jeden Band.

   In diesem Szenario beachten Sie, dass die SnapMirror -Richtlinie DPDefault ist und der SnapMirror -Zeitplan stündlich fünf Minuten nach der vollen Stunde aktualisiert wird. Sie stellen fest, dass alle Volumes in der Beziehung gleichzeitig versuchen, eine SnapMirror -Übertragung abzuschließen.

7. Um das Verzögerungsproblem zu beheben, ändern Sie die Zeitpläne für zwei der kaskadierten Volumes, sodass jedes Ziel eine SnapMirror Übertragung beginnt, nachdem seine Quelle eine Übertragung abgeschlossen hat.

Verwalten und Überwachen von Schutzbeziehungen

Mit Active IQ Unified Manager können Sie Schutzbeziehungen erstellen, SnapMirror und SnapVault -Beziehungen auf verwalteten Clustern überwachen und Fehler beheben sowie Daten wiederherstellen, wenn diese 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 bestimmt.

- Synchron

  Die Replikation wird gleichzeitig auf dem primären und sekundären Volume durchgeführt.

Sie können bis zu 10 Schutzaufträge gleichzeitig ausführen, ohne dass die Leistung darunter leidet. Wenn Sie zwischen 11 und 30 Jobs gleichzeitig ausführen, kann es zu Leistungseinbußen kommen. Es wird nicht empfohlen, mehr als 30 Jobs gleichzeitig auszuführen.

Anzeigen des Volume-Schutzstatus

Die Seite „Datenschutz“ bietet eine ganzheitliche Ansicht der Datenschutzdetails für alle geschützten Volumes in einem einzelnen Cluster oder für alle Cluster in einem Rechenzentrum.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Dashboard**.
2. Je nachdem, ob Sie den Datenschutzstatus für alle überwachten Cluster oder für einen einzelnen Cluster anzeigen möchten, wählen Sie **Alle Cluster** oder einen einzelnen Cluster aus dem Dropdown-Menü aus.
3. Klicken Sie oben im Bereich „Datenschutz“ auf den Rechtspfeil. Die Seite **Datenschutz** wird angezeigt.

Je nachdem, ob Sie einen einzelnen oder alle Cluster in Ihrem Rechenzentrum ausgewählt haben, wird auf dieser Seite der Datenschutzstatus der durch Snapshot-Kopien oder SnapMirror Richtlinien geschützten Volumes sowie die Anzahl der ungeschützten Volumes angezeigt.

Wenn Sie einen Cluster aus der Liste **Einzelner Cluster** auswählen, werden der Snapshot-Schutz und der SnapMirror Beziehungsstatus der geschützten Volumes in diesem Cluster angezeigt.

Wenn Sie auf dieser Seite auf die Ereignisse klicken, gelangen Sie zur Seite mit den Ereignisdetails. Sie können auf den Link **Alle anzeigen** klicken, um alle aktiven Schutzereignisse auf der Inventarseite der Ereignisverwaltung anzuzeigen. Sie können mit der Maus darüberfahren, um die jeweiligen Zählungen und Legenden anzuzeigen. Sie können auf Folgendes klicken:

- Die Balkendiagramme für ungeschützte Volumes und durch Snapshot-Kopien geschützte Volumes ermöglichen es Ihnen, zur Seite „Volumes“ zu gelangen und die Details anzuzeigen.
- Die Balkendiagramme für alle Beziehungen führen zur Seite „Beziehungen“, wo die Details nach dem Quellcluster gefiltert werden.

Anzeigen des Schutzstatus von Volumes, die durch Snapshot-Kopien geschützt sind

Übersicht über Snapshot-Kopien: Eine Übersicht über die durch Snapshot-Kopien geschützten Volumes, wie etwa:

- Die Gesamtzahl der durch Snapshot-Kopien geschützten und nicht geschützten Volumes.
- Die Gesamtzahl der Volumes, die den reservierten Speicherplatz für die Snapshot-Kopien verwenden oder überschreiten.

Analyse von Snapshot-Kopien enthält die folgenden Informationen:

- Einzelne Ereignisse für Snapshot-Kopien, einschließlich der in den letzten 24 Stunden ausgelösten Ereignisse.
- Detailliertes Diagramm für durch Snapshot-Kopien geschützte und nicht geschützte Volumes.
- Volumes, die die reservierte Snapshot-Kopierkapazität nutzen, nicht nutzen und überschreiten.
- Die Aufschlüsselung der Volumezählung erfolgt anhand der Anzahl ihrer Snapshot-Kopien.

Zu beachtende Punkte bei Snapshot-Kopien

- Beim Zählen der durch Snapshot-Kopien geschützten Volumes werden sowohl Quell- als auch Zielvolumes 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. Es 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 Speicherplatzes anzuzeigen oder um den Speicherplatz zu berechnen, der zurückgewonnen werden kann, wenn eine oder mehrere Snapshot-Kopien gelöscht werden.

Schutzstatus für SnapMirror -Beziehungen anzeigen

- SnapMirror -Übersicht*: Eine Übersicht über die durch SnapMirror -Richtlinien geschützten Volumes, wie z. B.:
- Die Anzahl der durch die jeweiligen SnapMirror Richtlinien geschützten Volumes, z. B. Volume- SnapMirror -Beziehungen, Storage VM Disaster Recovery (SVM-DR) und deren Kombinationen.
- Die Gesamtzahl der SnapMirror -Beziehungen, bei denen basierend auf dem Verzögerungsstatus eine Verzögerung des Recovery Point Objectives (RPO) auftritt.
- SnapMirror -Analyse* enthält die folgenden Informationen:
- Einzelne Ereignisse, die für SnapMirror -Beziehungen ausgelöst wurden, einschließlich der Ereignisse, die in den letzten 24 Stunden ausgelöst wurden
- Die Anzahl der durch jeden SnapMirror Richtlinientyp geschützten Volumes.
- Die Anzahl der durch die SnapMirror Beziehungstypen geschützten Beziehungen, z. B. Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StricxtSync, SnapMirror Active Sync Consistency Group und Sync.
- Die Anzahl gesunder und ungesunder Beziehungen.
- Aufschlüsselung der Volumenverhältniszählung. Sie können die Diagramme nach RPO-Verzögerungszeit und -Status umschalten.
- Verzögerungsschwellenwerte für nicht verwaltete Beziehungen. Sie können auf das Einstellungssymbol

  ( ), um die Einstellungen für den Verzögerungsschwellenwert zu konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von Verzögerungsschwellenwerteinstellungen für nicht verwaltete Schutzbeziehungen".

Zu beachtende Punkte für SnapMirror -Beziehungen

- Zum Zählen der SnapMirror -Beziehungen werden die Quellvolumes gezählt, die zum Lesen und Schreiben aktiviert sind. Ziel- und Stammvolumes werden nicht berücksichtigt.
- Bei SnapMirror -Beziehungen werden die Ereignisse für den Quellcluster angezeigt.
- Die SnapMirror Beziehungsanzahl umfasst die Anzahl der Volumes mit Quellen und Zielen auf demselben oder auf verschiedenen Clustern.
- Die Verzögerungsdauer der RPO-Verzögerung bei der Datenreplikation basiert auf der SnapMirror -Beziehung. Der Status wird kategorisiert als `ok` , `warning` , oder `error` , basierend auf dem festgelegten Beziehungsschwellenwert. Sie können den Status überprüfen, um festzustellen, ob die Parameter wie erwartet funktionieren oder ob Sie ein Problem beheben müssen.
- Wenn ein Volume über mehrere SnapMirror -Beziehungen verfügt, wird jeder Beziehungstyp für die RPO-Verzögerung gezählt.
- Volume-Beziehungen gelten als fehlerhaft, wenn es Probleme bei der Datenreplikation zwischen Quelle

und Ziel gibt, beispielsweise wenn die Beziehung unterbrochen ist.

Durch die MetroCluster Konfiguration geschützte Cluster anzeigen

Das Bedienfeld * MetroCluster -Schutz* auf der Seite **Datenschutz** zeigt die Anzahl der Cluster an, die an Ihrem Standort durch MetroCluster über FC oder IP-Konfiguration geschützt oder nicht geschützt sind. Wenn Sie auf die Balkendiagramme in diesem Bereich klicken, gelangen Sie zur Seite „Cluster“, auf der die Clusterdetails basierend auf den geschützten oder ungeschützten Clustern gefiltert werden. Informationen zur Überwachung Ihrer MetroCluster -Konfiguration finden Sie unter"Überwachung von MetroCluster -Konfigurationen" .

Anzeigen von Volume-Schutzbeziehungen

In der Ansicht „Beziehung: Alle Beziehungen“ und auf der Seite „Volume-Beziehungen“ können Sie den Status bestehender Volume- SnapMirror und SnapVault -Beziehungen anzeigen. Sie können auch Details zu Schutzbeziehungen prüfen, einschließlich Übertragungs- und Verzögerungsstatus, Quell- und Zieldetails, Zeitplan- und Richtlinieninformationen usw.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können von dieser Seite aus auch Beziehungsbefehle initiieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Beziehung“ > „Alle Beziehungen“ aus.

   Die Ansicht „Beziehung: Alle Beziehungen“ wird angezeigt.

3. Wählen Sie eine der folgenden Möglichkeiten, um die Details zum Volumeschutz anzuzeigen:

   - Um aktuelle Informationen zu allen Volumenbeziehungen anzuzeigen, bleiben Sie auf der Standardseite **Alle Beziehungen**.
   - Um detaillierte Informationen zu den Volumenübertragungstrends über einen bestimmten Zeitraum anzuzeigen, wählen Sie im Menü „Ansicht“ die Option „Beziehung: Übertragungsstatusansicht des letzten Monats“.
   - Um detaillierte Informationen zur täglichen Volumenübertragungsaktivität anzuzeigen, wählen Sie im Menü „Ansicht“ die Option „Beziehung: Übertragungsrate des letzten Monats“ aus.

   Die Volume-Übertragungsansichten zeigen nur Informationen zu Volumes in asynchronen Beziehungen an – Volumes in synchronen Beziehungen werden nicht angezeigt.

Überwachen von LUNs in einer Konsistenzgruppenbeziehung

Wenn Ihre ONTAP Umgebung SnapMirror Active Sync zum Schutz von Anwendungen mit LUNs unterstützt, können Sie diese LUNs auf Active IQ Unified Manager anzeigen und überwachen.

SnapMirror Active Sync gewährleistet beim Failover in SAN-Umgebungen eine Recovery Time Objective

(RTO) von Null. In einer typischen Bereitstellung, die 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 über die Quell- und Zielstandorte dieser zusammengesetzten LUNs gemultiplext, um Transparenz zu gewährleisten.

Zum Anzeigen zusammengesetzter LUNs sollten sowohl die primären als auch die sekundären Cluster mit den LUNs, die Teil der Konsistenzgruppenbeziehung sind, hinzugefügt und im Unified Manager erkannt werden. Es werden nur iSCSI- und FCP-LUNs unterstützt.

Informationen zur SnapMirror Active Sync finden Sie unter"ONTAP 9-Dokumentation für SnapMirror Active Sync (früher SM-BC)" .

Um zusammengesetzte LUNs in Ihrer Umgebung anzuzeigen, führen Sie die folgenden Schritte aus:

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **LUNs**.
2. Wählen Sie im Menü „Ansicht“ die Option „Beziehung“ > „Alle LUNs“ aus.

   Die Ansicht „Beziehung: Alle LUNs“ wird angezeigt.

Sie können die LUN-Details anzeigen, z. B. den LUN-Namen, das Volume, die Speicher-VM, auf der die LUN gehostet wird, den Cluster, die Konsistenzgruppe und die Partner-LUN. Sie können auf jede dieser Komponenten klicken, um eine Detailansicht anzuzeigen. Durch Klicken auf die Konsistenzgruppe gelangen Sie zur Seite „Beziehungen“.

Durch Klicken auf die Partner-LUN können Sie deren Konfigurationsdetails auf der Registerkarte „SAN“ der Seite „Storage-VM-Details“ für die Storage-VM anzeigen, auf der die Partner-LUN gehostet wird. Es werden Informationen wie die Initiatoren und Initiatorgruppen sowie andere Aspekte der Partner-LUN angezeigt.

Sie können die Standardfunktionen auf Rasterebene zum Sortieren, Filtern, Generieren und Hochladen von Berichten für die geschützten LUNs in Ihrer Umgebung ausführen.

Erstellen Sie eine SnapVault -Schutzbeziehung aus der Ansicht „Health: Alle Volumes“

Sie können die Ansicht „Health: Alle Volumes“ verwenden, um SnapVault -Beziehungen für ein oder mehrere Volumes auf derselben Storage-VM zu erstellen, um Datensicherungen zu Schutzzwecken zu ermöglichen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Das Menü **Schützen** wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: zum Beispiel, wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie in der Ansicht **Health: All Volumes** ein Volume aus, das Sie schützen möchten, und klicken Sie auf **Schützen**.

   Alternativ können Sie zum Erstellen mehrerer Schutzbeziehungen auf derselben virtuellen Speichermaschine (SVM) ein oder mehrere Volumes in der Ansicht „Integrität: Alle Volumes“ auswählen und in der Symbolleiste auf **Schützen** klicken.

3. Wählen Sie * SnapVault* aus dem Menü.

   Das Dialogfeld „Schutz konfigurieren“ wird geöffnet.

4. Klicken Sie auf * SnapVault*, um die Registerkarte * SnapVault* anzuzeigen und die Informationen zum sekundären Volume zu konfigurieren.
5. Klicken Sie auf **Erweitert**, um Deduplizierung, Komprimierung, automatische Vergrößerung und Speicherplatzgarantie nach Bedarf einzustellen, und klicken Sie dann auf **Übernehmen**.
6. Füllen Sie den Bereich **Zielinformationen** und den Bereich **Beziehungseinstellungen** auf der Registerkarte * SnapVault* aus.
7. Klicken Sie auf **Übernehmen**.

   Sie kehren zur Ansicht „Health: All Volumes“ zurück.

8. Klicken Sie oben in der Ansicht „Integrität: Alle Volumes“ auf den Link zum Schutzkonfigurationsauftrag.

   Wenn Sie nur eine Schutzbeziehung erstellen, wird die Seite „Jobdetails“ angezeigt. Wenn Sie jedoch mehr als eine Schutzbeziehung erstellen, wird eine gefilterte Liste aller mit dem Schutzvorgang verknüpften Jobs angezeigt.

9. Führen Sie einen der folgenden Schritte aus:
   - Wenn Sie nur einen Job haben, klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails im Zusammenhang mit dem Schutzkonfigurationsjob zu aktualisieren und festzustellen, wann der Job abgeschlossen ist.
   - Wenn Sie mehr als einen Job haben:
     i. Klicken Sie in der Jobliste auf einen Job.
     ii. Klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails im Zusammenhang mit dem Schutzkonfigurationsauftrag zu aktualisieren und festzustellen, wann der Auftrag abgeschlossen ist.
     iii. Verwenden Sie die Schaltfläche **Zurück**, um zur gefilterten Liste zurückzukehren und einen anderen Job anzuzeigen.

Erstellen Sie eine SnapVault -Schutzbeziehung auf der Seite „Volume/Health-Details“

Sie können mithilfe der Seite „Volume-/Integritätsdetails“ eine SnapVault Beziehung erstellen, sodass Datensicherungen zu Schutzzwecken auf Volumes aktiviert werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

- Sie müssen die Workflow-Automatisierung eingerichtet haben, um diese Aufgabe auszuführen.

Das Menü **Schützen** wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: zum Beispiel, wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** mit der rechten Maustaste auf ein Volume in der Topologieansicht, das Sie schützen möchten.
2. Wählen Sie im Menü **Schützen** > * SnapVault*.

   Das Dialogfeld „Schutz konfigurieren“ wird geöffnet.

3. Klicken Sie auf * SnapVault*, um die Registerkarte * SnapVault* anzuzeigen und die Informationen zur sekundären Ressource zu konfigurieren.
4. Klicken Sie auf **Erweitert**, um Deduplizierung, Komprimierung, automatische Vergrößerung und Speicherplatzgarantie nach Bedarf einzustellen, und klicken Sie dann auf **Übernehmen**.
5. Füllen Sie die Bereiche **Zielinformationen** und **Beziehungseinstellungen** im Dialogfeld **Schutz konfigurieren** aus.
6. Klicken Sie auf **Übernehmen**.

   Sie werden zur Seite mit den Volumen-/Gesundheitsdetails zurückgeleitet.

7. Klicken Sie oben auf der Detailseite **Volume/Integrität** auf den Link zum Schutzkonfigurationsauftrag.

   Die Seite mit den Auftragsdetails wird angezeigt.

8. Klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails im Zusammenhang mit dem Schutzkonfigurationsauftrag zu aktualisieren und festzustellen, wann der Auftrag abgeschlossen ist.

   Wenn die Jobaufgaben abgeschlossen sind, werden die neuen Beziehungen in der Topologieansicht der Seite „Volume-/Integritätsdetails“ angezeigt.

Erstellen Sie eine SnapMirror -Schutzbeziehung aus der Ansicht „Health: All Volumes“

Mithilfe der Ansicht „Health: Alle Volumes“ können Sie mehrere SnapMirror Schutzbeziehungen gleichzeitig erstellen, indem Sie mehr als ein Volume auf derselben Speicher-VM auswählen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Das Menü **Schützen** wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: zum Beispiel, wenn Sie nur über Operator-

Berechtigungen verfügen

- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde

Schritte

1. Wählen Sie in der Ansicht **Health: All Volumes** ein Volume aus, das Sie schützen möchten.

   Alternativ können Sie zum Erstellen mehrerer Schutzbeziehungen auf derselben SVM ein oder mehrere Volumes in der Ansicht „Integrität: Alle Volumes“ auswählen und in der Symbolleiste auf **Schützen** > * SnapMirror* klicken.

   Das Dialogfeld „Schutz konfigurieren“ wird angezeigt.

2. Klicken Sie auf * SnapMirror*, um die Registerkarte * SnapMirror* anzuzeigen und die Zielinformationen zu konfigurieren.
3. Klicken Sie auf **Erweitert**, um die Speicherplatzgarantie nach Bedarf festzulegen, und klicken Sie dann auf **Übernehmen**.
4. Füllen Sie den Bereich **Zielinformationen** und den Bereich **Beziehungseinstellungen** auf der Registerkarte * SnapMirror* aus.
5. Klicken Sie auf **Übernehmen**.

   Sie kehren zur Ansicht „Health: All Volumes“ zurück.

6. Klicken Sie oben in der Ansicht „Integrität: Alle Volumes“ auf den Link zum Auftrag zur Schutzkonfiguration.

   Wenn Sie nur eine Schutzbeziehung erstellen, wird die Seite „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 Sie nur einen Job haben, klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails im Zusammenhang mit dem Schutzkonfigurationsjob zu aktualisieren und festzustellen, wann der Job abgeschlossen ist.
   - Wenn Sie mehr als einen Job haben:
     i. Klicken Sie in der Jobliste auf einen Job.
     ii. Klicken Sie auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails im Zusammenhang mit dem Schutzkonfigurationsauftrag zu aktualisieren und festzustellen, wann der Auftrag abgeschlossen ist.
     iii. Verwenden Sie die Schaltfläche **Zurück**, um zur gefilterten Liste zurückzukehren und einen anderen Job anzuzeigen.

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 Variationen sein:

- Wenn Sie eine Ziel-SVM angegeben haben, die im Vergleich zum Quellvolume unter derselben oder einer neueren Version von ONTAP ausgeführt wird, ist eine auf Blockreplikation basierende SnapMirror Beziehung das Standardergebnis.
- Wenn Sie eine Ziel-SVM angegeben haben, die unter derselben oder einer neueren Version von ONTAP im Vergleich zum Quellvolume ausgeführt wird, Sie 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 der des Quellvolumes ausgeführt wird und die frühere Version versionsflexible Replikation unterstützt, ist eine SnapMirror Beziehung mit versionsflexibler Replikation das automatische Ergebnis.

Erstellen Sie eine SnapMirror -Schutzbeziehung auf der Seite „Volume/Health-Details“

Sie können die Seite mit den Volume-/Integritätsdetails verwenden, um eine SnapMirror -Beziehung zu erstellen, sodass die Datenreplikation zu Schutzzwecken aktiviert wird. Mit der SnapMirror -Replikation können Sie im Falle eines Datenverlusts auf der Quelle Daten vom Zielvolume wiederherstellen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Das Menü **Schützen** wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: zum Beispiel, wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde

Sie können bis zu 10 Schutzaufträge gleichzeitig ausführen, ohne dass die Leistung darunter leidet. Wenn Sie zwischen 11 und 30 Jobs gleichzeitig ausführen, kann es zu Leistungseinbußen kommen. Es wird nicht empfohlen, mehr als 30 Jobs gleichzeitig auszuführen.

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** in der Topologieansicht mit der rechten Maustaste auf den Namen eines Volumes, das Sie schützen möchten.
2. Wählen Sie im Menü **Schützen** > * SnapMirror*.

   Das Dialogfeld „Schutz konfigurieren“ wird angezeigt.

3. Klicken Sie auf * SnapMirror*, um die Registerkarte * SnapMirror* anzuzeigen und die Zielinformationen zu konfigurieren.
4. Klicken Sie auf **Erweitert**, um die Speicherplatzgarantie nach Bedarf festzulegen, und klicken Sie dann auf **Übernehmen**.
5. Füllen Sie die Bereiche **Zielinformationen** und **Beziehungseinstellungen** im Dialogfeld **Schutz konfigurieren** aus.
6. Klicken Sie auf **Übernehmen**.

   Sie werden zur Seite mit den Volumen-/Gesundheitsdetails zurückgeleitet.

7. Klicken Sie oben auf der Detailseite **Volume/Integrität** auf den Link zum Schutzkonfigurationsauftrag.

   Die Aufgaben und Details des Auftrags werden auf der Seite „Auftragsdetails“ angezeigt.

8. Klicken Sie auf der Detailseite des **Auftrags** auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Schutzkonfigurationsauftrag verknüpft sind, und um festzustellen, wann der Auftrag abgeschlossen ist.
9. Wenn die Jobaufgaben abgeschlossen sind, klicken Sie in Ihrem Browser auf **Zurück**, um zur Detailseite **Volumen/Zustand** zurückzukehren.

   Die neue Beziehung wird in der Topologieansicht der Seite „Volume-/Integritätsdetails“ 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 Variationen sein:

- Wenn Sie eine Ziel-SVM angegeben haben, die im Vergleich zum Quellvolume unter derselben oder einer neueren Version von ONTAP ausgeführt wird, ist eine auf Blockreplikation basierende SnapMirror Beziehung das Standardergebnis.
- Wenn Sie eine Ziel-SVM angegeben haben, die unter derselben oder einer neueren Version von ONTAP im Vergleich zum Quellvolume ausgeführt wird, Sie 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 einer höheren Version als die des Quellvolumes ausgeführt wird und die frühere Version versionsflexible Replikation unterstützt, ist eine SnapMirror -Beziehung mit versionsflexibler Replikation das automatische Ergebnis.

Erstellen einer SnapMirror -Beziehung mit versionsflexibler Replikation

Sie können eine SnapMirror -Beziehung mit versionsflexibler Replikation erstellen. Durch die versionsflexible Replikation können Sie den SnapMirror Schutz implementieren, auch wenn Quell- und Zielvolumes unter unterschiedlichen ONTAP Versionen ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.
- Für die Quell- und Ziel-SVMs muss jeweils eine SnapMirror -Lizenz aktiviert sein.
- Die Quell- und Ziel-SVMs müssen jeweils unter einer Version der ONTAP -Software ausgeführt werden, die eine versionsflexible Replikation unterstützt.

SnapMirror mit versionsflexibler Replikation ermöglicht Ihnen die Implementierung des SnapMirror Schutzes auch in heterogenen Speicherumgebungen, in denen nicht der gesamte Speicher unter einer ONTAP-Version läuft. Allerdings werden Spiegelvorgänge unter SnapMirror mit versionsflexibler Replikation nicht so schnell ausgeführt wie unter herkömmlicher SnapMirror-Blockreplikation.

Schritte

1. Zeigen Sie das Dialogfeld **Schutz konfigurieren** für das Volume an, das Sie schützen möchten.
   - Wenn Sie die Registerkarte „Schutz“ der Seite „Volume-/Integritätsdetails“ anzeigen, klicken Sie mit der rechten Maustaste in die Topologieansicht mit dem Namen eines Volumes, das Sie schützen möchten, und wählen Sie im Menü „Schützen“ > „SnapMirror“ aus.
   - Wenn Sie die Ansicht „Integrität: Alle Volumes“ anzeigen, suchen Sie ein Volume, das Sie schützen

möchten, und klicken Sie mit der rechten Maustaste darauf. Wählen Sie dann im Menü **Schützen** > * SnapMirror* aus. Das Dialogfeld „Schutz konfigurieren“ wird angezeigt.

2. Klicken Sie auf * SnapMirror*, um die Registerkarte * SnapMirror* anzuzeigen.
3. Füllen Sie die Bereiche **Zielinformationen** und **Beziehungseinstellungen** im Dialogfeld **Schutz konfigurieren** aus.

   Wenn Sie eine Ziel-SVM angeben, die unter einer früheren Version von ONTAP ausgeführt wird als das Quellvolume, das Sie schützen, und wenn diese frühere Version die versionsflexible Replikation unterstützt, konfiguriert diese Aufgabe SnapMirror automatisch mit versionsflexibler Replikation.

4. Wenn Sie eine Ziel-SVM angeben, die unter derselben ONTAP -Version wie das Quellvolume ausgeführt wird, SnapMirror aber dennoch mit versionsflexibler Replikation konfigurieren möchten, klicken Sie auf **Erweitert**, um die versionsflexible Replikation zu aktivieren, und klicken Sie dann auf **Übernehmen**.
5. Klicken Sie auf **Übernehmen**.

   Sie werden zur Seite mit den Volumen-/Gesundheitsdetails zurückgeleitet.

6. Klicken Sie oben auf der Detailseite **Volume/Integrität** auf den Link zum Schutzkonfigurationsauftrag.

   Die Aufgaben und Details des Auftrags werden auf der Seite „Auftragsdetails“ angezeigt.

7. Klicken Sie auf der Detailseite des **Auftrags** auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Schutzkonfigurationsauftrag verknüpft sind, und um festzustellen, wann der Auftrag abgeschlossen ist.
8. Wenn die Jobaufgaben abgeschlossen sind, klicken Sie in Ihrem Browser auf **Zurück**, um zur Detailseite **Volumen/Zustand** zurückzukehren.

   Die neue Beziehung wird in der Topologieansicht der Seite „Volume-/Integritätsdetails“ angezeigt.

Erstellen Sie SnapMirror -Beziehungen mit versionsflexibler Replikation mit Backup-Option

Sie können eine SnapMirror -Beziehung mit versionsflexibler Replikations- und Sicherungsoption erstellen. Mit der Backup-Option können Sie den SnapMirror Schutz implementieren und außerdem mehrere Versionen von Backup-Kopien am Zielort aufbewahren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.
- Für die Quell- und Ziel-SVMs muss jeweils eine SnapMirror -Lizenz aktiviert sein.
- Für die Quell- und Ziel-SVMs muss jeweils eine SnapVault -Lizenz aktiviert sein.
- Die Quell- und Ziel-SVMs müssen jeweils unter einer Version der ONTAP -Software ausgeführt werden, die eine versionsflexible Replikation unterstützt.

Durch die Konfiguration von SnapMirror mit Backup-Optionsfunktion können Sie Ihre Daten mit den Disaster-Recovery-Funktionen von SnapMirror schützen, beispielsweise mit der Volume-Failover-Funktion, und gleichzeitig SnapVault -Funktionen nutzen, beispielsweise mit dem Schutz mehrerer Backup-Kopien.

Schritte

1. Zeigen Sie das Dialogfeld **Schutz konfigurieren** für das Volume an, das Sie schützen möchten.
   - Wenn Sie die Registerkarte „Schutz“ der Seite „Volume-/Integritätsdetails“ anzeigen, klicken Sie in der Topologieansicht mit der rechten Maustaste auf den Namen eines Volumes, das Sie schützen möchten, und wählen Sie im Menü „Schützen“ > „SnapMirror“ aus.
   - Wenn Sie die Ansicht „Integrität: Alle Volumes“ anzeigen, suchen Sie ein Volume, das Sie schützen möchten, und klicken Sie mit der rechten Maustaste darauf. Wählen Sie dann im Menü **Schützen** > * SnapMirror* aus. Das Dialogfeld „Schutz konfigurieren“ wird angezeigt.
2. Klicken Sie auf * SnapMirror*, um die Registerkarte * SnapMirror* anzuzeigen.
3. Füllen Sie die Bereiche **Zielinformationen** und **Beziehungseinstellungen** im Dialogfeld **Schutz konfigurieren** aus.
4. Klicken Sie auf **Erweitert**, um das Dialogfeld **Erweiterte Zieleinstellungen** anzuzeigen.
5. Wenn das Kontrollkästchen **Versionsflexible Replikation** noch nicht aktiviert ist, aktivieren Sie es jetzt.
6. Aktivieren Sie das Kontrollkästchen **Mit Sicherungsoption**, um die Sicherungsoption zu aktivieren. Klicken Sie anschließend auf **Übernehmen**.
7. Klicken Sie auf **Übernehmen**.

   Sie werden zur Seite mit den Volumen-/Gesundheitsdetails zurückgeleitet.
8. Klicken Sie oben auf der Detailseite **Volume/Integrität** auf den Link zum Schutzkonfigurationsauftrag.

   Die Aufgaben und Details des Auftrags werden auf der Seite „Auftragsdetails“ angezeigt.
9. Klicken Sie auf der Detailseite des **Auftrags** auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails des Schutzkonfigurationsauftrags zu aktualisieren und festzustellen, wann der Auftrag abgeschlossen ist.
10. Wenn die Jobaufgaben abgeschlossen sind, klicken Sie in Ihrem Browser auf **Zurück**, um zur Detailseite **Volumen/Zustand** zurückzukehren.

    Die neue Beziehung wird in der Topologieansicht der Seite „Volume-/Integritätsdetails“ angezeigt.

Konfigurieren der Zieleffizienzeinstellungen

Sie können Zieleffizienzeinstellungen wie Deduplizierung, Komprimierung, automatische Vergrößerung und Speicherplatzgarantie auf einem Schutzziel mithilfe des Dialogfelds „Erweiterte Zieleinstellungen“ konfigurieren. Sie verwenden diese Einstellungen, wenn Sie die Speicherplatznutzung auf einem Ziel- oder sekundären Volume maximieren möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Standardmäßig entsprechen die Effizienzeinstellungen denen des Quellvolumes, mit Ausnahme der Komprimierungseinstellungen in einer SnapVault -Beziehung, die standardmäßig deaktiviert sind.

Schritte

1. Klicken Sie im Dialogfeld **Schutz konfigurieren** entweder auf die Registerkarte * SnapMirror* oder auf die Registerkarte * SnapVault*, je nachdem, welche Art von Beziehung Sie konfigurieren.
2. Klicken Sie im Bereich **Zielinformationen** auf **Erweitert**.

Das Dialogfeld „Erweiterte Zieleinstellungen“ wird geöffnet.

3. Aktivieren oder deaktivieren Sie die Effizienzeinstellungen für Deduplizierung, Komprimierung, Autogrow und Speicherplatzgarantie nach Bedarf.
4. Klicken Sie auf **Übernehmen**, um Ihre Auswahl zu speichern und zum Dialogfeld **Schutz konfigurieren** zurückzukehren.

Erstellen Sie SnapMirror und SnapVault -Zeitpläne

Sie können einfache oder erweiterte SnapMirror und SnapVault -Zeitpläne erstellen, um automatische Datenschutzübertragungen auf einem Quell- oder Primärvolume zu ermöglichen, sodass Übertragungen je nachdem, wie oft sich die Daten auf Ihren Volumes ändern, häufiger oder seltener stattfinden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen den Bereich „Zielinformationen“ im Dialogfeld „Schutz konfigurieren“ bereits ausgefüllt haben.
- Sie müssen die Workflow-Automatisierung eingerichtet haben, um diese Aufgabe auszuführen.

Schritte

1. Klicken Sie auf der Registerkarte * SnapMirror* oder * SnapVault* des Dialogfelds * Schutz konfigurieren * im Bereich * Beziehungseinstellungen * auf den Link * Zeitplan erstellen *.

   Das Dialogfeld „Zeitplan erstellen“ wird angezeigt.

2. Geben Sie im Feld **Zeitplanname** den Namen ein, den Sie dem Zeitplan geben möchten.
3. Wähle eine der folgenden:
   - **Basic**

     Wählen Sie diese Option aus, wenn Sie einen einfachen Intervallplan erstellen möchten.

   - **Fortschrittlich**

     Wählen Sie aus, ob Sie einen Zeitplan im Cron-Stil erstellen möchten.

4. Klicken Sie auf **Erstellen**.

   Der neue Zeitplan wird in der Dropdown-Liste „SnapMirror -Zeitplan“ oder „SnapVault -Zeitplan“ angezeigt.

Erstellen Sie Kaskaden- oder Fanout-Beziehungen, um den Schutz einer bestehenden Schutzbeziehung zu erweitern.

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 können Sie tun, wenn Sie Daten von einer Site auf mehrere Sites kopieren müssen oder um durch die Erstellung weiterer Sicherungen zusätzlichen Schutz zu bieten.

Sie können den Schutz auf Volumes erweitern, indem Sie eine Konsistenzgruppe verwenden. Dabei handelt

es sich um einen Container, der mehrere Volumes enthält, sodass Sie alle Volumes als eine Einheit verwalten können. Sie können die SnapMirror Active Sync Consistency Group und die synchrone Consistency Group-Beziehung auf der Seite „Beziehungen“ von Unified Manager anzeigen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Schritte

1. Klicken Sie auf **Schutz** > **Beziehungen**. Alternativ können Sie die Beziehungen auf der Seite mit den Volumedetails anzeigen.
2. Wählen Sie auf der Seite **Volume-Beziehungen** die SnapMirror -Beziehung aus, deren Schutz Sie erweitern möchten.
3. Klicken Sie in der Aktionsleiste auf **Schutz erweitern**.
4. Wählen Sie im Menü entweder **Von der Quelle** oder **Vom Ziel** aus, je nachdem, ob Sie eine Fanout-Beziehung von der Quelle oder eine Kaskadenbeziehung vom Ziel erstellen.
5. Wählen Sie je nach Art der Schutzbeziehung, die Sie erstellen, entweder **Mit SnapMirror** oder **Mit SnapVault**.

   Das Dialogfeld **Schutz konfigurieren** wird angezeigt.

   Dies kann über die vereinheitlichte Detailseite „Beziehung/Volumenbeziehung“ und „Volumen/Gesundheit“ erreicht werden.

6. Vervollständigen Sie die Informationen wie im Dialogfeld **Schutz konfigurieren** angegeben.

Bearbeiten Sie Schutzbeziehungen auf der Seite „Volume-Beziehungen“.

Sie können vorhandene Schutzbeziehungen bearbeiten, um die maximale Übertragungsrate, die Schutzrichtlinie oder den Schutzzeitplan zu ändern. Sie können eine Beziehung bearbeiten, um die für Übertragungen verwendete Bandbreite zu verringern oder die Häufigkeit geplanter Übertragungen zu erhöhen, da sich die Daten häufig ändern.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die ausgewählten Volumes müssen Ziele mit Schutzbeziehung sein. Sie können Beziehungen nicht bearbeiten, wenn Quellvolumes, Load-Sharing-Volumes oder Volumes ausgewählt sind, die nicht das Ziel einer SnapMirror oder SnapVault -Beziehung sind.

Schritte

1. Wählen Sie auf der Seite **Volume-Beziehungen** in der Volume-Liste ein oder mehrere Volumes in derselben SVM aus, für die Sie die Beziehungseinstellungen bearbeiten möchten, und wählen Sie dann in der Symbolleiste **Bearbeiten** aus.

   Das Dialogfeld „Beziehung bearbeiten“ wird angezeigt.

2. Bearbeiten Sie im Dialogfeld **Beziehung bearbeiten** nach Bedarf die maximale Übertragungsrate, die Schutzrichtlinie oder den Schutzzeitplan.

3. Klicken Sie auf **Übernehmen**.

   Die Änderungen werden auf die ausgewählten Beziehungen angewendet.

Bearbeiten Sie Schutzbeziehungen auf der Seite „Volume-/Integritätsdetails“.

Sie können vorhandene Schutzbeziehungen bearbeiten, um die aktuelle maximale Übertragungsrate, Schutzrichtlinie oder den Schutzzeitplan zu ändern. Sie können eine Beziehung bearbeiten, um die für Übertragungen verwendete Bandbreite zu verringern oder die Häufigkeit geplanter Übertragungen zu erhöhen, da sich die Daten häufig ändern.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen Workflow Automation installiert und konfiguriert haben.

Die ausgewählten Volumes müssen Ziele mit Schutzbeziehung sein. Sie können Beziehungen nicht bearbeiten, wenn Quellvolumes, Load-Sharing-Volumes oder Volumes ausgewählt sind, die nicht das Ziel einer SnapMirror oder SnapVault -Beziehung sind.

Schritte

1. Suchen Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** in der Topologie die Schutzbeziehung, die Sie bearbeiten möchten, und klicken Sie mit der rechten Maustaste darauf.
2. Wählen Sie im Menü **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. Bearbeiten Sie im Dialogfeld „Beziehung bearbeiten“ nach Bedarf die maximale Übertragungsrate, die Schutzrichtlinie oder den Schutzzeitplan.
4. Klicken Sie auf **Übernehmen**.

   Die Änderungen werden auf die ausgewählten Beziehungen angewendet.

Erstellen Sie eine SnapMirror -Richtlinie, um die Übertragungseffizienz zu maximieren

Sie können eine SnapMirror Richtlinie erstellen, um die SnapMirror Übertragungspriorität für Schutzbeziehungen festzulegen. Mithilfe der SnapMirror -Richtlinien können Sie die Übertragungseffizienz von der Quelle zum Ziel maximieren, indem Sie Prioritäten zuweisen, sodass Übertragungen mit niedrigerer Priorität nach Übertragungen mit normaler Priorität ausgeführt werden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

- Diese Aufgabe setzt voraus, dass Sie den Bereich „Zielinformationen“ im Dialogfeld „Schutz konfigurieren“ bereits ausgefüllt haben.

Schritte

1. Klicken Sie auf der Registerkarte * SnapMirror* des Dialogfelds **Schutz konfigurieren** im Bereich **Beziehungseinstellungen** auf den Link **Richtlinie erstellen**.

   Das Dialogfeld „SnapMirror -Richtlinie erstellen“ wird angezeigt.

2. Geben Sie im Feld **Richtlinienname** einen Namen ein, den Sie der Richtlinie geben möchten.
3. Wählen Sie im Feld **Übertragungspriorität** die Übertragungspriorität aus, die Sie der Richtlinie zuweisen möchten.
4. Geben Sie im Feld **Kommentar** einen optionalen Kommentar zur Richtlinie ein.
5. Klicken Sie auf **Erstellen**.

   Die neue Richtlinie wird in der Dropdown-Liste „SnapMirror -Richtlinie“ angezeigt.

Erstellen Sie eine SnapVault -Richtlinie, um die Übertragungseffizienz zu maximieren

Sie können eine neue SnapVault -Richtlinie erstellen, um die Priorität für eine SnapVault Übertragung festzulegen. Sie verwenden Richtlinien, um die Effizienz von Übertragungen vom primären zum sekundären Server in einer Schutzbeziehung zu maximieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.
- Sie müssen den Bereich „Zielinformationen“ im Dialogfeld „Schutz konfigurieren“ bereits ausgefüllt haben.

Schritte

1. Klicken Sie auf der Registerkarte * SnapVault* des Dialogfelds **Schutz konfigurieren** im Bereich **Beziehungseinstellungen** auf den Link **Richtlinie erstellen**.

   Die Registerkarte SnapVault wird angezeigt.

2. Geben Sie im Feld **Richtlinienname** den Namen ein, den Sie der Richtlinie geben möchten.
3. Wählen Sie im Feld **Übertragungspriorität** die Übertragungspriorität aus, die Sie der Richtlinie zuweisen möchten.
4. **Optional:** Geben Sie im Feld **Kommentar** einen Kommentar zur Richtlinie ein.
5. Fügen Sie im Bereich **Replikationsbezeichnung** nach Bedarf eine Replikationsbezeichnung hinzu oder bearbeiten Sie sie.
6. Klicken Sie auf **Erstellen**.

   Die neue Richtlinie wird in der Dropdown-Liste „Richtlinie erstellen“ angezeigt.

Brechen Sie eine aktive Datenschutzübertragung von der Seite „Volume-Beziehungen“ ab

Sie können eine aktive Datensicherungsübertragung abbrechen, wenn Sie eine laufende SnapMirror -Replikation stoppen möchten. Sie können den Neustart-Checkpoint auch für Übertragungen löschen, die auf die Basisübertragung folgen. Sie können eine Übertragung abbrechen, wenn ein Konflikt mit einem anderen Vorgang auftritt, beispielsweise einer Volumeverschiebung.

Sie können Volume-Beziehungen, die durch die Konsistenzgruppe geschützt sind, nicht abbrechen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Die Abbruchaktion wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: zum Beispiel, wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde

Sie können den Neustart-Checkpoint für eine Baseline-Übertragung nicht löschen.

Schritte

1. Um Übertragungen für eine oder mehrere Schutzbeziehungen abzubrechen, wählen Sie auf der Seite **Volume-Beziehungen** ein oder mehrere Volumes aus und klicken Sie in der Symbolleiste auf **Abbrechen**.

   Das Dialogfeld „Übertragung abbrechen“ wird angezeigt.

2. Wenn Sie den Neustart-Checkpoint für eine Übertragung löschen möchten, bei der es sich nicht um eine Basislinienübertragung handelt, wählen Sie **Checkpoints löschen**.
3. Klicken Sie auf **Weiter**.

   Das Dialogfeld „Übertragung abbrechen“ wird geschlossen und der Status des Abbruchauftrags wird oben auf der Seite „Volume-Beziehungen“ zusammen mit einem Link zu den Auftragsdetails angezeigt.

4. **Optional:** Klicken Sie auf den Link **Details anzeigen**, um zur Detailseite des **Auftrags** zu gelangen und dort weitere Einzelheiten zu erfahren und den Auftragsfortschritt anzuzeigen.

Brechen Sie eine aktive Datensicherungsübertragung von der Seite „Volume-/Integritätsdetails“ ab

Sie können eine aktive Datensicherungsübertragung abbrechen, wenn Sie eine laufende SnapMirror -Replikation stoppen möchten. Sie können den Neustart-Checkpoint für eine Übertragung auch löschen, wenn es sich nicht um eine Basislinienübertragung handelt. Sie können eine Übertragung abbrechen, wenn ein Konflikt mit einem anderen Vorgang auftritt, beispielsweise einer Volumeverschiebung.

Sie können Volume-Beziehungen, die durch die Konsistenzgruppe geschützt sind, nicht abbrechen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Die Abbruchaktion wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen: zum Beispiel, wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist: beispielsweise, wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde

Sie können den Neustart-Checkpoint für eine Baseline-Übertragung nicht löschen.

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** mit der rechten Maustaste auf die Beziehung in der Topologieansicht für die Datenübertragung, die Sie abbrechen möchten, und wählen Sie **Abbrechen**.

   Das Dialogfeld „Übertragung abbrechen“ wird angezeigt.

2. Wenn Sie den Neustart-Checkpoint für eine Übertragung löschen möchten, bei der es sich nicht um eine Basislinienübertragung handelt, wählen Sie **Checkpoints löschen**.
3. Klicken Sie auf **Weiter**.

   Das Dialogfeld „Übertragung abbrechen“ wird geschlossen und der Status des Abbruchvorgangs wird oben auf der Seite mit den Datenträger-/Integritätsdetails zusammen mit einem Link zu den Auftragsdetails angezeigt.

4. **Optional:** Klicken Sie auf den Link **Details anzeigen**, um zur Detailseite des **Auftrags** zu gelangen und dort weitere Einzelheiten zu erfahren und den Auftragsfortschritt anzuzeigen.
5. Klicken Sie auf jede Arbeitsaufgabe, um ihre Details anzuzeigen.
6. Klicken Sie in Ihrem Browser auf den Zurück-Pfeil, um zur Detailseite **Volumen/Gesundheit** zurückzukehren.

   Der Abbruchvorgang ist abgeschlossen, wenn alle Jobaufgaben erfolgreich abgeschlossen wurden.

Quiesce einer Schutzbeziehung auf der Seite „Volume-Beziehungen“

Auf der Seite „Volume-Beziehungen“ können Sie eine Schutzbeziehung stilllegen, um Datenübertragungen vorübergehend zu verhindern. Sie können eine Beziehung stilllegen, wenn Sie eine Snapshot-Kopie eines SnapMirror Zielvolumes erstellen möchten, das eine Datenbank enthält, und Sie sicherstellen möchten, dass der Inhalt während des Snapshot-Kopiervorgangs stabil bleibt.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Die Stilllegungsaktion wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist, z. B. wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde
- Wenn Sie Workflow Automation und Unified Manager nicht gekoppelt haben

Schritte

1. Um Übertragungen für eine oder mehrere Schutzbeziehungen stillzulegen, wählen Sie auf der Seite **Volume-Beziehungen** ein oder mehrere Volumes aus und klicken Sie in der Symbolleiste auf **Stilllegen**.

   Das Dialogfeld „Stilllegen“ wird angezeigt.

2. Klicken Sie auf **Weiter**.

   Der Status des Quiesce-Jobs wird oben auf der Seite „Volume-/Integritätsdetails“ zusammen mit einem Link zu den Jobdetails angezeigt.

3. Klicken Sie auf den Link **Details anzeigen**, um zur Detailseite des **Auftrags** zu gelangen und dort weitere Einzelheiten und Informationen zum Auftragsfortschritt anzuzeigen.
4. **Optional:** Klicken Sie in Ihrem Browser auf den Pfeil **Zurück**, um zur Seite **Volumenbeziehungen** zurückzukehren.

   Der Quiesce-Job ist beendet, wenn alle Job-Aufgaben erfolgreich abgeschlossen wurden.

Beenden Sie eine Schutzbeziehung auf der Seite „Volume-/Integritätsdetails“.

Sie können eine Schutzbeziehung stilllegen, um Datenübertragungen vorübergehend zu verhindern. Sie können eine Beziehung stilllegen, wenn Sie eine Snapshot-Kopie eines SnapMirror Zielvolumes erstellen möchten, das eine Datenbank enthält, und Sie sicherstellen möchten, dass der Inhalt während der Snapshot-Kopie stabil bleibt.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Die Stilllegungsaktion wird in den folgenden Fällen nicht angezeigt:

- Wenn die RBAC-Einstellungen diese Aktion nicht zulassen, z. B. wenn Sie nur über Operator-Berechtigungen verfügen
- Wenn die Volume-ID unbekannt ist, z. B. wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde
- Wenn Sie Workflow Automation und Unified Manager nicht gekoppelt haben

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** in der Topologieansicht mit der rechten Maustaste auf die Beziehung für die Schutzbeziehung, die Sie stilllegen möchten.

2. Wählen Sie im Menü „Ruhezustand“ aus.
3. Klicken Sie auf **Ja**, um fortzufahren.

   Der Status des Quiesce-Jobs wird oben auf der Seite „Volume-/Integritätsdetails“ zusammen mit einem Link zu den Jobdetails angezeigt.

4. Klicken Sie auf den Link **Details anzeigen**, um zur Detailseite des **Auftrags** zu gelangen und dort weitere Einzelheiten und Informationen zum Auftragsfortschritt anzuzeigen.
5. **Optional:** Klicken Sie in Ihrem Browser auf den Zurück-Pfeil, um zur Detailseite **Volumen/Gesundheit** zurückzukehren.

   Der Quiesce-Job ist beendet, wenn alle Job-Aufgaben erfolgreich abgeschlossen wurden.

Brechen Sie eine SnapMirror -Beziehung von der Seite „Volume-Beziehungen“ ab

Sie können eine Schutzbeziehung unterbrechen, um Datenübertragungen zwischen einem Quellvolume und einem Zielvolume in einer SnapMirror -Beziehung zu stoppen. Sie können eine Beziehung unterbrechen, wenn Sie Daten migrieren, eine Notfallwiederherstellung durchführen oder Anwendungen testen möchten. Das Zielvolume wird in ein Lese-/Schreibvolume geändert. Sie können eine SnapVault -Beziehung nicht unterbrechen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Schritte

1. Wählen Sie auf der Seite **Volume-Beziehungen** ein oder mehrere Volumes mit Schutzbeziehungen aus, für die Sie die Datenübertragung stoppen möchten, und klicken Sie in der Symbolleiste auf **Unterbrechen**.

   Das Dialogfeld „Beziehung auflösen“ wird angezeigt.

2. Klicken Sie auf **Weiter**, um die Beziehung zu beenden.
3. Überprüfen Sie auf der Seite **Volume-Beziehungen** in der Spalte **Beziehungsstatus**, ob die Beziehung unterbrochen ist.

   Die Spalte „Beziehungsstatus“ ist standardmäßig ausgeblendet. Sie müssen sie daher möglicherweise in der Liste „Spalten anzeigen/ausblenden“ auswählen. .

Entfernen einer Schutzbeziehung von der Seite „Volume-Beziehungen“

Auf der Seite „Volume-Beziehungen“ können Sie eine Schutzbeziehung entfernen, um eine bestehende Beziehung zwischen der ausgewählten Quelle und dem ausgewählten 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

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Schritte

1. Wählen Sie auf der Seite **Volume-Beziehungen** ein oder mehrere Volumes mit Schutzbeziehungen aus, die Sie entfernen möchten, und klicken Sie in der Symbolleiste auf **Entfernen**.

   Das Dialogfeld „Beziehung entfernen“ wird angezeigt.

2. Klicken Sie auf **Weiter**, um die Beziehung zu entfernen.

   Die Beziehung wird von der Seite „Volumenbeziehungen“ entfernt.

Fortsetzen geplanter Übertragungen einer stillgelegten Beziehung über die Seite „Volume-Beziehungen“

Nachdem Sie eine Beziehung stillgelegt haben, um geplante Übertragungen zu verhindern, können Sie mit **Fortsetzen** geplante Übertragungen wieder aktivieren, sodass die Daten auf dem Quell- oder Primärdatenträger geschützt sind. Die Übertragungen werden ab einem Prüfpunkt (sofern vorhanden) beim nächsten geplanten Übertragungsintervall fortgesetzt.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Sie können nicht mehr als 10 stillgelegte Beziehungen auswählen, für die die Übertragungen wieder aufgenommen werden sollen.

Schritte

1. Wählen Sie auf der Seite „Volume-Beziehungen“ ein oder mehrere Volumes mit stillgelegten Beziehungen aus und klicken Sie in der Symbolleiste auf „Fortsetzen“.
2. Klicken Sie im Dialogfeld **Fortsetzen** auf **Weiter**.

   Sie werden zur Seite „Volumenbeziehungen“ zurückgeleitet.

3. Um die zugehörigen Jobaufgaben anzuzeigen und ihren Fortschritt zu verfolgen, klicken Sie auf den Joblink, der oben auf der Seite **Volumenbeziehungen** angezeigt wird.
4. Führen Sie einen der folgenden Schritte aus:
   - Wenn nur ein Job angezeigt wird, klicken Sie auf der Seite „Jobdetails“ auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Schutzkonfigurationsjob verknüpft sind, und um festzustellen, wann der Job abgeschlossen ist.
   - Wenn mehr als ein Job angezeigt wird,
     i. Klicken Sie auf der Seite „Jobs“ auf den Job, dessen Details Sie anzeigen möchten.
     ii. Klicken Sie auf der Seite „Auftragsdetails“ auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails im Zusammenhang mit dem Schutzkonfigurationsauftrag zu aktualisieren und festzustellen, wann der Auftrag abgeschlossen ist. Nach Abschluss der Jobs werden die Datenübertragungen im nächsten geplanten Übertragungsintervall fortgesetzt.

Fortsetzen geplanter Übertragungen in einer stillgelegten Beziehung von der Seite „Volumen-/Gesundheitsdetails“

Nachdem Sie eine Beziehung stillgelegt haben, um geplante Übertragungen zu verhindern, können Sie auf der Seite „Volume-/Integritätsdetails“ mit „**Fortsetzen**“ geplante Übertragungen wieder aktivieren, sodass die Daten auf dem Quell- oder Primärvolume geschützt sind. Die Übertragungen werden ab einem Prüfpunkt (sofern vorhanden) beim nächsten geplanten Übertragungsintervall fortgesetzt.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Schritte

1. Klicken Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** in der Topologieansicht mit der rechten Maustaste auf eine stillgelegte Beziehung, die Sie fortsetzen möchten.

   Alternativ können Sie im Menü **Aktionen** > **Beziehung** die Option **Fortsetzen** auswählen.

2. Klicken Sie im Dialogfeld **Fortsetzen** auf **Weiter**.

   Sie werden zur Seite mit den Volumen-/Gesundheitsdetails zurückgeleitet.

3. Um die zugehörigen Jobaufgaben anzuzeigen und ihren Fortschritt zu verfolgen, klicken Sie auf den Joblink, der oben auf der Detailseite **Volumen/Integrität** angezeigt wird.
4. Klicken Sie auf der Detailseite des **Auftrags** auf **Aktualisieren**, um die Aufgabenliste und die Aufgabendetails zu aktualisieren, die mit dem Schutzkonfigurationsauftrag verknüpft sind, und um festzustellen, wann der Auftrag abgeschlossen ist.

   Nachdem die Aufträge abgeschlossen sind, werden die Datenübertragungen im nächsten geplanten Übertragungsintervall fortgesetzt.

Initialisieren oder aktualisieren Sie Schutzbeziehungen auf der Seite „Volume-Beziehungen“.

Auf der Seite „Volume-Beziehungen“ können Sie eine erstmalige Baseline-Übertragung für eine neue Schutzbeziehung durchführen oder eine Beziehung aktualisieren, wenn sie bereits initialisiert ist und Sie eine manuelle, ungeplante inkrementelle Aktualisierung durchführen möchten, um die Übertragung sofort durchzuführen.

Sie können durch Konsistenzgruppen geschützte Volumes weder initialisieren noch aktualisieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Klicken Sie auf der Seite **Volume-Beziehungen** mit der rechten Maustaste auf ein Volume und wählen Sie

ein oder mehrere Volumes mit Beziehungen aus, die Sie aktualisieren oder initialisieren möchten. Klicken Sie dann in der Symbolleiste auf **Initialisieren/Aktualisieren**.

Das Dialogfeld **Initialisieren/Aktualisieren** wird angezeigt.

2. Wählen Sie auf der Registerkarte **Übertragungsoptionen** eine Übertragungspriorität und die maximale Übertragungsrate aus.
3. Klicken Sie auf **Quell-Snapshot-Kopien** und dann in der Spalte **Snapshot-Kopie** auf **Standard**.

   Das Dialogfeld „Quell-Snapshot-Kopie auswählen“ wird angezeigt.

4. Wenn Sie eine vorhandene Snapshot-Kopie angeben möchten, anstatt die Standard-Snapshot-Kopie zu übertragen, klicken Sie auf **Vorhandene Snapshot-Kopie** und wählen Sie eine Snapshot-Kopie aus der Liste aus.
5. Klicken Sie auf **Senden**.

   Sie werden zum Dialogfeld **Initialisieren/Aktualisieren** zurückgeleitet.

6. Wenn Sie mehr als eine Quelle zum Initialisieren oder Aktualisieren ausgewählt haben, klicken Sie auf **Standard** für die nächste Quelle, für die Sie eine vorhandene Snapshot-Kopie angeben möchten.
7. Klicken Sie auf **Senden**, um den Initialisierungs- oder Aktualisierungsauftrag zu starten.

   Der Initialisierungs- oder Aktualisierungsauftrag wird gestartet, Sie werden zur Seite „Volume-Beziehungen“ zurückgeleitet und oben auf der Seite wird ein Auftragslink angezeigt.

8. **Optional:** Klicken Sie in der Ansicht **Health: All Volumes** auf **View Jobs**, um den Status jedes Initialisierungs- oder Aktualisierungsjobs zu verfolgen.

   Es wird eine gefilterte Liste mit Jobs angezeigt.

9. **Optional:** Klicken Sie auf jeden Job, um seine Details anzuzeigen.
10. **Optional:** Klicken Sie in Ihrem Browser auf den Pfeil **Zurück**, um zur Seite **Volumenbeziehungen** zurückzukehren.

    Der Initialisierungs- oder Aktualisierungsvorgang ist abgeschlossen, wenn alle Aufgaben erfolgreich abgeschlossen wurden.

Initialisieren oder aktualisieren Sie Schutzbeziehungen auf der Seite „Volume-/Integritätsdetails“.

Sie können eine erstmalige Baseline-Übertragung für eine neue Schutzbeziehung durchführen oder eine Beziehung aktualisieren, wenn sie bereits initialisiert ist und Sie eine manuelle, ungeplante inkrementelle Aktualisierung durchführen möchten, um die Daten sofort zu übertragen.

HINWEIS: Sie können durch Konsistenzgruppen geschützte Volumes nicht initialisieren oder aktualisieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die OnCommand Workflow Automation eingerichtet haben.

Schritte

1. Suchen Sie auf der Registerkarte **Schutz** der Detailseite **Volume/Integrität** in der Topologie die Schutzbeziehung, die Sie initialisieren oder aktualisieren möchten, und klicken Sie dann mit der rechten Maustaste darauf.
2. Wählen Sie im Menü **Initialisieren/Aktualisieren**.

   Alternativ können Sie im Menü **Aktionen** die Option **Beziehung** > **Initialisieren/Aktualisieren** auswählen, um die Beziehung zu initialisieren oder zu aktualisieren, deren Details Sie gerade anzeigen.

   Das Dialogfeld „Initialisieren/Aktualisieren“ wird angezeigt.
3. Wählen Sie auf der Registerkarte **Übertragungsoptionen** eine Übertragungspriorität und die maximale Übertragungsrate aus.
4. Klicken Sie auf **Quell-Snapshot-Kopien** und dann in der Spalte **Snapshot-Kopie** auf **Standard**.

   Das Dialogfeld „Quell-Snapshot-Kopie auswählen“ wird angezeigt.
5. Wenn Sie eine vorhandene Snapshot-Kopie angeben möchten, anstatt die Standard-Snapshot-Kopie zu übertragen, klicken Sie auf **Vorhandene Snapshot-Kopie** und wählen Sie eine Snapshot-Kopie aus der Liste aus.
6. Klicken Sie auf **Senden**.

   Sie kehren zum Dialogfeld „Initialisieren/Aktualisieren“ zurück.
7. Wenn Sie mehr als eine Quelle zum Initialisieren oder Aktualisieren ausgewählt haben, klicken Sie auf **Standard** für die nächste Lese-/Schreibquelle, für die Sie eine vorhandene Snapshot-Kopie angeben möchten.

   Sie können für Datenschutzvolumes keine andere Snapshot-Kopie auswählen.
8. Klicken Sie auf **Senden**, um den Initialisierungs- oder Aktualisierungsauftrag zu starten.

   Der Initialisierungs- oder Aktualisierungsauftrag wird gestartet, Sie werden zur Seite mit den Volume-/Integritätsdetails zurückgeleitet und oben auf der Seite wird ein Auftragslink angezeigt.
9. **Optional:** Klicken Sie auf der Detailseite **Volume/Integrität** auf **Jobs anzeigen**, um den Status jedes Initialisierungs- oder Aktualisierungsjobs zu verfolgen.

   Es wird eine gefilterte Liste mit Jobs angezeigt.
10. **Optional:** Klicken Sie auf jeden Job, um seine Details anzuzeigen.
11. **Optional:** Klicken Sie in Ihrem Browser auf den Zurück-Pfeil, um zur Detailseite **Volumen/Gesundheit** zurückzukehren.

    Der Initialisierungs- oder Aktualisierungsvorgang ist abgeschlossen, wenn alle Jobaufgaben erfolgreich abgeschlossen wurden.

Synchronisieren Sie Schutzbeziehungen über die Seite „Volume-Beziehungen“ erneut.

Auf der Seite „Volume-Beziehungen“ können Sie eine Beziehung neu synchronisieren, um sie nach einem Ereignis wiederherzustellen, das Ihr Quellvolume deaktiviert hat, oder

wenn Sie die aktuelle Quelle auf ein anderes Volume ändern möchten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.

Schritte

1. Wählen Sie auf der Seite **Volume-Beziehungen** ein oder mehrere Volumes mit stillgelegten Beziehungen aus und klicken Sie in der Symbolleiste auf **Neu synchronisieren**.

   Das Dialogfeld „Neu synchronisieren“ wird angezeigt.

2. Wählen Sie auf der Registerkarte **Resynchronisierungsoptionen** eine Übertragungspriorität und die maximale Übertragungsrate aus.
3. Klicken Sie auf **Quell-Snapshot-Kopien** und dann in der Spalte **Snapshot-Kopie** auf **Standard**.

   Das Dialogfeld „Quell-Snapshot-Kopie auswählen“ wird angezeigt.

4. Wenn Sie eine vorhandene Snapshot-Kopie angeben möchten, anstatt die Standard-Snapshot-Kopie zu übertragen, klicken Sie auf **Vorhandene Snapshot-Kopie** und wählen Sie eine Snapshot-Kopie aus der Liste aus.
5. Klicken Sie auf **Senden**.

   Sie kehren zum Dialogfeld „Neu synchronisieren“ zurück.

6. Wenn Sie mehr als eine Quelle zur Neusynchronisierung ausgewählt haben, klicken Sie auf **Standard** für die nächste Quelle, für die Sie eine vorhandene Snapshot-Kopie angeben möchten.
7. Klicken Sie auf **Senden**, um den Neusynchronisierungsauftrag zu starten.

   Der Neusynchronisierungsauftrag wird gestartet, Sie werden zur Seite „Volume-Beziehungen“ zurückgeleitet und oben auf der Seite wird ein Auftragslink angezeigt.

8. **Optional:** Klicken Sie auf der Seite **Volume-Beziehungen** auf **Jobs anzeigen**, um den Status jedes Resynchronisierungsjobs zu verfolgen.

   Es wird eine gefilterte Liste mit Jobs angezeigt.

9. **Optional:** Klicken Sie in Ihrem Browser auf den Pfeil **Zurück**, um zur Seite **Volumenbeziehungen** zurückzukehren.

   Der Neusynchronisierungsvorgang ist abgeschlossen, wenn alle Jobaufgaben erfolgreich abgeschlossen wurden.

Umkehren von Schutzbeziehungen auf der Seite „Volume-Beziehungen“

Wenn das Quellvolume in Ihrer Schutzbeziehung durch einen Notfall deaktiviert wird, können Sie das Zielvolume zum Bereitstellen von Daten verwenden, indem Sie es in ein Lese-/Schreibvolume konvertieren, während Sie die Quelle reparieren oder ersetzen. Wenn die Quelle wieder zum Empfangen von Daten verfügbar ist, können Sie den umgekehrten Resynchronisierungsvorgang verwenden, um die Beziehung in umgekehrter Richtung herzustellen und die Daten auf der Quelle mit den Daten auf dem

Lese-/Schreibziel zu synchronisieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die Workflow-Automatisierung eingerichtet haben.
- Bei der Beziehung darf es sich nicht um eine SnapVault -Beziehung handeln.
- Es muss bereits ein Schutzverhältnis bestehen.
- Das Schutzverhältnis muss aufgelöst werden.
- Sowohl die Quelle als auch das Ziel müssen online sein.
- Die Quelle darf nicht das Ziel eines anderen Datensicherungsvolumes sein.
- Wenn Sie diese Aufgabe ausführen, werden Daten auf der Quelle gelöscht, die neuer sind als die Daten auf der gemeinsamen Snapshot-Kopie.
- Für umgekehrte Resynchronisierungsbeziehungen erstellte Richtlinien und Zeitpläne sind dieselben wie für die ursprüngliche Schutzbeziehung.

  Wenn keine Richtlinien und Zeitpläne vorhanden sind, werden sie erstellt.

Schritte

1. Wählen Sie auf der Seite **Volume-Beziehungen** ein oder mehrere Volumes mit Beziehungen aus, die Sie umkehren möchten, und klicken Sie in der Symbolleiste auf **Reverse Resync**.

   Das Dialogfeld „Umgekehrte Neusynchronisierung“ wird angezeigt.

2. Überprüfen Sie, ob die im Dialogfeld **Reverse Resync** angezeigten Beziehungen diejenigen sind, für die Sie den umgekehrten Resynchronisierungsvorgang durchführen möchten, und klicken Sie dann auf **Senden**.

   Der umgekehrte Resynchronisierungsvorgang wird gestartet, Sie werden zur Seite „Volume-Beziehungen“ zurückgeleitet und oben auf der Seite wird ein Job-Link angezeigt.

3. **Optional:** Klicken Sie auf der Seite **Volume-Beziehungen** auf **Jobs anzeigen**, um den Status jedes umgekehrten Resynchronisierungsjobs zu verfolgen.

   Es wird eine gefilterte Liste der mit diesem Vorgang verbundenen Jobs angezeigt.

4. **Optional:** Klicken Sie in Ihrem Browser auf den Pfeil **Zurück**, um zur Seite **Volumenbeziehungen** zurückzukehren.

   Der umgekehrte Resynchronisierungsvorgang ist abgeschlossen, wenn alle Jobaufgaben erfolgreich abgeschlossen wurden.

Wiederherstellen von Daten mithilfe der Detailseiten „Volume“ und „Volume/Integrität“

Sie können überschriebene oder gelöschte Dateien, Verzeichnisse oder ein ganzes Volume aus einer Snapshot-Kopie wiederherstellen, indem Sie die Wiederherstellungsfunktion auf den Detailseiten „Volume“ und „Volume/Integrität“ verwenden.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Beachten Sie die folgenden Punkte:

- Sie können NTFS-Dateistreams nicht wiederherstellen.
- Die Wiederherstellungsoption ist in folgenden Fällen nicht verfügbar:
  - Die Volume-ID ist unbekannt: beispielsweise, wenn Sie eine Intercluster-Beziehung haben und der Zielcluster noch nicht erkannt wurde.
  - Das Volume ist für die synchrone SnapMirror Replikation konfiguriert.

Schritte

1. Gehen Sie im linken Navigationsbereich zu **Speicher > Volumes**.
2. Wählen Sie das Volume aus und klicken Sie auf die Schaltfläche **Wiederherstellen**. Alternativ können Sie auf das Volume klicken, um zu **Volume-/Integritätsdetails > Aktionen > Wiederherstellen** zu gelangen. Das Dialogfeld „Wiederherstellen“ wird angezeigt. Informationen zu dieser Seite finden Sie unter"Dialogfeld „Wiederherstellen“" .
3. Wählen Sie das Volume und die Snapshot-Kopie aus, von denen Sie Daten wiederherstellen möchten, falls diese von der Standardeinstellung abweichen.
4. Wählen Sie die Elemente aus, die Sie wiederherstellen möchten, beispielsweise die Quell-LUN.

   Sie können das gesamte Volume wiederherstellen oder die Ordner und Dateien angeben, die Sie wiederherstellen möchten.
5. Wählen Sie den Speicherort aus, an dem die ausgewählten Elemente wiederhergestellt werden sollen: entweder **Ursprünglicher Speicherort** oder **Alternativer vorhandener Speicherort**.
6. Wenn Sie einen anderen vorhandenen Standort auswählen, führen Sie einen der folgenden Schritte aus:
   - Geben Sie im Textfeld „Pfad wiederherstellen“ den Pfad des Speicherorts ein, an dem Sie die Daten wiederherstellen möchten, und klicken Sie dann auf **Verzeichnis auswählen**.
   - Klicken Sie auf **Durchsuchen**, um das Dialogfeld „Verzeichnisse durchsuchen“ zu öffnen, und führen Sie die folgenden Schritte aus:
     i. Wählen Sie den Zielcluster, die Speicher-VM (SVM) und das Volume aus, auf dem Sie die Wiederherstellung durchführen möchten.
     ii. Wählen Sie in der Namenstabelle einen Verzeichnisnamen aus, der wiederhergestellt werden soll.
     iii. Klicken Sie auf **Verzeichnis auswählen**.
7. Klicken Sie auf **Wiederherstellen**.

   Der Wiederherstellungsprozess beginnt. Um den Wiederherstellungsprozess abzuschließen, wird im Backend ein Job erstellt.
8. Wenn Sie den Auftragsfortschritt anzeigen möchten, navigieren Sie im linken Navigationsbereich zu **Schutz > Aufträge**, um den Status des Wiederherstellungsauftrags aus der Auftragsliste anzuzeigen.

Wenn ein Wiederherstellungsvorgang zwischen Cloud Volumes ONTAP HA-Clustern mit einem NDMP-Fehler fehlschlägt, müssen Sie möglicherweise eine explizite AWS-Route im Zielcluster hinzufügen, damit das Ziel mit dem Cluster-Management-LIF des Quellsystems kommunizieren kann. Sie führen diesen Konfigurationsschritt mithilfe der NetApp Console durch.

Was sind Ressourcenpools

Ressourcenpools sind Gruppen von Aggregaten, die von einem Speicheradministrator mithilfe von Unified Manager erstellt werden, um Partneranwendungen die Bereitstellung für die Sicherungsverwaltung zu ermöglichen.

Sie können Ihre Ressourcen basierend auf Attributen wie Leistung, Kosten, physischem Standort oder Verfügbarkeit bündeln. Durch die Gruppierung verwandter Ressourcen in einem Pool können Sie den Pool für die Überwachung und Bereitstellung als eine einzelne Einheit behandeln. Dies vereinfacht die Verwaltung dieser Ressourcen und ermöglicht eine flexiblere und effizientere Nutzung des Speichers.

Während der Bereitstellung des sekundären Speichers ermittelt Unified Manager anhand der folgenden Kriterien das für den Schutz am besten geeignete Aggregat im Ressourcenpool:

- Das Aggregat ist ein Datenaggregat (kein Stammaggregat) und es ist ONLINE.
- Das Aggregat befindet sich auf einem Zielclusterknoten, dessen ONTAP -Version gleich oder höher als die Hauptversion des Quellclusters ist.
- Das Aggregat verfügt von allen Aggregaten im Ressourcenpool über den größten verfügbaren Speicherplatz.
- Nach der Bereitstellung des Zielvolumes liegt der aggregierte Speicherplatz innerhalb des für das Aggregat definierten Schwellenwerts für „fast voll“ und „fast überbelegt“ (je nachdem, welcher Schwellenwert zutrifft: globaler oder lokaler Schwellenwert).
- Die Anzahl der FlexVol -Volumes auf dem Zielknoten darf das Plattformlimit nicht überschreiten.

Erstellen von Ressourcenpools

Sie können das Dialogfeld „Ressourcenpool erstellen“ verwenden, um Aggregate für Bereitstellungszwecke zu gruppieren.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

Ressourcenpools können Aggregate aus verschiedenen Clustern enthalten, aber dasselbe Aggregat kann nicht zu verschiedenen Ressourcenpools gehören.

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcenpools**.
2. Klicken Sie auf der Seite **Ressourcenpools** auf **Erstellen**.
3. Befolgen Sie die Anweisungen im Dialogfeld **Ressourcenpool erstellen**, um einen Namen und eine Beschreibung anzugeben und Aggregate als Mitglieder zum Ressourcenpool hinzuzufügen, den Sie erstellen möchten.

Ressourcenpools bearbeiten

Sie können einen vorhandenen Ressourcenpool bearbeiten, wenn Sie den Namen und die Beschreibung des Ressourcenpools ändern möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die Schaltfläche **Bearbeiten** ist nur aktiviert, wenn ein Ressourcenpool ausgewählt ist. Wenn mehr als ein Ressourcenpool ausgewählt ist, ist die Schaltfläche **Bearbeiten** deaktiviert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcenpools**.
2. Wählen Sie einen Ressourcenpool aus der Liste aus.
3. Klicken Sie auf **Bearbeiten**.

   Das Fenster „Ressourcenpool bearbeiten“ wird angezeigt.

4. Bearbeiten Sie den Namen und die Beschreibung des Ressourcenpools nach Bedarf.
5. Klicken Sie auf **Speichern**.

   Der neue Name und die neue Beschreibung werden in der Ressourcenpoolliste angezeigt.

Anzeigen des Ressourcenpoolbestands

Auf der Seite „Ressourcenpools“ können Sie den Bestand des Ressourcenpools anzeigen und die verbleibende Kapazität für jeden Ressourcenpool überwachen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritt

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcenpools**.

   Der Bestand des Ressourcenpools wird angezeigt.

Hinzufügen von Ressourcenpoolmitgliedern

Ein Ressourcenpool besteht aus einer Reihe von Mitgliedsaggregaten. Sie können Aggregate zu vorhandenen Ressourcenpools hinzufügen, um den für die Bereitstellung sekundärer Volumes verfügbaren Speicherplatz zu erhöhen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können einem Ressourcenpool nicht mehr als 200 Aggregate gleichzeitig hinzufügen. Im Dialogfeld „Aggregate“ angezeigte Aggregate gehören keinem anderen Ressourcenpool an.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcenpools**.
2. Wählen Sie einen Ressourcenpool aus der Liste **Ressourcenpools** aus.

   Die Mitglieder des Ressourcenpools werden im Bereich unterhalb der Ressourcenpoolliste angezeigt.

3. Klicken Sie im Mitgliederbereich des Ressourcenpools auf **Hinzufügen**.

   Das Dialogfeld „Aggregate“ wird angezeigt.

4. Wählen Sie ein oder mehrere Aggregate aus.
5. Klicken Sie auf **Hinzufügen**.

   Das Dialogfeld wird geschlossen und die Aggregate werden in der Mitgliederliste für den ausgewählten Ressourcenpool angezeigt.

Entfernen von Aggregaten aus Ressourcenpools

Sie können Aggregate aus einem vorhandenen Ressourcenpool entfernen, beispielsweise wenn Sie ein Aggregat für einen anderen Zweck verwenden möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Mitglieder des Ressourcenpools werden nur angezeigt, wenn ein Ressourcenpool ausgewählt ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcenpools**.
2. Wählen Sie den Ressourcenpool aus, aus dem Sie Mitgliedsaggregate entfernen möchten.

   Die Liste der Mitgliedsaggregate wird im Bereich „Mitglieder“ angezeigt.

3. Wählen Sie ein oder mehrere Aggregate aus.

   Die Schaltfläche **Entfernen** ist aktiviert.

4. Klicken Sie auf **Entfernen**.

   Es wird ein Warndialogfeld angezeigt.

5. Klicken Sie auf **Ja**, um fortzufahren.

   Die ausgewählten Aggregate werden aus dem Bereich „Mitglieder“ entfernt.

Ressourcenpools löschen

Sie können Ressourcenpools löschen, wenn sie nicht mehr benötigt werden. Beispielsweise möchten Sie möglicherweise die Mitgliedsaggregate eines Ressourcenpools auf mehrere andere Ressourcenpools umverteilen, wodurch der ursprüngliche Ressourcenpool obsolet wird.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die Schaltfläche **Löschen** ist nur aktiviert, wenn mindestens ein Ressourcenpool ausgewählt ist.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Ressourcenpools**.
2. Wählen Sie den Ressourcenpool aus, den Sie löschen möchten.
3. Klicken Sie auf **Löschen**.

   Der Ressourcenpool wird aus der Ressourcenpoolliste entfernt und seine Aggregate werden aus der Mitgliederliste entfernt.

Überwachen der Schutzbeziehungen für Storage-VM-Disaster-Recovery

Active IQ Unified Manager unterstützt die Überwachung von Disaster-Recovery-Beziehungen zwischen Speicher-VMs und ermöglicht so eine Disaster-Recovery auf der Granularitätsebene einer Speicher-VM. Die Notfallwiederherstellung der Speicher-VM ermöglicht die Wiederherstellung der in den einzelnen Volumes der Speicher-VM vorhandenen Daten und die Wiederherstellung der Speicher-VM-Konfiguration.

Um eine asynchrone Notfallwiederherstellung zu ermöglichen, wird eine Speicher-VM-DR-Beziehung von der Quell-Speicher-VM zur Ziel-Speicher-VM erstellt. Sie können auswählen, ob die gesamte oder eine Teilmenge der Speicher-VM-Konfiguration (ohne Netzwerk- und Protokollkonfiguration) zusammen mit den Datenvolumes basierend auf der Cluster-Einrichtung repliziert werden soll.

Nachdem die Disaster-Recovery-Beziehung der Speicher-VM konfiguriert wurde und die Quell-Speicher-VM aufgrund eines Hardwarefehlers oder einer Umweltkatastrophe nicht mehr verfügbar ist, wird die Ziel-Speicher-VM gestartet, die den Datenzugriff mit der geringsten Unterbrechung ermöglicht. Wenn die Quellspeicher-VM verfügbar wird, wird sie auf ähnliche Weise mit der Zielspeicher-VM neu synchronisiert. Anschließend wird die Quelle neu gestartet, um Daten bereitzustellen. Sie können SnapMirror -Befehle verwenden, um die Disaster-Recovery-Beziehung zwischen Speicher-VMs zu konfigurieren und zu verwalten.

Überwachen von Speicher-VMs mithilfe der Seite „Beziehungen“

Sie können die Disaster-Recovery-Beziehungen Ihrer Storage-VMs auf der Seite „Beziehungen“ im Abschnitt „SCHUTZ“ des Inventars überwachen. Standardmäßig werden auf der Seite „Beziehungen“ nur die Beziehungen der obersten Ebene aufgelistet, da der Filter für die Beziehungen der Bestandteile angewendet wird.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie verwenden Filter, um die Disaster-Recovery-Beziehungen der Speicher-VM anzuzeigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **SCHUTZ** > **Beziehungen**.

   Auf der Seite werden alle Beziehungstypen angezeigt: Volume-, Konsistenzgruppen- und Speicher-VM-Beziehungen.

2. Klicken Sie auf **Filter** und wählen Sie dann **Beziehungsobjekttyp** und **Speicher-VM** aus, um nur die Beziehungen zur Notfallwiederherstellung von Speicher-VMs anzuzeigen.
3. Klicken Sie auf **Filter anwenden**.

> Sie sollten den Filter für die Bestandteilbeziehungen löschen, um alle Schutzbeziehungen anzuzeigen.

Auf der Seite werden nur Speicher-VM-Notfallwiederherstellungsbeziehungen angezeigt.

Schutzbeziehungen auf der Seite „Speicher-VMs“ anzeigen

Auf der Seite „Storage-VMs“ können Sie den Status der Disaster-Recovery-Beziehungen vorhandener Storage-VMs anzeigen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können auch Details der Schutzbeziehungen prüfen, einschließlich Übertragungs- und Verzögerungsstatus sowie Quell- und Zieldetails. Sie können Berichte planen oder vorhandene Berichte im gewünschten Format herunterladen. Mit der Schaltfläche **Anzeigen/Ausblenden** können Sie den Berichten die erforderlichen Spalten hinzufügen, da diese standardmäßig nicht angezeigt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **STORAGE** > **Storage-VMs**.
2. Wählen Sie im Menü **ANSICHT** die Option **Beziehung** > **Alle Beziehungen**.

   Die Ansicht „Beziehung: Alle Beziehungen“ wird mit allen konfigurierten Speicher-VMs angezeigt.

Anzeigen von Speicher-VMs basierend auf dem Schutzstatus

Sie können die Seite „Speicher-VMs“ des Inventars verwenden, um alle Speicher-VMs in Active IQ Unified Manager anzuzeigen und die Speicher-VMs basierend auf ihrem Schutzstatus zu filtern.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Der Ansicht „Speicher-VMs“ wurde eine neue Spalte „Schutzrolle“ hinzugefügt, die Informationen darüber bereitstellt, ob die Speicher-VM geschützt oder ungeschützt ist.

> Wenn ein Quellcluster nicht zu Active IQ Unified Manager hinzugefügt wird, sind alle Informationen zu diesem Cluster in den Rastern nicht verfügbar.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **STORAGE** > **Storage-VMs**.
2. Wählen Sie im Menü **ANSICHT** die Option **Integrität** > **Alle Speicher-VMs**.

   Der Zustand: Alle Speicher-VMs wird angezeigt.

3. Klicken Sie auf **Filter**, um eine der folgenden Speicher-VMs anzuzeigen.

Zum Ansehen	Filterwert
Geschützte Speicher-VMs	**Schutzrolle** ist **Geschützt**
Ungeschützte Speicher-VMs	**Schutzrolle** ist **Ungeschützt**

> Sie können die geschützten und ungeschützten Speicher-VMs nicht gleichzeitig anzeigen. Sie müssen den vorhandenen Filter löschen, um eine neue Filteroption erneut anzuwenden.

4. Klicken Sie auf **Filter anwenden**.

   In der Ansicht „Nicht gespeichert“ werden alle Speicher-VMs angezeigt, die je nach Ihren Filterauswahlen durch die Notfallwiederherstellung der Speicher-VM entweder geschützt oder ungeschützt sind.

Grundlegendes zu Storage-VM-Zuordnungen

Bei Zuordnungen virtueller Speichermaschinen (Storage-VMs) handelt es sich um Zuordnungen von einer Quell-Storage-VM zu einer Ziel-Storage-VM, die von Partneranwendungen zur Ressourcenauswahl und Bereitstellung sekundärer Volumes verwendet werden.

Es werden Verknüpfungen zwischen einer Quell-Speicher-VM und einer Ziel-Speicher-VM erstellt, unabhängig davon, ob es sich bei der Ziel-Speicher-VM um ein sekundäres oder ein tertiäres Ziel handelt. Sie können keine sekundäre Zielspeicher-VM als Quelle verwenden, um eine Zuordnung zu einer tertiären Zielspeicher-VM herzustellen.

Als Anwendungsadministrator oder Speicheradministrator können Sie die Speicher-VM-Zuordnungen in Ihrer Umgebung auf der Seite **Schutz** > **Speicher-VM-Zuordnungen** anzeigen.

Sie können SVMs auf drei Arten zuordnen:

- **Beliebige Speicher-VM zuordnen**: Sie können eine Zuordnung zwischen jeder primären Quell-Speicher-VM und einer oder mehreren Ziel-SVMs erstellen. Dies bedeutet, dass alle vorhandenen SVMs, die derzeit Schutz benötigen, sowie alle SVMs, die in Zukunft erstellt werden, mit den angegebenen Ziel-SVMs verknüpft werden. Beispielsweise möchten Sie möglicherweise Anwendungen aus mehreren unterschiedlichen Quellen an unterschiedlichen Standorten auf einer oder mehreren Ziel-SVMs an einem Standort sichern.
- **Eine bestimmte Speicher-VM zuordnen**: Sie können eine Zuordnung zwischen einer bestimmten Quell-Speicher-VM und einer oder mehreren bestimmten Ziel-SVMs erstellen. Wenn Sie beispielsweise Speicherdienste für viele Clients bereitstellen, deren Daten voneinander getrennt sein müssen, können Sie diese Option wählen, um eine bestimmte Quellspeicher-VM einer bestimmten Zielspeicher-VM zuzuordnen, die nur diesem Client zugewiesen ist.
- **Mit einer externen Speicher-VM verknüpfen**: Sie können eine Verknüpfung zwischen einer Quellspeicher-VM und einem externen flexiblen Volume einer Zielspeicher-VM erstellen.

Erstellen von Speicher-VM-Zuordnungen

Der Assistent „Zuordnungen virtueller Speichermaschinen erstellen“ ermöglicht Partnerschutzanwendungen,

eine Quellspeicher-VM mit einer Zielspeicher-VM zur Verwendung mit SnapMirror und SnapVault -Beziehungen zu verknüpfen. Partneranwendungen verwenden diese Zuordnungen zum Zeitpunkt der ersten Bereitstellung von Zielvolumes, um zu bestimmen, welche Ressourcen ausgewählt werden sollen.dd

Bevor Sie beginnen

- Die Speicher-VM, die Sie zuordnen, muss bereits vorhanden sein.
- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Für jede Quellspeicher-VM und jeden Beziehungstyp können Sie auf jedem Zielcluster nur eine Zielspeicher-VM auswählen.

Das Ändern von Zuordnungen mithilfe der Lösch- und Erstellungsfunktionen wirkt sich nur auf zukünftige Bereitstellungsvorgänge aus. Vorhandene Zielvolumes werden nicht verschoben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Speicher-VM-Zuordnungen**.
2. Klicken Sie auf der Seite **Storage-VM-Zuordnungen** auf **Erstellen**.

   Der Assistent **Zuordnungen virtueller Speichermaschinen erstellen** wird gestartet.

3. Wählen Sie eine der folgenden Quellen:
   - **Beliebig**

     Wählen Sie diese Option, wenn Sie eine Verknüpfung zwischen einer beliebigen primären Speicher-VM-Quelle und einer oder mehreren Ziel-Speicher-VMs erstellen möchten. Dies bedeutet, dass alle vorhandenen Speicher-VMs, die derzeit geschützt werden müssen, sowie alle Speicher-VMs, die in Zukunft erstellt werden, mit der angegebenen Ziel-Speicher-VM verknüpft werden. Beispielsweise möchten Sie möglicherweise Anwendungen aus mehreren unterschiedlichen Quellen an unterschiedlichen Standorten auf einer oder mehreren Zielspeicher-VMs an einem Standort sichern.

   - **Einzel**

     Wählen Sie diese Option, wenn Sie eine bestimmte Quell-Speicher-VM auswählen möchten, die mit einer oder mehreren Ziel-Speicher-VMs verknüpft ist. Wenn Sie beispielsweise Speicherdienste für viele Clients bereitstellen, deren Daten voneinander getrennt sein müssen, wählen Sie diese Option, um eine bestimmte Speicher-VM-Quelle einem bestimmten Speicher-VM-Ziel zuzuordnen, das nur diesem Client zugewiesen ist.

   - **Keine (Extern)**

     Wählen Sie diese Option, wenn Sie eine Zuordnung zwischen einer Quellspeicher-VM und einem externen flexiblen Volume einer Zielspeicher-VM erstellen möchten.

4. Wählen Sie einen oder beide Schutzbeziehungstypen aus, die Sie erstellen möchten:
   - * SnapMirror*
   - * SnapVault*
5. Klicken Sie auf **Weiter**.
6. Wählen Sie ein oder mehrere Speicher-VM-Schutzziele aus.
7. Klicken Sie auf **Fertig**.

Speicher-VM-Zuordnungen löschen

Sie können Speicher-VM-Zuordnungen für Partneranwendungen löschen, um die sekundäre Bereitstellungsbeziehung zwischen Quell- und Ziel-Speicher-VM zu entfernen. Dies können Sie beispielsweise tun, wenn die Ziel-Speicher-VM voll ist und Sie neue Speicher-VM-Schutzzuordnungen erstellen möchten.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Die Schaltfläche **Löschen** ist deaktiviert, bis mindestens eine Speicher-VM-Zuordnung ausgewählt ist. Das Ändern von Zuordnungen mithilfe der Lösch- und Erstellungsfunktionen wirkt sich nur auf zukünftige Bereitstellungsvorgänge aus; vorhandene Zielvolumes werden dadurch nicht verschoben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Speicher-VM-Zuordnungen**.
2. Wählen Sie mindestens eine Speicher-VM-Zuordnung aus.

   Die Schaltfläche **Löschen** ist aktiviert.

3. Klicken Sie auf **Löschen**.

   Es wird ein Warndialogfeld angezeigt.

4. Klicken Sie auf **Ja**, um fortzufahren.

   Die ausgewählte Speicher-VM-Zuordnung wird aus der Liste entfernt.

SVM- und Ressourcenpoolanforderungen zur Unterstützung von Speicherdiensten

Sie können die Konformität in Partneranwendungen besser sicherstellen, wenn Sie einige SVM-Zuordnungs- und Ressourcenpoolanforderungen beachten, die spezifisch für Speicherdienste sind: beispielsweise, wenn Sie SVM zuordnen und Ressourcenpools in Unified Manager erstellen, um eine Schutztopologie in einem von einer Partneranwendung bereitgestellten Speicherdienst zu unterstützen.

Einige Anwendungen arbeiten mit dem Unified Manager-Server zusammen, um Dienste bereitzustellen, die den SnapMirror oder SnapVault -Backup-Schutz zwischen Quellvolumes und Schutzvolumes an sekundären oder tertiären Standorten automatisch konfigurieren und ausführen. Um diese Schutzspeicherdienste zu unterstützen, müssen Sie Unified Manager verwenden, um die erforderlichen SVM-Zuordnungen und Ressourcenpools zu konfigurieren.

Um den Single-Hop- oder kaskadierten Schutz des Speicherdienstes zu unterstützen, einschließlich der Replikation von einer SnapMirror Quelle oder einem SnapVault Primärvolume entweder zum Ziel SnapMirror oder zu SnapVault -Sicherungsvolumes, die sich an sekundären oder tertiären Standorten befinden, müssen Sie die folgenden Anforderungen beachten:

- SVM-Zuordnungen müssen zwischen dem SVM, das die SnapMirror Quelle oder das SnapVault Primärvolume enthält, und jedem SVM konfiguriert werden, auf dem sich entweder ein Sekundärvolume oder ein Tertiärvolume befindet.
  - Um beispielsweise eine Schutztopologie zu unterstützen, in der sich das Quellvolume Vol_A auf SVM_1, das sekundäre SnapMirror -Zielvolume Vol_B auf SVM_2 und das tertiäre SnapVault Sicherungsvolume Vol_C auf SVM_3 befindet, müssen Sie die Unified Manager-Web-

Benutzeroberfläche verwenden, um eine SnapMirror Zuordnung zwischen SVM_1 und SVM_2 und eine SnapVault -Sicherungszuordnung zwischen SVM_1 und SVM_3 zu konfigurieren.

In diesem Beispiel ist keine SnapMirror Zuordnung oder SnapVault -Sicherungszuordnung zwischen SVM_2 und SVM_3 erforderlich und wird nicht verwendet.

- Um eine Schutztopologie zu unterstützen, in 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 Cluster-Aggregatressourcen enthalten, die den zugehörigen SVMs zur Verfügung stehen.

  Sie konfigurieren Ressourcenpools über die Web-Benutzeroberfläche von Unified Manager und weisen dann über die Partneranwendung die sekundären Ziel- und tertiären Zielknoten des Speicherdienstes zu.

Welche Jobs sind

Ein Job ist eine Reihe von Aufgaben, die Sie mit Unified Manager überwachen können. Durch die Anzeige von Aufträgen und den zugehörigen Aufgaben können Sie feststellen, ob diese erfolgreich abgeschlossen wurden.

Jobs werden initiiert, wenn Sie SnapMirror und SnapVault -Beziehungen erstellen, wenn Sie Beziehungsvorgänge ausführen (Unterbrechen, Bearbeiten, Stilllegen, Entfernen, Fortsetzen, Neusynchronisieren und umgekehrte Neusynchronisierung), wenn Sie Datenwiederherstellungsaufgaben ausführen, wenn Sie sich bei einem Cluster anmelden usw.

Wenn Sie einen Job initiieren, können Sie die Seite „Jobs“ und die Seite „Jobdetails“ verwenden, um den Job und den Fortschritt der zugehörigen Jobaufgaben zu überwachen.

Überwachen von Jobs

Auf der Seite „Jobs“ können Sie den Jobstatus überwachen und Jobeigenschaften wie Speicherdiensttyp, Status, Übermittlungszeit und Abschlusszeit anzeigen, um festzustellen, ob ein Job erfolgreich abgeschlossen wurde oder nicht.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Jobs**.

   Die Seite „Jobs“ wird angezeigt.

2. Sehen Sie sich die Spalte **Status** an, um den Status der aktuell ausgeführten Jobs zu ermitteln.
3. Klicken Sie auf einen Jobnamen, um Details zu diesem bestimmten Job anzuzeigen.

   Die Seite mit den Auftragsdetails wird angezeigt.

Jobdetails anzeigen

Nachdem Sie einen Auftrag gestartet haben, können Sie seinen Fortschritt auf der Seite „Auftragsdetails“ verfolgen und die zugehörigen Aufgaben auf mögliche Fehler überwachen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Jobs**.
2. Klicken Sie auf der Seite „Jobs“ in der Spalte „Name“ auf einen Jobnamen, um die Liste der mit dem Job verknüpften Aufgaben anzuzeigen.
3. Klicken Sie auf eine Aufgabe, um zusätzliche Informationen im Bereich **Aufgabendetails** und im Bereich **Aufgabennachrichten** rechts neben der Aufgabenliste anzuzeigen.

Jobs abbrechen

Auf der Seite „Jobs“ können Sie einen Job abbrechen, wenn seine Fertigstellung zu lange dauert, zu viele Fehler auftreten oder er nicht mehr benötigt wird. Sie können einen Job nur abbrechen, wenn sein Status und Typ dies zulassen. Sie können jeden laufenden Job abbrechen.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Jobs**.
2. Wählen Sie aus der Jobliste einen Job aus und klicken Sie dann auf **Abbrechen**.
3. Klicken Sie in der Bestätigungsaufforderung auf **Ja**, um den ausgewählten Auftrag abzubrechen.

Wiederholen Sie einen fehlgeschlagenen Schutzauftrag

Nachdem Sie Maßnahmen zum Beheben eines fehlgeschlagenen Schutzauftrags ergriffen haben, können Sie den Auftrag mit **Wiederholen** erneut ausführen. Durch die Wiederholung eines Auftrags wird ein neuer Auftrag mit der ursprünglichen Auftrags-ID erstellt.

Bevor Sie beginnen

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können jeweils nur einen fehlgeschlagenen Auftrag wiederholen. Wenn Sie mehr als einen Job auswählen, wird die Schaltfläche **Wiederholen** deaktiviert. Nur Jobs vom Typ „Schutzkonfiguration“ und „Schutzbeziehungsvorgang“ können wiederholt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Schutz** > **Jobs**.
2. Wählen Sie aus der Jobliste einen einzelnen fehlgeschlagenen Job vom Typ „Schutzkonfiguration“ oder

„Schutzbeziehungsvorgang“ aus.

Die Schaltfläche **Wiederholen** ist aktiviert.

3. Klicken Sie auf **Wiederholen**.

Der Job wird neu gestartet.

Beschreibung der Fenster und Dialogfelder zu Schutzbeziehungen

Sie können schutzbezogene Details wie Ressourcenpools, SVM-Zuordnungen und Schutzaufträge anzeigen und verwalten. Sie können die entsprechende Seite „Integritätsschwellenwerte“ verwenden, um globale Integritätsschwellenwerte für Aggregate, Volumes und Beziehungen zu konfigurieren.

Seite „Ressourcenpools“

Auf der Seite „Ressourcenpools“ werden vorhandene Ressourcenpools und ihre Mitglieder angezeigt. Außerdem können Sie Ressourcenpools zu Bereitstellungszwecken erstellen, überwachen und verwalten.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Erstellen**

  Öffnet das Dialogfeld „Ressourcenpool erstellen“, in dem Sie Ressourcenpools erstellen können.

- **Bearbeiten**

  Ermöglicht Ihnen, den Namen und die Beschreibung der von Ihnen erstellten Ressourcenpools zu bearbeiten.

- **Löschen**

  Ermöglicht Ihnen, einen oder mehrere Ressourcenpools zu löschen.

Liste der Ressourcenpools

In der Liste „Ressourcenpools“ werden (in tabellarischer Form) die Eigenschaften vorhandener Ressourcenpools angezeigt.

- **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 Aggregate nur eines SnapLock -Typs enthalten.

- **Gesamtkapazität**

  Zeigt die Gesamtkapazität (in MB, GB usw.) des Ressourcenpools an.

- **Genutzte Kapazität**

  Zeigt die Menge an Speicherplatz (in MB, GB usw.) an, die im Ressourcenpool verwendet wird.

- **Verfügbare Kapazität**

  Zeigt die Menge an Speicherplatz (in MB, GB usw.) an, die im Ressourcenpool verfügbar ist.

- **Gebraucht %**

  Zeigt den Prozentsatz des im Ressourcenpool verwendeten Speicherplatzes an.

Befehlsschaltflächen für die Mitgliederliste

Mit den Befehlsschaltflächen der Mitgliederliste können Sie die folgenden Aufgaben ausführen:

- **Hinzufügen**

  Ermöglicht Ihnen, Mitglieder zum Ressourcenpool hinzuzufügen.

- **Löschen**

  Ermöglicht Ihnen, ein oder mehrere Mitglieder aus dem Ressourcenpool zu löschen.

Mitgliederliste

Die Mitgliederliste zeigt (in Tabellenform) die Mitglieder des Ressourcenpools und ihre Eigenschaften an, wenn ein Ressourcenpool ausgewählt wird.

- **Status**

  Zeigt den aktuellen Status des Mitgliedsaggregats an. Der Status kann „Kritisch“ ( ), Fehler ( ), Warnung ( ) oder Normal ( ).

- **Aggregatname**

  Zeigt den Namen des Mitgliedsaggregats an.

- **Zustand**

  Zeigt den aktuellen Status des Aggregats an, der einer der folgenden sein kann:

  - Offline

    Lese- oder Schreibzugriff ist nicht zulässig.

  - Online

Lese- und Schreibzugriff auf die Volumes, die auf diesem Aggregat gehostet werden, ist zulässig.

- Eingeschränkt

  Eingeschränkte Vorgänge (wie etwa die Rekonstruktion der Parität) sind zulässig, der Datenzugriff ist jedoch nicht gestattet.

- 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.

- Eisenbeschränkt

  Auf dem Aggregat können keine Diagnosetools ausgeführt werden.

- Montage

  Das Aggregat befindet sich im Montageprozess.

- Teilweise

  Für das Aggregat wurde mindestens eine Festplatte gefunden, es fehlen jedoch zwei oder mehr Festplatten.

- Stilllegung

  Das Aggregat wird stillgelegt.

- Ruhezustand

  Das Aggregat wird in den Ruhezustand versetzt.

- Zurückgesetzt

  Die Rückgängigmachung eines Aggregats ist abgeschlossen.

- Unmontiert

  Das Aggregat wurde demontiert.

- Aushängen

  Das Aggregat wird offline genommen.

- Unbekannt

  Das Aggregat wurde erkannt, aber die Aggregatinformationen wurden noch nicht vom Unified Manager-Server abgerufen.

Standardmäßig ist diese Spalte 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 Menge an Speicherplatz (in MB, GB usw.) an, die im Aggregat verwendet wird.

- **Verfügbare Kapazität**

  Zeigt die Menge an Speicherplatz (in MB, GB usw.) an, die im Aggregat verfügbar ist.

- **Gebraucht %**

  Zeigt den Prozentsatz des Speicherplatzes an, der im Aggregat verwendet wird.

- **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). Standardmäßig ist diese Spalte ausgeblendet.

Dialogfeld „Ressourcenpool erstellen“

Sie können das Dialogfeld „Ressourcenpool erstellen“ verwenden, um einen neuen Ressourcenpool zu benennen und zu beschreiben und um Aggregate zu diesem Ressourcenpool hinzuzufügen und aus diesem zu löschen.

Name des Ressourcenpools

In den Textfeldern können Sie die folgenden Informationen hinzufügen, um einen Ressourcenpool zu erstellen:

Ermöglicht Ihnen, einen Ressourcenpoolnamen anzugeben.

Beschreibung

Ermöglicht Ihnen, einen Ressourcenpool zu beschreiben.

Mitglieder

Zeigt die Mitglieder des Ressourcenpools an. Sie können auch Mitglieder hinzufügen und löschen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden 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, aber dieselben Aggregate können nicht zu mehr als einem Ressourcenpool hinzugefügt werden.

- **Entfernen**

  Ermöglicht Ihnen, ausgewählte Aggregate aus dem Ressourcenpool zu entfernen.

- **Erstellen**

  Erstellt den Ressourcenpool. Diese Schaltfläche wird erst aktiviert, wenn in den Feldern „Name des Ressourcenpools“ oder „Beschreibung“ Informationen eingegeben wurden.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld „Ressourcenpool erstellen“.

Dialogfeld „Ressourcenpool bearbeiten“

Sie können das Dialogfeld „Ressourcenpool bearbeiten“ verwenden, um den Namen und die Beschreibung eines vorhandenen Ressourcenpools zu ändern. Wenn beispielsweise der ursprüngliche Name und die Beschreibung ungenau oder falsch sind, können Sie sie ändern, sodass sie präziser sind.

Textfelder

Über die Textfelder können Sie die folgenden Informationen für den ausgewählten Ressourcenpool ändern:

- **Name des Ressourcenpools**

  Ermöglicht Ihnen, einen neuen Namen einzugeben.

- **Beschreibung**

  Ermöglicht Ihnen, eine neue Beschreibung einzugeben.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Speichern**

  Speichert die Änderungen am Namen und der Beschreibung des Ressourcenpools.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld „Ressourcenpool bearbeiten“.

Dialogfeld „Aggregate“

Sie können das Dialogfeld „Aggregate“ verwenden, um die Aggregate auszuwählen, die Sie Ihrem Ressourcenpool hinzufügen möchten.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Hinzufügen**

  Fügt die ausgewählten Aggregate zum Ressourcenpool hinzu. Die Schaltfläche „Hinzufügen“ wird erst aktiviert, wenn mindestens ein Aggregat ausgewählt ist.

- **Stornieren**

  Verwirft die Änderungen und schließt das Dialogfeld „Aggregate“.

Aggregatliste

Die Liste „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 ( ).

  Sie können den Zeiger über den Status bewegen, um weitere Informationen zu dem oder den für das Volume generierten Ereignissen anzuzeigen.

- **Aggregatname**

  Zeigt den Namen des Aggregats an.

- **Zustand**

  Zeigt den aktuellen Status des Aggregats an, der einer der folgenden sein kann:

  - Offline

    Lese- oder Schreibzugriff ist nicht zulässig.

  - Eingeschränkt

Eingeschränkte Vorgänge (wie etwa die Rekonstruktion der Parität) sind zulässig, der Datenzugriff ist jedoch nicht gestattet.

- 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.

- Eisenbeschränkt

  Auf dem Aggregat können keine Diagnosetools ausgeführt werden.

- Montage

  Das Aggregat befindet sich im Montageprozess.

- Teilweise

  Für das Aggregat wurde mindestens eine Festplatte gefunden, es fehlen jedoch zwei oder mehr Festplatten.

- Stilllegung

  Das Aggregat wird stillgelegt.

- Ruhezustand

  Das Aggregat wird in den Ruhezustand versetzt.

- Zurückgesetzt

  Die Rückgängigmachung eines Aggregats ist abgeschlossen.

- Unmontiert

  Das Aggregat ist offline.

◦ Aushängen

Das Aggregat wird offline genommen.

◦ Unbekannt

Das Aggregat wurde erkannt, aber die Aggregatinformationen wurden 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 Speichercontrollers an, der das Aggregat enthält.

- **Gesamtkapazität**

  Zeigt die Gesamtdatengröße (in MB, GB usw.) des Aggregats an. Standardmäßig ist diese Spalte ausgeblendet.

- **Verpflichtete Kapazität**

  Zeigt den gesamten Speicherplatz (in MB, GB usw.) an, der für alle Volumes im Aggregat reserviert ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Genutzte Kapazität**

  Zeigt die Menge an Speicherplatz (in MB, GB usw.) an, die im Aggregat verwendet wird.

- **Verfügbare Kapazität**

  Zeigt die Menge an Speicherplatz (in MB, GB usw.) an, die für Daten im Aggregat verfügbar ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Verfügbar %**

  Zeigt den Prozentsatz des Speicherplatzes an, der für Daten im Aggregat verfügbar ist. Standardmäßig ist diese Spalte ausgeblendet.

- **Gebraucht %**

  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.

Seite „Jobs“

Auf der Seite „Jobs“ können Sie den aktuellen Status und andere Informationen zu allen derzeit laufenden und abgeschlossenen Jobs zum Schutz von Partneranwendungen anzeigen. Anhand dieser Informationen können Sie erkennen, welche Jobs noch laufen

und ob ein Job erfolgreich war oder fehlgeschlagen ist.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Abbrechen**

  Bricht den ausgewählten Job ab. Diese Option ist nur verfügbar, wenn der ausgewählte Job ausgeführt wird.

- **Wiederholen**

  Startet einen fehlgeschlagenen Job vom Typ „Schutzkonfiguration“ oder „Schutzbeziehungsvorgang“ neu. Sie können jeweils nur einen fehlgeschlagenen Auftrag wiederholen. Wenn mehr als ein fehlgeschlagener Job ausgewählt ist, ist die Schaltfläche **Wiederholen** deaktiviert. Sie können fehlgeschlagene Speicherdienstaufträge nicht wiederholen.

- **Aktualisieren**

  Aktualisiert die Liste der Jobs und die damit verbundenen Informationen.

Stellenliste

Die Jobliste zeigt in tabellarischer Form eine Liste der laufenden Jobs an. Standardmäßig zeigt die Liste nur die Jobs an, die in der letzten Woche generiert wurden. Sie können die Spaltensortierung und -filterung verwenden, um anzupassen, welche Jobs angezeigt werden.

- **Status**

  Zeigt den aktuellen Status eines Auftrags an. Der Status kann Fehler (❗) oder Normal (✅).

- **Job-ID**

  Zeigt die Identifikationsnummer des Auftrags an. Standardmäßig ist diese Spalte ausgeblendet.

  Die Job-Identifikationsnummer ist eindeutig und wird vom Server beim Start des Jobs zugewiesen. 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 Auftragstyp an. Die Jobtypen sind wie folgt:

  - **Cluster-Akquisition**

    Ein Workflow-Automatisierungsjob erkennt einen Cluster neu.

  - **Schutzkonfiguration**

    Ein Schutzauftrag initiiert Workflow-Automatisierungs-Workflows, wie etwa Cron-Zeitpläne, SnapMirror

-Richtlinienerstellung usw.

- **Schutzbeziehungsoperation**

  Ein Schutzauftrag führt SnapMirror -Vorgänge aus.

- **Schutz-Workflow-Kette**

  Ein Workflow-Automatisierungsjob führt mehrere Workflows aus.

- **Wiederherstellen**

  Ein Wiederherstellungsauftrag wird ausgeführt.

- **Aufräumen**

  Die Aufgabe besteht darin, Artefakte von Speicherdienstmitgliedern zu bereinigen, die für Wiederherstellungszwecke nicht mehr benötigt werden.

- **Konform**

  Die Aufgabe besteht darin, die Konfiguration der Speicherdienstmitglieder zu überprüfen, um sicherzustellen, dass sie konform sind.

- **Zerstören**

  Der Job zerstört einen Speicherdienst.

- **Import**

  Der Job importiert nicht verwaltete Speicherobjekte in einen vorhandenen Speicherdienst.

- **Ändern**

  Der Job besteht darin, Attribute eines vorhandenen Speicherdienstes zu ändern.

- **Abonnieren**

  Der Job besteht darin, Mitglieder für einen Speicherdienst anzumelden.

- **Abbestellen**

  Der Job besteht darin, Mitglieder von einem Speicherdienst abzumelden.

- **Aktualisieren**

  Ein Schutzaktualisierungsauftrag wird ausgeführt.

- **WFA-Konfiguration**

  Ein Workflow-Automatisierungsjob überträgt Cluster-Anmeldeinformationen und synchronisiert Datenbank-Caches.

- **Zustand**

Zeigt den Ausführungsstatus des Auftrags an. Die Statusoptionen lauten wie folgt:

- **Abgebrochen**

  Der Auftrag wurde abgebrochen.

- **Abbruch**

  Der Job wird gerade abgebrochen.

- **Vollendet**

  Der Auftrag ist abgeschlossen.

- **Läuft**

  Der Job wird ausgeführt.

- **Eingereichte Zeit**

  Zeigt die Uhrzeit an, zu der der Auftrag übermittelt wurde.

- **Dauer**

  Zeigt die Zeit an, die für die Ausführung des Auftrags benötigt wurde. Diese Spalte wird standardmäßig angezeigt.

- **Abgeschlossene Zeit**

  Zeigt die Zeit an, zu der der Auftrag beendet wurde. Standardmäßig ist diese Spalte ausgeblendet.

Seite mit den Auftragsdetails

Auf der Seite „Auftragsdetails“ können Sie den Status und andere Informationen zu bestimmten Schutzauftragsaufgaben anzeigen, die ausgeführt werden, sich in der Warteschlange befinden oder abgeschlossen sind. Sie können diese Informationen verwenden, um den Fortschritt von Schutzaufträgen zu überwachen und Auftragsfehler zu beheben.

Jobübersicht

In der Auftragszusammenfassung werden die folgenden Informationen angezeigt:

- Auftrags-ID
- Typ
- Status
- Eingereichte Zeit
- Abgeschlossene Zeit
- Dauer

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Aktualisieren**

  Aktualisiert die Aufgabenliste und die mit jeder Aufgabe verknüpften Eigenschaften.

- **Jobs anzeigen**

  Bringt Sie zurück zur Seite „Jobs“.

Liste der Arbeitsaufgaben

Die Job-Aufgabenliste zeigt in einer Tabelle alle Aufgaben an, die mit einem bestimmten Job verknüpft sind, sowie die Eigenschaften jeder Aufgabe.

- **Startzeit**

  Zeigt den Tag und die Uhrzeit an, zu der die Aufgabe gestartet wurde. Standardmäßig werden die aktuellsten Aufgaben oben in der Spalte und ältere Aufgaben unten angezeigt.

- **Typ**

  Zeigt den Aufgabentyp an.

- **Zustand**

  Der Status einer bestimmten Aufgabe:

  - **Vollendet**

    Die Aufgabe ist abgeschlossen.

  - **In der Warteschlange**

    Die Aufgabe wird gleich ausgeführt.

  - **Läuft**

    Die Aufgabe wird ausgeführt.

  - **Warten**

    Ein Auftrag wurde übermittelt und einige zugehörige Aufgaben warten darauf, in die Warteschlange gestellt und ausgeführt zu werden.

- **Status**

  Zeigt den Aufgabenstatus an:

  - **Fehler (❗)**

    Die Aufgabe ist fehlgeschlagen.

  - **Normal (✅)**

    Die Aufgabe war erfolgreich.

- **Übersprungen ( )**

  Eine Aufgabe ist fehlgeschlagen, was dazu führte, dass nachfolgende Aufgaben übersprungen wurden.

- **Dauer**

  Zeigt die seit Beginn der Aufgabe verstrichene Zeit an.

- **Abgeschlossene Zeit**

  Zeigt die Zeit an, zu der die Aufgabe abgeschlossen wurde. Standardmäßig ist diese Spalte ausgeblendet.

- **Aufgaben-ID**

  Zeigt die GUID an, die eine einzelne Aufgabe für einen Job identifiziert. Die Spalte kann sortiert und gefiltert werden. Standardmäßig ist diese Spalte ausgeblendet.

- **Abhängigkeitsreihenfolge**

  Zeigt eine Ganzzahl an, die die Abfolge der Aufgaben in einem Diagramm darstellt, wobei der ersten Aufgabe die Null zugewiesen wird. Standardmäßig ist diese Spalte ausgeblendet.

- **Bereich „Aufgabendetails“**

  Zeigt zusätzliche Informationen zu jeder Jobaufgabe an, darunter den Aufgabennamen, die Aufgabenbeschreibung und, falls die Aufgabe fehlgeschlagen ist, den Grund für das Fehlschlagen.

- **Aufgabennachrichtenbereich**

  Zeigt spezifische Nachrichten zur ausgewählten Aufgabe an. Die Nachrichten können einen Grund für den Fehler und Vorschläge zur Fehlerbehebung enthalten. Nicht alle Aufgaben zeigen Aufgabenmeldungen an.

Dialogfeld „Erweiterte sekundäre Einstellungen“

Sie können das Dialogfeld „Erweiterte sekundäre Einstellungen“ verwenden, um versionsflexible Replikation, Mehrfachkopiesicherung und speicherplatzbezogene Einstellungen auf einem sekundären Volume zu aktivieren. Sie können das Dialogfeld „Erweiterte sekundäre Einstellungen“ verwenden, wenn Sie die aktuellen Einstellungen ändern, aktivieren oder deaktivieren möchten.

Speicherplatzbezogene Einstellungen maximieren die Menge der gespeicherten Daten, darunter die folgenden: Deduplizierung, Datenkomprimierung, automatische Vergrößerung und Speicherplatzgarantie.

Das Dialogfeld enthält die folgenden Felder:

- **Versionsflexible Replikation aktivieren**

  Aktiviert SnapMirror mit versionsflexibler Replikation. Durch die versionsflexible Replikation ist der SnapMirror Schutz eines Quellvolumes möglich, selbst wenn das Zielvolume unter einer früheren ONTAP -Version als das Quellvolume ausgeführt wird.

  - Sicherung aktivieren

Wenn die versionsflexible Replikation aktiviert ist, können auch mehrere Snapshot-Kopien der SnapMirror Quelldaten zum SnapMirror -Ziel übertragen und dort aufbewahrt werden.

- **Deduplizierung aktivieren**

  Ermöglicht die Deduplizierung auf dem sekundären Volume in einer SnapVault -Beziehung, sodass doppelte Datenblöcke eliminiert werden, um Speicherplatz zu sparen. Sie können die Deduplizierung verwenden, wenn die Speicherplatzeinsparung mindestens 10 Prozent beträgt und die Datenüberschreibungsrate nicht hoch ist. Deduplizierung wird häufig für virtualisierte Umgebungen, Dateifreigaben und Sicherungsdaten verwendet. Diese Einstellung ist standardmäßig deaktiviert. Wenn aktiviert, wird dieser Vorgang nach jeder Übertragung gestartet.

  - Komprimierung aktivieren

    Ermöglicht transparente Datenkomprimierung. Sie können die Komprimierung verwenden, wenn die Speicherplatzeinsparung mindestens 10 Prozent beträgt, der potenzielle Mehraufwand akzeptabel ist und genügend Systemressourcen vorhanden sind, um die Komprimierung außerhalb der Spitzenzeiten abzuschließen. 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 Komprimieren der Daten vor dem Schreiben auf die Festplatte. Sie können die Inline-Komprimierung verwenden, wenn Ihr System während der Spitzenzeiten nicht mehr als 50 Prozent ausgelastet ist und wenn das System während der Spitzenzeiten neue Schreibvorgänge und zusätzliche CPU-Leistung bewältigen kann. Diese Einstellung ist nur verfügbar, wenn „Komprimierung aktivieren“ ausgewählt ist.

- **Automatisches Wachstum aktivieren**

  Ermöglicht Ihnen, das Zielvolume automatisch zu vergrößern, wenn der Prozentsatz des freien Speicherplatzes unter dem angegebenen Schwellenwert liegt, solange auf dem zugehörigen Aggregat Speicherplatz verfügbar ist.

- **Maximale Größe**

  Legt den maximalen Prozentsatz fest, auf den ein Volume anwachsen kann. Der Standardwert ist 20 Prozent größer als die Größe des Quellvolumes. Ein Volume wächst nicht automatisch, wenn die aktuelle Größe größer oder gleich dem maximalen Autogrow-Prozentsatz ist. Dieses Feld ist nur aktiviert, wenn die Einstellung „Autogrow“ aktiviert ist.

- **Größe erhöhen**

  Gibt den Prozentwert an, um den das Volume automatisch wächst, bevor der maximale Prozentsatz des Quellvolumes erreicht wird.

- **Platzgarantie**

  Stellt sicher, dass auf dem sekundären Volume genügend Speicherplatz zugewiesen wird, damit die Datenübertragung immer erfolgreich ist. Die Speicherplatzgarantie kann eine der folgenden Einstellungen sein:

  - Datei
  - Volumen

◦ Keine + Sie verfügen beispielsweise möglicherweise über ein 200 GB großes Volume mit insgesamt 50 GB großen Dateien, diese Dateien enthalten jedoch nur 10 GB Daten. Die Volumengarantie weist dem Zielvolumen 200 GB zu, unabhängig vom Inhalt der Quelle. Die Dateigarantie weist 50 GB zu, um sicherzustellen, dass auf der Quelle genügend Speicherplatz für Dateien reserviert ist. Wenn Sie in diesem Szenario „Keine“ auswählen, bedeutet dies, dass auf dem Ziel nur 10 GB für den tatsächlich von den Dateidaten auf der Quelle verwendeten Speicherplatz zugewiesen werden.

Die Speicherplatzgarantie ist standardmäßig auf Volume eingestellt.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Anwenden**

  Speichert die ausgewählten Effizienzeinstellungen und wendet sie an, wenn Sie im Dialogfeld „Schutz konfigurieren“ auf „Übernehmen“ klicken.

- **Stornieren**

  Verwirft Ihre Auswahl und schließt das Dialogfeld „Erweiterte Zieleinstellungen“.

Dialogfeld „Erweiterte Zieleinstellungen“

Sie können das Dialogfeld „Erweiterte Zieleinstellungen“ verwenden, um die Speicherplatzgarantieeinstellungen auf einem Zielvolume zu aktivieren. Sie können erweiterte Einstellungen auswählen, wenn die Speicherplatzgarantie auf der Quelle deaktiviert ist, Sie sie aber auf dem Ziel aktivieren möchten. Die Einstellungen für Deduplizierung, Komprimierung und Autogrow in einer SnapMirror -Beziehung werden vom Quellvolume übernommen und können nicht geändert werden.

Platzgarantie

Stellt sicher, dass auf dem Zielvolume genügend Speicherplatz zugewiesen wird, damit die Datenübertragung immer erfolgreich ist. Die Speicherplatzgarantie kann eine der folgenden Einstellungen sein:

- Datei
- Volumen
- Keine

Beispielsweise verfügen Sie möglicherweise über ein 200 GB großes Volume mit insgesamt 50 GB großen Dateien, diese Dateien enthalten jedoch nur 10 GB Daten. Die Volumengarantie weist dem Zielvolumen 200 GB zu, unabhängig vom Inhalt der Quelle. Die Dateigarantie weist 50 GB zu, um sicherzustellen, dass auf dem Ziel genügend Speicherplatz für Quelldateien reserviert ist. Wenn Sie in diesem Szenario **Keine** auswählen, bedeutet dies, dass auf dem Ziel nur 10 GB für den tatsächlich von den Dateidaten auf der Quelle verwendeten Speicherplatz zugewiesen werden.

Die Speicherplatzgarantie ist standardmäßig auf Volume eingestellt.

Dialogfeld „Wiederherstellen“

Sie können das Dialogfeld „Wiederherstellen“ verwenden, um Daten aus einer

bestimmten Snapshot-Kopie auf einem Volume wiederherzustellen.

Wiederherstellen von

Im Bereich „Wiederherstellen von“ können Sie angeben, von wo aus Sie die Daten wiederherstellen möchten.

- **Volumen**

  Gibt das Volume an, von dem Sie Daten wiederherstellen möchten. Standardmäßig ist das Volume ausgewählt, auf dem Sie die Wiederherstellungsaktion gestartet 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.

- **Schnappschusskopie**

  Gibt an, welche Snapshot-Kopie Sie zum Wiederherstellen der Daten verwenden möchten. Standardmäßig ist die aktuellste Snapshot-Kopie ausgewählt. Sie können auch eine andere Snapshot-Kopie aus der Dropdown-Liste auswählen. Die Snapshot-Kopierliste ändert sich je nach ausgewähltem Volume.

- **Listen Sie maximal 995 Dateien und Verzeichnisse auf**

  Standardmäßig werden maximal 995 Objekte in der Liste angezeigt. Sie können dieses Kontrollkästchen deaktivieren, wenn Sie alle Objekte innerhalb des ausgewählten Volumes anzeigen möchten. Dieser Vorgang kann einige Zeit dauern, wenn die Anzahl der Elemente sehr groß ist.

Auswählen der wiederherzustellenden Elemente

Im Bereich „Elemente zum Wiederherstellen 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. Wenn die maximale Anzahl von Elementen ausgewählt ist, werden die Kontrollkästchen zur Elementauswahl deaktiviert.

- **Pfadfeld**

  Zeigt den Pfad zu den Daten an, die Sie wiederherstellen möchten. Sie können entweder zu dem Ordner und den Dateien navigieren, die Sie wiederherstellen möchten, oder den Pfad eingeben. Dieses Feld ist leer, bis Sie einen Pfad auswählen oder eingeben. Klicken Nachdem Sie einen Pfad ausgewählt haben, gelangen Sie in der Verzeichnisstruktur eine Ebene nach oben.

- **Ordner- und Dateiliste**

  Zeigt den Inhalt des von Ihnen eingegebenen Pfads 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 Pfadfeld eingeben, wird die angegebene Datei in den Ordnern und Dateien angezeigt.
- Wenn Sie einen Pfad eingeben, ohne eine bestimmte Datei anzugeben, wird der Inhalt des Ordners in der Liste „Ordner und Dateien“ angezeigt 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 zum Anzeigen vorhanden sind. Wenn Sie mit dem Vorgang fortfahren, 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 Volumes anzeigen möchten.

Sie können NTFS-Dateistreams nicht wiederherstellen.

Wiederherstellen in

Im Bereich „Wiederherstellen nach“ können Sie angeben, wo Sie die Daten wiederherstellen möchten.

- **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 vorhanden sein. Sie können die Schaltfläche **Durchsuchen** verwenden, um zu dem Speicherort zu navigieren, an dem die Daten wiederhergestellt werden sollen, oder Sie können den Pfad manuell im Format „Cluster://svm/Volume/Pfad“ eingeben.

  - Verzeichnishierarchie beibehalten

    Wenn diese Option aktiviert ist, bleibt die Struktur der Originaldatei oder des Originalverzeichnisses erhalten. Wenn die Quelle beispielsweise /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

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Stornieren**

  Verwirft Ihre Auswahl und schließt das Dialogfeld „Wiederherstellen“.

- **Wiederherstellen**

  Wendet Ihre Auswahl an und beginnt mit dem Wiederherstellungsprozess.

Dialogfeld „Verzeichnisse durchsuchen“

Sie können das Dialogfeld „Verzeichnisse durchsuchen“ verwenden, wenn Sie Daten in einem Verzeichnis auf einem Cluster und einer SVM wiederherstellen möchten, das sich von der ursprünglichen Quelle unterscheidet. Standardmäßig sind der ursprüngliche Quellcluster und das ursprüngliche Quellvolume ausgewählt.

Im Dialogfeld „Verzeichnisse durchsuchen“ können Sie den Cluster, die SVM, das Volume und den

Verzeichnispfad auswählen, in dem die Daten wiederhergestellt werden sollen.

- **Cluster**

  Listet die verfügbaren Clusterziele auf, zu denen Sie eine Wiederherstellung durchführen können. Standardmäßig ist der Cluster des ursprünglichen Quellvolumes ausgewählt.

- **SVM-Dropdown-Liste**

  Listet die für den ausgewählten Cluster verfügbaren SVMs auf. Standardmäßig ist die SVM des ursprünglichen Quellvolumes ausgewählt.

- **Volumen**

  Listet alle Lese-/Schreibvolumes in einer ausgewählten SVM auf. Sie können die Bände nach Namen und verfügbarem Speicherplatz filtern. Das Volume mit dem größten Speicherplatz wird zuerst aufgeführt und so weiter in absteigender Reihenfolge. Standardmäßig ist das ursprüngliche Quellvolume ausgewählt.

- **Textfeld für den Dateipfad**

  Ermöglicht Ihnen, den Dateipfad einzugeben, in dem die Daten wiederhergestellt werden sollen. Der von Ihnen eingegebene Pfad muss bereits vorhanden sein.

- **Name**

  Zeigt die Namen der verfügbaren Ordner für das ausgewählte Volume an. Wenn Sie in der Namensliste auf einen Ordner klicken, werden die Unterordner angezeigt, sofern welche vorhanden sind. In den Ordnern enthaltene Dateien werden nicht angezeigt. Klicken Nachdem Sie einen Ordner ausgewählt haben, gelangen Sie in der Verzeichnisstruktur eine Ebene nach oben.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Verzeichnis auswählen**

  Übernimmt Ihre Auswahl 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“.

Dialogfeld „Schutz konfigurieren“

Sie können das Dialogfeld „Schutz konfigurieren“ verwenden, um SnapMirror und SnapVault -Beziehungen für alle Lese-, Schreib- und Datenschutzvolumes auf Clustern zu erstellen, um sicherzustellen, dass die Daten auf einem Quellvolume oder primären Volume repliziert werden.

Registerkarte „Quelle“

- **Topologieansicht**

Zeigt eine visuelle Darstellung der Beziehung an, die Sie erstellen. Die Quelle in der Topologie wird standardmäßig hervorgehoben.

- **Quelleninformationen**

  Zeigt Details zu den ausgewählten Quellvolumes an, einschließlich der folgenden Informationen:

  - Name des Quellclusters
  - Quell-SVM-Name
  - Kumulative Gesamtgröße des Volumens

    Zeigt die Gesamtgröße aller ausgewählten Quellvolumes an.

  - Kumulative Größe des verwendeten Volumens

    Zeigt die kumulierte verwendete Volumegröße für alle ausgewählten Quellvolumes an.

  - Quellvolumen

    Zeigt die folgenden Informationen in einer Tabelle an:

    - Quellvolumen

      Zeigt die Namen der ausgewählten Quellvolumes an.

    - Typ

      Zeigt den Datenträgertyp an.

    - SnapLock -Typ

      Zeigt den SnapLock -Typ des Volumes an. Die Optionen sind Compliance, Enterprise und Non-SnapLock.

    - Snapshot-Kopie

      Zeigt die Snapshot-Kopie an, die für die Baseline-Übertragung verwendet wird. Wenn das Quellvolume Lese-/Schreibzugriff hat, gibt der Wert „Standard“ in der Spalte „Snapshot-Kopie“ an, dass standardmäßig eine neue Snapshot-Kopie erstellt und für die Baseline-Übertragung verwendet wird. Wenn es sich bei dem Quellvolume um ein Datensicherungsvolume handelt, gibt der Wert „Standard“ in der Spalte „Snapshot-Kopie“ an, dass keine neue Snapshot-Kopie erstellt wird und alle vorhandenen Snapshot-Kopien zum Ziel übertragen werden. Wenn Sie auf den Wert „Snapshot-Kopie“ klicken, wird eine Liste mit Snapshot-Kopien angezeigt, aus der Sie eine vorhandene Snapshot-Kopie auswählen können, die Sie für die Baseline-Übertragung verwenden möchten. Sie können keine andere Standard-Snapshot-Kopie auswählen, wenn der Quelltyp Datenschutz ist.

Registerkarte „SnapMirror “

Ermöglicht Ihnen, beim Erstellen einer SnapMirror -Beziehung einen Zielcluster, eine Storage Virtual Machine (SVM) und ein Aggregat für eine Schutzbeziehung sowie eine Namenskonvention für Ziele anzugeben. Sie können auch eine SnapMirror -Richtlinie und einen Zeitplan angeben.

- **Topologieansicht**

Zeigt eine visuelle Darstellung der Beziehung an, die Sie erstellen. Die SnapMirror Zielressource in der Topologie ist standardmäßig hervorgehoben.

- **Zielinformationen**

  Ermöglicht Ihnen, die Zielressourcen für eine Schutzbeziehung auszuwählen:

  - Erweiterter Link

    Startet das Dialogfeld „Erweiterte Zieleinstellungen“, wenn Sie eine SnapMirror -Beziehung erstellen.

  - Cluster

    Listet die Cluster auf, die als Schutzzielhosts verfügbar sind. Dieses Feld ist erforderlich.

  - Speicher-Virtual-Machine (SVM)

    Listet die SVMs auf, die auf dem ausgewählten Cluster verfügbar sind. Bevor die SVM-Liste gefüllt wird, muss ein Cluster ausgewählt werden. Dieses Feld ist erforderlich.

  - Aggregat

    Listet die Aggregate auf, die auf der ausgewählten SVM verfügbar sind. Bevor die Aggregatliste gefüllt wird, muss ein Cluster ausgewählt werden. Dieses Feld ist erforderlich. Die aggregierte Liste zeigt die folgenden Informationen an:

    - Rang

      Wenn mehrere Aggregate alle Anforderungen für ein Ziel erfüllen, gibt der Rang die Priorität an, mit der das Aggregat gemäß den folgenden Bedingungen aufgelistet wird:

      A. Um eine Trennung der Fehlerdomänen zu ermöglichen, wird ein Aggregat bevorzugt, das sich auf einem anderen Knoten als dem Quellvolume-Knoten befindet.
      B. Um einen Lastenausgleich zwischen den Knoten in einem Cluster zu ermöglichen, wird ein Aggregat auf einem Knoten mit weniger Volumes bevorzugt.
      C. Um einen Kapazitätsausgleich zu ermöglichen, wird ein Aggregat bevorzugt, das über mehr freien Speicherplatz als andere Aggregate verfügt. Ein Rang von 1 bedeutet, dass das Aggregat gemäß den drei Kriterien am meisten bevorzugt wird.

    - Aggregatname

      Name des Aggregats

    - Verfügbare Kapazität
    - Menge an Speicherplatz, der auf dem Aggregat für Daten verfügbar ist
    - Ressourcenpool

      Name des Ressourcenpools, zu dem das Aggregat gehört

  - Namenskonvention

    Gibt die Standardbenennungskonvention an, die auf das Zielvolume angewendet wird. Sie können die bereitgestellte Namenskonvention akzeptieren oder eine benutzerdefinierte erstellen. Die Namenskonvention kann die folgenden Attribute haben: %C, %M, %V und %N, wobei %C der

Clustername, %M der SVM-Name, %V das Quellvolume und %N der Name des Zielknotens der Topologie ist.

Das Feld für die Namenskonvention wird rot hervorgehoben, wenn Ihre Eingabe ungültig ist. Wenn Sie auf den Link „Namensvorschau anzeigen“ klicken, wird eine Vorschau der von Ihnen eingegebenen Namenskonvention angezeigt. Der Vorschautext wird dynamisch aktualisiert, während Sie eine Namenskonvention in das Textfeld eingeben. Beim Erstellen der Beziehung wird dem Zielnamen ein Suffix zwischen 001 und 999 angehängt, das das im Vorschautext angezeigte nnn ersetzt, wobei 001 zuerst, 002 als zweites usw. zugewiesen wird.

- **Beziehungseinstellungen**

  Ermöglicht Ihnen, die maximale Übertragungsrate, die SnapMirror -Richtlinie und den Zeitplan anzugeben, die die Schutzbeziehung verwendet:

  - Max. Übertragungsrate

    Gibt die maximale Rate an, mit der Daten zwischen Clustern über das Netzwerk übertragen werden. Wenn Sie keine maximale Übertragungsrate verwenden möchten, ist die Basisübertragung zwischen Beziehungen unbegrenzt.

  - SnapMirror -Richtlinie

    Gibt die ONTAP SnapMirror -Richtlinie für die Beziehung an. 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. Zu den verfügbaren Zeitplänen gehören „Keine“, „5 Min.“, „8 Stunden“, „täglich“, „stündlich“ und „wöchentlich“. Der Standardwert ist „Keine“, was bedeutet, dass der Beziehung kein Zeitplan zugeordnet ist. Beziehungen ohne Zeitpläne haben keine Verzögerungsstatuswerte, es sei denn, sie gehören zu einem Speicherdienst.

  - Zeitplan erstellen

    Öffnet das Dialogfeld „Zeitplan erstellen“, in dem Sie einen neuen SnapMirror -Zeitplan erstellen können.

Registerkarte „SnapVault “

Ermöglicht Ihnen, beim Erstellen einer SnapVault -Beziehung einen sekundären Cluster, SVM und ein Aggregat für eine Schutzbeziehung sowie eine Namenskonvention für sekundäre Volumes anzugeben. Sie können auch eine SnapVault -Richtlinie und einen Zeitplan angeben.

- **Topologieansicht**

  Zeigt eine visuelle Darstellung der Beziehung an, die Sie erstellen. Die sekundäre SnapVault Ressource in der Topologie wird standardmäßig hervorgehoben.

- **Sekundäre Informationen**

Ermöglicht Ihnen, die sekundären Ressourcen für eine Schutzbeziehung auszuwählen:

- Erweiterter Link

  Öffnet das Dialogfeld „Erweiterte sekundäre Einstellungen“.

- Cluster

  Listet die Cluster auf, die als sekundäre Schutzhosts verfügbar sind. Dieses Feld ist erforderlich.

- Speicher-Virtual-Machine (SVM)

  Listet die SVMs auf, die auf dem ausgewählten Cluster verfügbar sind. Bevor die SVM-Liste gefüllt wird, muss ein Cluster ausgewählt werden. Dieses Feld ist erforderlich.

- Aggregat

  Listet die Aggregate auf, die auf der ausgewählten SVM verfügbar sind. Bevor die Aggregatliste gefüllt wird, muss ein Cluster ausgewählt werden. Dieses Feld ist erforderlich. Die aggregierte Liste zeigt die folgenden Informationen an:

  - Rang

    Wenn mehrere Aggregate alle Anforderungen für ein Ziel erfüllen, gibt der Rang die Priorität an, mit der das Aggregat gemäß den folgenden Bedingungen aufgelistet wird:

    A. Um eine Trennung der Fehlerdomänen zu ermöglichen, wird vorzugsweise ein Aggregat verwendet, das sich auf einem anderen Knoten als dem primären Volume-Knoten befindet.
    B. Um einen Lastenausgleich zwischen den Knoten in einem Cluster zu ermöglichen, wird ein Aggregat auf einem Knoten mit weniger Volumes bevorzugt.
    C. Um einen Kapazitätsausgleich zu ermöglichen, wird ein Aggregat bevorzugt, das über mehr freien Speicherplatz als andere Aggregate verfügt. Ein Rang von 1 bedeutet, dass das Aggregat gemäß den drei Kriterien am meisten bevorzugt wird.

  - Aggregatname

    Name des Aggregats

  - Verfügbare Kapazität
  - Menge an Speicherplatz, der auf dem Aggregat für Daten verfügbar ist
  - Ressourcenpool

    Name des Ressourcenpools, zu dem das Aggregat gehört

- Namenskonvention

  Gibt die Standardbenennungskonvention an, die auf das sekundäre Volume angewendet wird. Sie können die bereitgestellte Namenskonvention akzeptieren oder eine benutzerdefinierte erstellen. Die Namenskonvention kann die folgenden Attribute haben: %C, %M, %V und %N, wobei %C der Clustername, %M der SVM-Name, %V das Quellvolume und %N der Name des sekundären Knotens der Topologie ist.

Das Feld für die Namenskonvention wird rot hervorgehoben, wenn Ihre Eingabe ungültig ist. Wenn Sie auf den Link „Namensvorschau anzeigen“ klicken, wird eine Vorschau der von Ihnen eingegebenen

Namenskonvention angezeigt. Der Vorschautext wird dynamisch aktualisiert, während Sie eine Namenskonvention in das Textfeld eingeben. Wenn Sie einen ungültigen Wert eingeben, werden die ungültigen Informationen im Vorschaubereich als rote Fragezeichen angezeigt. Beim Erstellen der Beziehung wird dem sekundären Namen ein Suffix zwischen 001 und 999 angehängt, das das im Vorschautext angezeigte nnn ersetzt, wobei 001 zuerst, 002 als zweites usw. zugewiesen wird.

- **Beziehungseinstellungen**

  Ermöglicht Ihnen, die maximale Übertragungsrate, die SnapVault -Richtlinie und den SnapVault Zeitplan anzugeben, die die Schutzbeziehung verwendet:

  - Max. Übertragungsrate

    Gibt die maximale Rate an, mit der Daten zwischen Clustern über das Netzwerk übertragen werden. Wenn Sie keine maximale Übertragungsrate verwenden möchten, ist die Basisübertragung zwischen Beziehungen unbegrenzt.

  - SnapVault -Richtlinie

    Gibt die ONTAP SnapVault -Richtlinie für die Beziehung an. Der Standardwert ist XDPDefault.

  - Richtlinie erstellen

    Startet das Dialogfeld „SnapVault -Richtlinie erstellen“, in dem Sie eine neue SnapVault -Richtlinie erstellen und verwenden können.

  - SnapVault -Zeitplan

    Gibt den ONTAP SnapVault -Zeitplan für die Beziehung an. Zu den verfügbaren Zeitplänen gehören „Keine“, „5 Min.“, „8 Stunden“, „täglich“, „stündlich“ und „wöchentlich“. Der Standardwert ist „Keine“, was bedeutet, dass der Beziehung kein Zeitplan zugeordnet ist. Beziehungen ohne Zeitpläne haben keine Verzögerungsstatuswerte, es sei denn, sie gehören zu einem Speicherdienst.

  - Zeitplan erstellen

    Öffnet das Dialogfeld „Zeitplan erstellen“, in dem Sie einen SnapVault -Zeitplan erstellen können.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Stornieren**

  Verwirft Ihre Auswahl und schließt das Dialogfeld „Schutz konfigurieren“.

- **Anwenden**

  Wendet Ihre Auswahl an und beginnt mit dem Schutzvorgang.

Dialogfeld „Zeitplan erstellen“

Im Dialogfeld „Zeitplan erstellen“ können Sie einen grundlegenden oder erweiterten Schutzzeitplan für SnapMirror und SnapVault Beziehungsübertragungen erstellen. Sie können einen neuen Zeitplan erstellen, um die Häufigkeit der Datenübertragungen

aufgrund häufiger Datenaktualisierungen zu erhöhen, oder Sie können einen weniger häufigen Zeitplan erstellen, wenn sich die Daten selten ändern.

Für synchrone SnapMirror Beziehungen können keine Zeitpläne konfiguriert werden.

- **Zielcluster**

  Der Name des Clusters, den Sie auf der Registerkarte „SnapVault“ oder „SnapMirror “ des Dialogfelds „Schutz konfigurieren“ ausgewählt haben.

- **Zeitplanname**

  Der Name, den Sie für den Zeitplan angeben. Zeitplannamen können aus den Buchstaben A bis Z, a bis z, 0 bis 9 sowie den folgenden Sonderzeichen bestehen: ! @ # $ % ^ & * ( ) _ -. Zeitplannamen dürfen die folgenden Zeichen nicht enthalten: < >.

- **Grundlegend oder Fortgeschritten**

  Der Zeitplanmodus, den Sie verwenden möchten.

  Der Basismodus umfasst die folgenden Elemente:

  ◦ Wiederholen

    Wie oft eine geplante Übertragung erfolgt. Zur Auswahl stehen stündlich, täglich und wöchentlich.

  ◦ Tag

    Wenn eine wöchentliche Wiederholung ausgewählt ist, wird der Wochentag angegeben, an dem die Übertragung erfolgt.

  ◦ Zeit

    Wenn „Täglich“ oder „Wöchentlich“ ausgewählt ist, wird die Tageszeit angegeben, zu der eine Übertragung erfolgt.

    Der erweiterte Modus umfasst die folgenden Elemente:

  ◦ Monate

    Eine durch Kommas getrennte numerische Liste, die die Monate des Jahres darstellt. Gültige Werte sind 0 bis 11, wobei Null für Januar steht usw. Dieses Element ist optional. Wenn Sie das Feld leer lassen, bedeutet dies, dass die Überweisungen jeden Monat erfolgen.

  ◦ Tage

    Eine durch Kommas getrennte numerische Liste, die den Tag des Monats darstellt. Gültige Werte sind 1 bis 31. Dieses Element ist optional. Wenn Sie das Feld leer lassen, bedeutet dies, dass an jedem Tag des Monats eine Überweisung erfolgt.

  ◦ 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 Sie das Feld leer lassen, bedeutet dies, dass an jedem Wochentag eine Überweisung erfolgt. Wenn ein Wochentag angegeben ist, aber kein Tag im Monat, erfolgt eine Überweisung nur am angegebenen Wochentag und nicht täglich.

◦ Std

Eine durch Kommas getrennte numerische Liste, die die Anzahl der Stunden eines Tages darstellt. Gültige Werte sind 0 bis 23, wobei 0 Mitternacht darstellt. 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.

Dialogfeld „SnapMirror -Richtlinie erstellen“

Im Dialogfeld „SnapMirror -Richtlinie erstellen“ können Sie eine Richtlinie erstellen, um die Priorität für SnapMirror Übertragungen festzulegen. Sie verwenden Richtlinien, um die Effizienz der Übertragungen von der Quelle zum Ziel zu maximieren.

- **Zielcluster**

  Der Name des Clusters, den Sie auf der Registerkarte „SnapMirror “ des Dialogfelds „Schutz konfigurieren“ ausgewählt haben.

- **Ziel-SVM**

  Der Name der SVM, die Sie auf der Registerkarte „SnapMirror “ des Dialogfelds „Schutz konfigurieren“ ausgewählt haben.

- **Richtlinienname**

  Der Name, den Sie für die neue Richtlinie angeben. Richtliniennamen können aus den Zeichen A bis Z, a bis z, 0 bis 9, Punkt (.), Bindestrich (-) und Unterstrich (_) bestehen.

- **Transferpriorität**

  Die Priorität, mit der eine Übertragung für asynchrone Vorgänge ausgeführt wird. Sie können entweder „Normal“ oder „Niedrig“ auswählen. Übertragungsbeziehungen mit Richtlinien, die eine normale Übertragungspriorität festlegen, werden vor denen mit Richtlinien ausgeführt, die eine niedrige Übertragungspriorität festlegen.

- **Kommentar**

  Ein optionales Feld, in dem Sie Kommentare zur Richtlinie hinzufügen können.

- **Transfer-Neustart**

  Gibt an, welche Neustartaktion ausgeführt werden soll, wenn eine Übertragung durch einen Abbruchvorgang oder einen anderen Fehlertyp, beispielsweise einen Netzwerkausfall, unterbrochen wird. Sie können eine der folgenden Optionen auswählen:

  ◦ Stets

  Gibt an, dass vor dem Neustart einer Übertragung eine neue Snapshot-Kopie erstellt wird. Anschließend wird die Übertragung (sofern vorhanden) von einem Prüfpunkt aus neu gestartet, gefolgt von einer inkrementellen Übertragung von der neu erstellten Snapshot-Kopie.

◦ Niemals

Gibt an, dass unterbrochene Übertragungen nie neu gestartet werden.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Stornieren**

  Verwirft die Auswahl und schließt das Dialogfeld „Schutz konfigurieren“.

- **Anwenden**

  Wendet Ihre Auswahl an und beginnt mit dem Schutzvorgang.

Dialogfeld „SnapVault -Richtlinie erstellen“

Im Dialogfeld „SnapVault -Richtlinie erstellen“ können Sie eine Richtlinie erstellen, um die Priorität für SnapVault Übertragungen festzulegen. Sie verwenden Richtlinien, um die Effizienz von Übertragungen vom primären zum sekundären Volume zu maximieren.

- **Zielcluster**

  Der Name des Clusters, den Sie auf der Registerkarte „SnapVault “ des Dialogfelds „Schutz konfigurieren“ ausgewählt haben.

- **Ziel-SVM**

  Der Name der SVM, die Sie auf der Registerkarte „SnapVault “ des Dialogfelds „Schutz konfigurieren“ ausgewählt haben.

- **Richtlinienname**

  Der Name, den Sie für die neue Richtlinie angeben. 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. Sie können entweder „Normal“ oder „Niedrig“ auswählen. Übertragungsbeziehungen mit Richtlinien, die eine normale Übertragungspriorität festlegen, werden vor denen mit Richtlinien ausgeführt, die eine niedrige Übertragungspriorität festlegen. Die Standardeinstellung ist „Normal“.

- **Kommentar**

  Ein optionales Feld, in dem Sie einen Kommentar mit bis zu 255 Zeichen zur SnapVault -Richtlinie hinzufügen können.

- **Zugriffszeit ignorieren**

  Gibt an, ob inkrementelle Übertragungen für Dateien ignoriert werden, bei denen sich nur die Zugriffszeit geändert hat.

- **Replikationsbezeichnung**

  Listet in einer Tabelle die Regeln auf, die mit von ONTAP ausgewählten Snapshot-Kopien verknüpft sind, die in einer Richtlinie über ein bestimmtes Replikationslabel verfügen. Darüber hinaus stehen folgende Informationen und Aktionen zur Verfügung:

  - Befehlsschaltflächen

    Mit den Befehlsschaltflächen können Sie die folgenden Aktionen ausführen:

    - Hinzufügen

      Ermöglicht Ihnen das Erstellen einer Snapshot-Kopierbezeichnung und einer Aufbewahrungsanzahl.

    - Aufbewahrungsanzahl bearbeiten

      Ermöglicht Ihnen, die Aufbewahrungsanzahl für eine vorhandene Snapshot-Kopiebezeichnung zu ändern. Die Anzahl der Aufbewahrungen muss eine Zahl zwischen 1 und 251 sein. Die Summe aller Aufbewahrungszahlen für alle Regeln darf 251 nicht überschreiten.

    - Löschen

      Ermöglicht Ihnen, eine vorhandene Snapshot-Kopierbezeichnung zu löschen.

  - Snapshot-Kopie-Etikett

    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 auswählen, die über zwei oder mehr lokale Snapshot-Kopierrichtlinien verfügen, werden in der Tabelle alle Bezeichnungen aller Richtlinien angezeigt.

  - Zeitplan

    Zeigt den mit jedem Snapshot-Kopierlabel verknüpften Zeitplan an. Wenn einem Label mehr als ein Zeitplan zugeordnet ist, werden die Zeitpläne für dieses Label in einer durch Kommas getrennten Liste angezeigt. Wenn Sie mehrere Volumes mit derselben Bezeichnung, aber unterschiedlichen Zeitplänen auswählen, wird im Zeitplan „Verschiedene“ angezeigt, um darauf hinzuweisen, dass den ausgewählten Volumes mehr als ein Zeitplan zugeordnet ist.

  - Zielaufbewahrungsanzahl

    Zeigt die Anzahl der Snapshot-Kopien mit der angegebenen Bezeichnung an, die auf dem sekundären SnapVault aufbewahrt werden. Die Aufbewahrungszahlen für Labels mit mehreren Zeitplänen zeigen die Summe der Aufbewahrungszahlen jedes Label- und Zeitplanpaars an. Wenn Sie mehrere Volumes mit zwei oder mehr lokalen Snapshot-Kopierrichtlinien auswählen, ist die Aufbewahrungsanzahl leer.

Dialogfeld „Beziehung bearbeiten“

Sie können eine vorhandene Schutzbeziehung bearbeiten, um die maximale Übertragungsrate, die Schutzrichtlinie oder den Schutzzeitplan zu ändern.

Zielinformationen

- **Zielcluster**

  Der Name des ausgewählten Zielclusters.

- **Ziel-SVM**

  Der Name der ausgewählten SVM

- **Beziehungseinstellungen**

  Ermöglicht Ihnen, die maximale Übertragungsrate, die SnapMirror -Richtlinie und den Zeitplan anzugeben, die die Schutzbeziehung verwendet:

  - Max. Übertragungsrate

    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 (KBps), Megabyte pro Sekunde (MBps), Gigabyte pro Sekunde (GBps) oder Terabyte pro Sekunde (TBps) auswählen. Die von Ihnen angegebene maximale Übertragungsrate muss größer als 1 KBps und kleiner als 4 TBps sein. Wenn Sie keine maximale Übertragungsrate verwenden möchten, ist die Basisübertragung zwischen Beziehungen unbegrenzt. Wenn der primäre Cluster und der sekundäre Cluster identisch sind, ist diese Einstellung deaktiviert.

  - SnapMirror -Richtlinie

    Gibt die ONTAP SnapMirror -Richtlinie für die Beziehung an. 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. Zu den verfügbaren Zeitplänen gehören „Keine“, „5 Min.“, „8 Stunden“, „täglich“, „stündlich“ und „wöchentlich“. Der Standardwert ist „Keine“, was bedeutet, dass der Beziehung kein Zeitplan zugeordnet ist. Beziehungen ohne Zeitpläne haben keine Verzögerungsstatuswerte, es sei denn, sie gehören zu einem Speicherdienst.

  - Zeitplan erstellen

    Öffnet das Dialogfeld „Zeitplan erstellen“, in dem Sie einen neuen SnapMirror -Zeitplan erstellen können.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Stornieren**

  Verwirft die Auswahl und schließt das Dialogfeld „Schutz konfigurieren“.

- **Einreichen**

  Übernimmt Ihre Auswahl und schließt das Dialogfeld „Beziehung bearbeiten“.

Dialogfeld „Initialisieren/Aktualisieren“

Über das Dialogfeld „Initialisieren/Aktualisieren“ können Sie eine erstmalige Baseline-Übertragung für eine neue Schutzbeziehung durchführen oder eine Beziehung aktualisieren, wenn diese bereits initialisiert ist und Sie eine manuelle, ungeplante, inkrementelle Aktualisierung durchführen möchten.

Registerkarte „Übertragungsoptionen“

Auf der Registerkarte „Übertragungsoptionen“ können Sie die Initialisierungspriorität einer Übertragung und die während der Übertragungen verwendete Bandbreite ändern.

- **Transferpriorität**

  Die Priorität, mit der die Übertragung ausgeführt wird. Sie können entweder „Normal“ oder „Niedrig“ auswählen. Beziehungen mit Richtlinien, die eine normale Übertragungspriorität angeben, werden vor denen ausgeführt, die eine niedrige Übertragungspriorität angeben. Standardmäßig ist „Normal“ ausgewählt.

- **Maximale Übertragungsrate**

  Gibt die maximale Rate an, mit der Daten zwischen Clustern über das Netzwerk übertragen werden. Wenn Sie keine maximale Übertragungsrate verwenden möchten, ist die Basisübertragung zwischen Beziehungen unbegrenzt. Wenn Sie mehr als eine Beziehung mit unterschiedlichen maximalen Übertragungsraten auswählen, können Sie eine der folgenden Einstellungen für die maximale Übertragungsrate angeben:

  - Verwenden Sie die Werte, die Sie beim Einrichten oder Bearbeiten einzelner Beziehungen angegeben haben.

    Wenn diese Option ausgewählt ist, verwenden Initialisierungs- und Aktualisierungsvorgänge die maximale Übertragungsrate, die zum Zeitpunkt der Erstellung oder Bearbeitung jeder Beziehung angegeben wurde. Dieses Feld ist nur verfügbar, wenn mehrere Beziehungen mit unterschiedlichen Übertragungsraten initialisiert oder aktualisiert werden.

  - Unbegrenzt

    Gibt an, dass für Übertragungen zwischen Beziehungen keine Bandbreitenbeschränkung besteht. Dieses Feld ist nur verfügbar, wenn mehrere Beziehungen mit unterschiedlichen Übertragungsraten 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 (KBps), Megabyte pro Sekunde (MBps), Gigabyte pro Sekunde (GBps) oder Terabyte pro Sekunde (TBps) auswählen. Die von Ihnen angegebene maximale Übertragungsrate muss größer als 1 KBps und kleiner als 4 TBps sein.

Registerkarte „Quell-Snapshot-Kopien“

Auf der Registerkarte „Quell-Snapshot-Kopien“ werden die folgenden Informationen zur Quell-Snapshot-Kopie angezeigt, die für die Baseline-Übertragung verwendet wird:

- **Quellvolumen**

  Zeigt die Namen der entsprechenden Quellvolumes an.

- **Zielvolumen**

  Zeigt die Namen der ausgewählten Zielvolumes an.

- **Quellentyp**

  Zeigt den Datenträgertyp an. Der Typ kann entweder Lesen/Schreiben oder Datenschutz sein.

- **Schnappschusskopie**

  Zeigt die Snapshot-Kopie an, die für die Datenübertragung verwendet wird. Wenn Sie auf den Wert „Snapshot-Kopie“ klicken, wird das Dialogfeld „Quell-Snapshot-Kopie auswählen“ angezeigt, in dem Sie je nach Art Ihrer Schutzbeziehung und der von Ihnen ausgeführten Operation eine bestimmte Snapshot-Kopie für Ihre Übertragung auswählen können. Die Option zum Angeben einer anderen Snapshot-Kopie ist für Quellen vom Typ „Datenschutz“ nicht verfügbar.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aufgaben ausführen:

- **Stornieren**

  Verwirft Ihre Auswahl und schließt das Dialogfeld „Initialisieren/Aktualisieren“.

- **Einreichen**

  Speichert Ihre Auswahl und startet den Initialisierungs- oder Aktualisierungsjob.

Dialogfeld „Neu synchronisieren“

Über das Dialogfeld „Neu synchronisieren“ können Sie Daten einer SnapMirror oder SnapVault -Beziehung neu synchronisieren, die zuvor unterbrochen wurde und deren Ziel dann zu einem Lese-/Schreib-Volume gemacht wurde. Sie können die Synchronisierung auch dann erneut durchführen, wenn eine erforderliche gemeinsame Snapshot-Kopie auf dem Quellvolume gelöscht wird und dadurch SnapMirror oder SnapVault -Updates fehlschlagen.

Registerkarte „Resynchronisierungsoptionen“

Auf der Registerkarte „Resynchronisierungsoptionen“ können Sie die Übertragungspriorität und die maximale Übertragungsrate für die Schutzbeziehung festlegen, die Sie neu synchronisieren.

- **Transferpriorität**

  Die Priorität, mit der die Übertragung ausgeführt wird. Sie können entweder „Normal“ oder „Niedrig“

auswählen. Beziehungen mit Richtlinien, die eine normale Übertragungspriorität angeben, werden vor denen mit Richtlinien ausgeführt, die eine niedrige Übertragungspriorität angeben.

- **Maximale Übertragungsrate**

  Gibt die maximale Rate an, mit der Daten 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 (KBps), Megabyte pro Sekunde (MBps), Gigabyte pro Sekunde (GBps) oder TBps auswählen. Wenn Sie keine maximale Übertragungsrate verwenden möchten, ist die Basisübertragung zwischen Beziehungen unbegrenzt.

Registerkarte „Quell-Snapshot-Kopien“

Auf der Registerkarte „Quell-Snapshot-Kopien“ werden die folgenden Informationen zur Quell-Snapshot-Kopie angezeigt, die für die Baseline-Übertragung verwendet wird:

- **Quellvolumen**

  Zeigt die Namen der entsprechenden Quellvolumes an.

- **Zielvolumen**

  Zeigt die Namen der ausgewählten Zielvolumes an.

- **Quellentyp**

  Zeigt den Datenträgertyp an: entweder Lesen/Schreiben oder Datenschutz.

- **Schnappschusskopie**

  Zeigt die Snapshot-Kopie an, die für die Datenübertragung verwendet wird. Wenn Sie auf den Wert „Snapshot-Kopie“ klicken, wird das Dialogfeld „Quellen-Snapshot-Kopie auswählen“ angezeigt, in dem Sie je nach Art Ihrer Schutzbeziehung und der von Ihnen ausgeführten Operation eine bestimmte Snapshot-Kopie für Ihre Übertragung auswählen können.

Befehlsschaltflächen

- **Einreichen**

  Startet den Resynchronisierungsprozess und schließt das Dialogfeld „Resynchronisieren“.

- **Stornieren**

  Bricht Ihre Auswahl ab und schließt das Dialogfeld „Neu synchronisieren“.

Dialogfeld „Quell-Snapshot-Kopie auswählen“

Sie verwenden das Dialogfeld „Quell-Snapshot-Kopie auswählen“, um eine bestimmte Snapshot-Kopie zum Übertragen von Daten zwischen Schutzbeziehungen auszuwählen, oder Sie wählen das Standardverhalten aus, das davon abhängt, ob Sie eine Beziehung initialisieren, aktualisieren oder neu synchronisieren und ob es sich bei der Beziehung um einen SnapMirror oder SnapVault handelt.

Standard

Ermöglicht Ihnen, das Standardverhalten auszuwählen, um zu bestimmen, welche Snapshot-Kopie zum Initialisieren, Aktualisieren und erneuten Synchronisieren von Übertragungen für SnapVault und SnapMirror -Beziehungen verwendet wird.

Wenn Sie eine SnapVault -Übertragung durchführen, ist das Standardverhalten für jeden Vorgang wie folgt:

Betrieb	**Standardmäßiges SnapVault -Verhalten, wenn die Quelle Lese-/Schreibzugriff hat**	**Standardmäßiges SnapVault -Verhalten, wenn die Quelle Datenschutz (DP) ist**
Initialisieren	Erstellt eine neue Snapshot-Kopie und überträgt sie.	Überträgt die zuletzt exportierte Snapshot-Kopie.
Aktualisieren	Überträgt nur gekennzeichnete Snapshot-Kopien, wie in der Richtlinie angegeben.	Überträgt die zuletzt exportierte Snapshot-Kopie.
Neu synchronisieren	Überträgt alle gekennzeichneten Snapshot-Kopien, die nach der neuesten gemeinsamen Snapshot-Kopie erstellt wurden.	Überträgt die neueste beschriftete Snapshot-Kopie.

Wenn Sie eine SnapMirror -Übertragung durchführen, ist das Standardverhalten für jeden Vorgang wie folgt:

Betrieb	**Standardmäßiges SnapMirror -Verhalten**	**Standardmäßiges SnapMirror Verhalten, wenn die Beziehung der zweite Hop in einer SnapMirror zu SnapMirror Kaskade ist**
Initialisieren	Erstellt eine neue Snapshot-Kopie und überträgt diese und alle Snapshot-Kopien, die vor der neuen Snapshot-Kopie erstellt wurden.	Überträgt alle Snapshot-Kopien von der Quelle.
Aktualisieren	Erstellt eine neue Snapshot-Kopie und überträgt diese und alle Snapshot-Kopien, die vor der neuen Snapshot-Kopie erstellt wurden.	Überträgt alle Snapshot-Kopien.
Neu synchronisieren	Erstellt eine neue Snapshot-Kopie und überträgt dann 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-Kopie

Ermöglicht Ihnen, eine vorhandene Snapshot-Kopie aus der Liste auszuwählen, wenn die Auswahl einer Snapshot-Kopie für diesen Vorgang zulässig ist.

- **Schnappschusskopie**

  Zeigt die vorhandenen Snapshot-Kopien an, aus denen Sie für eine Übertragung auswählen können.

- **Erstellungsdatum**

  Zeigt das Datum und die Uhrzeit der Erstellung der Snapshot-Kopie an. Snapshot-Kopien werden in der Reihenfolge der aktuellsten bis zur ältesten aufgelistet, wobei die aktuellsten ganz oben in der Liste stehen.

Wenn Sie eine SnapVault Übertragung durchführen und eine vorhandene Snapshot-Kopie auswählen möchten, um sie von einer Quelle zu einem Ziel zu übertragen, ist das Verhalten für jeden Vorgang 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 der Quell-Snapshot-Kopie wird für Datensicherungsvolumes nicht unterstützt.
Aktualisieren	Überträgt die angegebene Snapshot-Kopie.	Die Auswahl der Quell-Snapshot-Kopie wird für Datensicherungsvolumes nicht unterstützt.
Neu synchronisieren	Überträgt die ausgewählte Snapshot-Kopie.	Die Auswahl der Quell-Snapshot-Kopie wird für Datensicherungsvolumes nicht unterstützt.

Wenn Sie eine SnapMirror Übertragung durchführen und eine vorhandene Snapshot-Kopie auswählen möchten, um sie von einer Quelle zu einem Ziel zu übertragen, ist 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 der Quelle bis zur angegebenen Snapshot-Kopie.	Die Auswahl der Quell-Snapshot-Kopie wird für Datensicherungsvolumes nicht unterstützt.

Betrieb	SnapMirror -Verhalten beim Angeben einer Snapshot-Kopie	SnapMirror -Verhalten beim Angeben einer Snapshot-Kopie in einer Kaskade
Aktualisieren	Überträgt alle Snapshot-Kopien auf der Quelle bis zur angegebenen Snapshot-Kopie.	Die Auswahl der Quell-Snapshot-Kopie wird für Datensicherungsvolumes nicht unterstützt.
Neu synchronisieren	Überträgt alle Snapshot-Kopien von der Quelle bis zur ausgewählten Snapshot-Kopie und löscht dann alle Daten, die nach der Erstellung der neuesten gemeinsamen Snapshot-Kopie hinzugefügt wurden.	Die Auswahl der Quell-Snapshot-Kopie wird für Datensicherungsvolumes nicht unterstützt.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden 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“.

Dialogfeld „Umgekehrte Neusynchronisierung“

Wenn eine Schutzbeziehung unterbrochen wird, weil das Quellvolume deaktiviert und das Ziel zu einem Lese-/Schreibvolume gemacht wurde, können Sie mit der umgekehrten Neusynchronisierung die Richtung der Beziehung umkehren, sodass das Ziel zur neuen Quelle und die Quelle zum neuen Ziel wird.

Wenn das Quellvolume in Ihrer Schutzbeziehung durch einen Notfall deaktiviert wird, können Sie das Zielvolume zum Bereitstellen von Daten verwenden, indem Sie es in einen Lese-/Schreibdatenträger konvertieren, während Sie die Quelle reparieren oder ersetzen, die Quelle aktualisieren und die Beziehung wiederherstellen. Wenn Sie einen umgekehrten Resynchronisierungsvorgang durchführen, werden Daten auf der Quelle gelöscht, die neuer sind als die Daten auf der gemeinsamen Snapshot-Kopie.

Vor der umgekehrten Neusynchronisierung

Zeigt die Quelle und das Ziel einer Beziehung vor einem umgekehrten Resynchronisierungsvorgang an.

- **Quellvolumen**

  Der Name und der Speicherort des Quellvolumes vor einem umgekehrten Resynchronisierungsvorgang.

- **Zielvolumen**

Der Name und der Speicherort des Zielvolumes vor einem umgekehrten Resynchronisierungsvorgang.

Nach der umgekehrten Neusynchronisierung

Zeigt die Quelle und das Ziel einer Beziehung nach einem Reserve-Resynchronisierungsvorgang an.

- **Quellvolumen**

  Der Name und der Speicherort des Quellvolumes nach einem umgekehrten Resynchronisierungsvorgang.

- **Zielvolumen**

  Der Name und der Speicherort des Zielvolumes nach einem umgekehrten Resynchronisierungsvorgang.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie die folgenden Aktionen ausführen:

- **Einreichen**

  Startet den umgekehrten Resynchronisierungsprozess.

- **Stornieren**

  Schließt das Dialogfeld „Reverse Resync“, ohne einen Reverse Resync-Vorgang zu starten.

Beziehung: Ansicht „Alle Beziehungen“

In der Ansicht „Beziehung: Alle Beziehungen“ werden Informationen zu Schutzbeziehungen auf dem Speichersystem angezeigt.

Wenn Sie auf die Seite „Beziehungen“ zugreifen, enthält der angezeigte Bericht standardmäßig die Schutzbeziehungen der obersten Ebene für Volumes und Speicher-VMs. Mit den Steuerelementen oben auf der Seite können Sie eine bestimmte Ansicht auswählen, Suchen durchführen, um bestimmte Objekte zu finden, Filter erstellen und anwenden, um die Liste der angezeigten Daten einzugrenzen, Spalten auf der Seite hinzufügen/entfernen/neu anordnen und die Daten auf der Seite in eine CSV-, PDF- oder XLSX-Datei exportieren. Nachdem Sie die Seite angepasst haben, können Sie die Ergebnisse als benutzerdefinierte Ansicht speichern und dann einen Bericht dieser Daten planen, der regelmäßig generiert und per E-Mail versendet wird. Wenn Sie das Menü **Beziehungen** auswählen, enthält der angezeigte Bericht standardmäßig Schutzbeziehungen sowohl für Volumes als auch für Speicher-VMs in Ihrem Rechenzentrum. Sie können die Option **Filter** verwenden, um nur ausgewählte Speichersysteme anzuzeigen, z. B. nur Volumes oder nur Speicher-VMs. Derselbe Bericht wird auf der Speicherseite und nur für die ausgewählte Speichereinheit angezeigt. Wenn Sie Volume- oder Speicher-VM-Beziehungen anzeigen möchten, können Sie entweder auf die Seite **Speicher** > **Volumes** > **Beziehung: Alle Beziehungen** zugreifen oder auf **Schutz** > **Beziehungen** > **Beziehung: Alle Beziehungen** und die Option **Beziehungsobjekttyp** im **Filter** verwenden, um nur Volume- oder Speicher-VM-Daten herauszufiltern.

Die Seite „Beziehungen“, auf der alle Schutzbeziehungen aufgelistet sind, enthält den Link **Im System Manager anzeigen** für den Zielcluster, mit dem Sie dieselben Objekte im ONTAP System Manager anzeigen können.

- **Status**

  Zeigt den aktuellen Status der Schutzbeziehung an.

Der Status kann einer von Fehler ( ), Warnung ( ) oder OK ( ).

- **Quellspeicher-VM**

  Zeigt den Namen der Quell-SVM an. Sie können weitere Details zur Quell-SVM anzeigen, indem Sie auf den SVM-Namen klicken.

  Wenn im Cluster ein SVM vorhanden ist, aber noch nicht zum Unified Manager-Inventar hinzugefügt wurde, oder wenn das SVM nach der letzten Aktualisierung des Clusters erstellt wurde, ist dieses Feld leer. Sie müssen sicherstellen, dass die SVM vorhanden ist, oder eine erneute Erkennung des Clusters durchführen, um die Liste der Ressourcen zu aktualisieren.

- **Quelle**

  Zeigt je nach Ihrer Auswahl entweder das Quellvolume oder die Quellspeicher-VM an, die geschützt wird. Sie können weitere Details zum Quellvolume oder zur Speicher-VM anzeigen, indem Sie auf den Namen des Volumes oder der Speicher-VM klicken.

  Wenn die Nachricht `Resource-key not discovered` angezeigt wird, kann dies darauf hinweisen, dass das Volume im Cluster vorhanden ist, aber noch nicht zum Unified Manager-Inventar hinzugefügt wurde, oder dass das Volume nach der letzten Aktualisierung des Clusters erstellt wurde. Sie müssen sicherstellen, dass das Volume vorhanden ist, oder eine erneute Erkennung des Clusters durchführen, um die Liste der Ressourcen zu aktualisieren.

- **Zielspeicher-VM**

  Zeigt den Namen der Ziel-SVM an. Sie können weitere Details zum Ziel-SVM anzeigen, indem Sie auf den SVM-Namen klicken.

- **Ziel**

  Zeigt den Namen des Zielvolumes oder der Speicher-VM basierend auf Ihrer Auswahl an. Weitere Details zum Zielvolume bzw. zur Speicher-VM können Sie durch Klicken auf den jeweiligen Objektnamen anzeigen.

- **Beziehungsobjekttyp**

  Zeigt den in der Beziehung verwendeten Objekttyp an, z. B. Speicher-VM, Volume und Konsistenzgruppe. Bei Objekten in einer Konsistenzbeziehung wird in der Quelle und den Zielen der Beziehung die Konsistenzgruppe angezeigt. Durch Klicken darauf gelangen Sie zur Seite „LUNs“, um die Beziehung anzuzeigen.

- **Politik**

  Zeigt den Namen der Schutzrichtlinie für die SnapMirror -Beziehung an. Sie können auf den Richtliniennamen klicken, um die mit dieser Richtlinie verknüpften Details anzuzeigen, einschließlich der folgenden Informationen:

  - Übertragungspriorität

    Gibt die Priorität an, 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. Die Standardeinstellung ist „Normal“.

  - Zugriffszeit ignorieren

Gilt nur für SnapVault -Beziehungen. Hiermit wird festgelegt, ob bei inkrementellen Übertragungen Dateien ignoriert werden, bei denen sich nur die Zugriffszeit geändert hat. Die Werte sind entweder „True“ oder „False“. Der Standardwert ist „False“.

- Wenn die Beziehung nicht im Einklang ist

  Gibt die Aktion an, die ONTAP ausführt, wenn eine synchrone Beziehung nicht synchronisiert werden kann. StrictSync-Beziehungen beschränken den Zugriff auf das primäre Volume, wenn die Synchronisierung mit dem sekundären Volume fehlschlägt. Synchronisierungsbeziehungen schränken den Zugriff auf das Primärsystem nicht ein, wenn die Synchronisierung mit dem Sekundärsystem fehlschlägt.

- Versuchslimit

  Gibt die maximale Anzahl von Versuchen für jede manuelle oder geplante Übertragung einer SnapMirror -Beziehung an. Der Standardwert ist 8.

- Kommentare

  Bietet ein Textfeld für Kommentare, die sich speziell auf die ausgewählte Richtlinie beziehen.

- SnapMirror -Etikett

  Gibt die SnapMirror -Bezeichnung für den ersten Zeitplan an, der mit der Snapshot-Kopierrichtlinie verknüpft ist. Das SnapMirror -Label wird vom SnapVault Subsystem verwendet, wenn Sie Snapshot-Kopien auf einem SnapVault -Ziel sichern.

- Aufbewahrungseinstellung

  Gibt an, wie lange Sicherungen aufbewahrt werden, basierend auf der Zeit oder der Anzahl der Sicherungen.

- Tatsächliche Snapshot-Kopien

  Gibt die Anzahl der Snapshot-Kopien auf diesem Volume an, die mit der angegebenen Bezeichnung übereinstimmen.

- Snapshot-Kopien aufbewahren

  Gibt die Anzahl der SnapVault -Snapshot-Kopien an, die nicht automatisch gelöscht werden, selbst wenn das maximale Limit für die Richtlinie erreicht ist. Die Werte sind entweder „True“ oder „False“. Der Standardwert ist „False“.

- Schwellenwert für Aufbewahrungswarnung

  Gibt das Limit für Snapshot-Kopien an, bei dem eine Warnung gesendet wird, dass das maximale Aufbewahrungslimit fast erreicht ist.

- **Lag-Dauer**

  Zeigt die Zeitspanne an, um die die Daten auf dem Spiegel hinter der Quelle zurückliegen.

  Die Verzögerungsdauer sollte für StrictSync-Beziehungen nahe 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 sein:

- Fehler

  Die Verzögerungsdauer ist größer oder gleich dem Verzögerungsfehlerschwellenwert.

- Warnung

  Die Verzögerungsdauer ist größer oder gleich dem Verzögerungswarnschwellenwert.

- OK

  Die Verzögerungsdauer liegt im normalen Rahmen.

- Nicht zutreffend

  Der Verzögerungsstatus ist für synchrone Beziehungen nicht anwendbar, da kein Zeitplan konfiguriert werden kann.

- **Letztes erfolgreiches Update**

  Zeigt den Zeitpunkt des letzten erfolgreichen SnapMirror oder SnapVault -Vorgangs an.

  Das letzte erfolgreiche Update ist für synchrone Beziehungen nicht anwendbar.

- **Konstituierende Beziehungen**

  Zeigt an, ob im ausgewählten Objekt Datenträger vorhanden sind.

- **Beziehungstyp**

  Zeigt den Beziehungstyp an, der zum Replizieren eines Volumes verwendet wird. Zu den Beziehungstypen gehören:

  - Asynchroner Spiegel
  - Asynchroner Tresor
  - Asynchroner 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 ein Übertragungsabbruchvorgang ausgeführt, der möglicherweise die Entfernung des Prüfpunkts umfasst.

  - Überprüfung

    Das Zielvolume wird einer Diagnoseprüfung unterzogen und es findet keine Übertragung statt.

- Finalisieren

  SnapMirror Übertragungen sind aktiviert. Das Volume befindet sich derzeit in der Nachübertragungsphase für inkrementelle SnapVault Übertragungen.

- Leerlauf

  Übertragungen sind aktiviert und es findet keine Übertragung statt.

- Synchron

  Die Daten in den beiden Volumes in der synchronen Beziehung werden synchronisiert.

- Nicht synchron

  Die Daten im Zielvolume werden nicht mit dem Quellvolume synchronisiert.

- Vorbereitung

  SnapMirror Übertragungen sind aktiviert. Das Volume befindet sich derzeit in der Vorübertragungsphase für inkrementelle SnapVault Übertragungen.

- In der Warteschlange

  SnapMirror Übertragungen sind aktiviert. Es sind keine Überweisungen im Gange.

- Ruhezustand

  SnapMirror -Übertragungen sind deaktiviert. Es ist keine Übertragung im Gange.

- Stilllegung

  Eine SnapMirror -Übertragung ist im Gange. Weitere Übertragungen sind deaktiviert.

- Übertragen

  SnapMirror Übertragungen sind aktiviert und eine Übertragung ist im Gange.

- Übergang

  Die asynchrone Datenübertragung vom Quell- zum Zieldatenträger ist abgeschlossen und der Übergang zum synchronen Betrieb hat begonnen.

- Warten

  Eine SnapMirror Übertragung wurde eingeleitet, aber einige zugehörige Aufgaben warten darauf, in die Warteschlange gestellt zu werden.

- **Dauer der letzten Übertragung**

  Zeigt die Zeit an, die bis zum Abschluss der letzten Datenübertragung verstrichen ist.

  Die Übertragungsdauer ist für StrictSync-Beziehungen nicht anwendbar, da die Übertragung gleichzeitig erfolgen sollte.

- **Letzte Übertragungsgröße**

Zeigt die Größe der letzten Datenübertragung in Bytes an.

Die Übertragungsgröße ist für StrictSync-Beziehungen nicht anwendbar.

- **Mediatoren**

  Zeigt den Mediatorstatus an.

  - Nicht zutreffend

    Wenn der Cluster SnapMirror Active Sync nicht unterstützt.

  - Nicht konfiguriert

    Wenn es nicht konfiguriert ist oder wenn es konfiguriert ist, aber nur der Zielcluster hinzugefügt wird und der Quellcluster nicht in Unified Manager hinzugefügt wird.

  - Mediator-IP-Adresse

    Wenn es konfiguriert ist und sowohl Quell- als auch Zielcluster in Unified Manager hinzugefügt werden.

- **Zustand**

  Zeigt den Status der SnapMirror oder SnapVault -Beziehung an. Der Status kann „Nicht initialisiert“, „SnapMirrored“ oder „Abgebrochen“ sein. Wenn ein Quellvolume ausgewählt ist, ist der Beziehungsstatus nicht anwendbar und wird nicht angezeigt.

- **Beziehungsgesundheit**

  Zeigt den Beziehungszustand des Clusters an.

- **Ungesunder Grund**

  Der Grund dafür ist, dass die Beziehung in einem ungesunden Zustand ist.

- **Transferpriorität**

  Zeigt die Priorität an, mit der eine Übertragung ausgeführt wird. Die Übertragungspriorität ist Normal oder Niedrig. Übertragungen mit normaler Priorität werden vor Übertragungen mit niedriger Priorität geplant.

  Bei synchronen Beziehungen ist die Übertragungspriorität nicht anwendbar, da alle Übertragungen mit der gleichen Priorität behandelt werden.

- **Zeitplan**

  Zeigt den Namen des der Beziehung zugewiesenen Schutzzeitplans an.

  Der Zeitplan ist nicht auf synchrone Beziehungen anwendbar.

- **Version Flexible Replikation**

  Zeigt entweder „Ja“, „Ja mit Sicherungsoption“ oder „Keine“ an.

- **Quellcluster**

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Quellclusters für die SnapMirror -Beziehung an.

- **Quellcluster-FQDN**

  Zeigt den Namen des Quellclusters für die SnapMirror -Beziehung an.

- **Quellknoten**

  Zeigt den Namen des Quellknotennamen-Links für die SnapMirror -Beziehung eines Volumes an und zeigt den Link zur Knotenanzahl der SnapMirror -Beziehung an, wenn es sich bei dem Objekt um eine Storage-VM oder eine Konsistenzgruppe handelt.

Wenn Sie in der benutzerdefinierten Ansicht auf den Link zum Knotennamen klicken, können Sie den Schutz für Speicherobjekte anzeigen und erweitern, bei denen die Volumes dieser Konsistenzgruppen zu einer SnapMirror Active Sync-Beziehung gehören.

Wenn Sie auf den Link zur Knotenanzahl klicken, gelangen Sie zur Knotenseite mit den entsprechenden Knoten, die dieser Beziehung zugeordnet sind. Wenn die Knotenanzahl 0 ist, wird kein Wert angezeigt, da der Beziehung keine Knoten zugeordnet sind.

- **Zielknoten**

  Zeigt den Namen des Zielknotennamen-Links für die SnapMirror -Beziehung eines Volumes an und zeigt den Link zur Knotenanzahl der SnapMirror -Beziehung an, wenn es sich bei dem Objekt um eine Storage-VM oder eine Konsistenzgruppe handelt.

  Wenn Sie auf den Link zur Knotenanzahl klicken, gelangen Sie zur Knotenseite mit den entsprechenden Knoten, die dieser Beziehung zugeordnet sind. Wenn die Knotenanzahl 0 ist, wird kein Wert angezeigt, da der Beziehung keine Knoten zugeordnet sind.

- **Zielcluster**

  Zeigt den Namen des Zielclusters für die SnapMirror -Beziehung an.

- **Zielcluster-FQDN**

  Zeigt den FQDN, den Kurznamen oder die IP-Adresse des Zielclusters für die SnapMirror -Beziehung an.

- **Geschützt durch**

  Zeigt die verschiedenen Beziehungen an. In dieser Spalte können Sie Volume- und Konsistenzgruppenbeziehungen für Cluster und die Reihenfolge virtueller Speichermaschinen anzeigen, einschließlich:

  - SnapMirror
  - Speicher-VM-DR
  - SnapMirror, Speicher-VM-DR
  - Konsistenzgruppe
  - SnapMirror, Konsistenzgruppe.

Verwandte Informationen

- Informationen zur Ansicht **Relationship: MetroCluster** finden Sie unter"Überwachung von MetroCluster -Konfigurationen" .

- Informationen zur Ansicht **Beziehung: Transferstatus des letzten Monats** finden Sie unter"Beziehung: Ansicht des Übertragungsstatus des letzten Monats" .
- Informationen zur Ansicht **Beziehung: Alle Beziehungen** finden Sie unter"Beziehung: Ansicht der Übertragungsrate des letzten Monats" .

Beziehung: Ansicht des Übertragungsstatus des letzten Monats

Mit der Ansicht „Beziehung: Übertragungsstatus des letzten Monats“ können Sie die Übertragungstrends über einen bestimmten Zeitraum für Volumes und Speicher-VMs in asynchronen Beziehungen analysieren. Auf dieser Seite wird auch angezeigt, ob die Übertragung erfolgreich war oder fehlgeschlagen ist.

Mit den Steuerelementen oben auf der Seite können Sie Suchen durchführen, um bestimmte Objekte zu finden, Filter erstellen und anwenden, um die Liste der angezeigten Daten einzugrenzen, Spalten auf der Seite hinzufügen/entfernen/neu anordnen und die Daten auf der Seite in ein `.csv` , `.pdf` , oder `.xlsx` Datei. Nachdem Sie die Seite angepasst haben, können Sie die Ergebnisse als benutzerdefinierte Ansicht speichern und dann einen Bericht dieser Daten planen, der regelmäßig generiert und per E-Mail versendet wird. Sie können die Option **Filter** verwenden, um nur ausgewählte Speichersysteme anzuzeigen, z. B. nur Volumes oder nur Speicher-VMs. Derselbe Bericht wird auf der Speicherseite und nur für die ausgewählte Speichereinheit angezeigt. Wenn Sie beispielsweise Volume-Beziehungen anzeigen möchten, können Sie entweder über das Menü **Speicher** > **Speicher-VMs** > **Beziehung: Übertragungsstatus des letzten Monats** oder über das Menü **Schutz** > **Beziehungen** > **Beziehung: Übertragungsstatus des letzten Monats** auf den Bericht „Beziehung: Übertragungsstatus des letzten Monats“ für die Storage-VMs zugreifen und den **Filter** verwenden, um nur Daten für Volumes anzuzeigen.

- **Quellvolumen**

  Zeigt den Namen des Quellvolumes an.

- **Zielvolumen**

  Zeigt den Namen des Zielvolumes an.

- **Operationstyp**

  Zeigt die Art der Volumenübertragung an.

- **Operationsergebnis**

  Zeigt an, ob die Volumeübertragung erfolgreich war.

- **Übertragungsstartzeit**

  Zeigt die Startzeit der Volumeübertragung an.

- **Endzeit der Übertragung**

  Zeigt die Endzeit der Volumeübertragung an.

- **Transferdauer**

  Zeigt die Zeit (in Stunden) an, die zum Abschließen der Volumeübertragung benötigt wurde.

- **Übertragungsgröße**

Zeigt die Größe (in MB) des übertragenen Datenträgers an.

- **Quelle SVM**

  Zeigt den Namen der virtuellen Speichermaschine (SVM) an.

- **Quellcluster**

  Zeigt den Namen des Quellclusters an.

- **Ziel-SVM**

  Zeigt den Ziel-SVM-Namen an.

- **Zielcluster**

  Zeigt den Namen des Zielclusters an.

Verwandte Informationen

- Informationen zur Ansicht **Beziehung: Alle Beziehungen** finden Sie unter"Beziehung: Ansicht „Alle Beziehungen“" .
- Informationen zur Ansicht **Relationship: MetroCluster** finden Sie unter"Überwachung von MetroCluster -Konfigurationen" .
- Informationen zur Ansicht **Beziehung: Alle Beziehungen** finden Sie unter"Beziehung: Ansicht der Übertragungsrate des letzten Monats" .

Beziehung: Ansicht der Übertragungsrate des letzten Monats

Mit der Ansicht „Beziehung: Übertragungsrate des letzten Monats“ können Sie das täglich übertragene Datenvolumen für Datenträger in asynchronen Beziehungen analysieren. Auf dieser Seite finden Sie auch Einzelheiten zu den täglichen Übertragungen und zur Zeit, die zum Abschließen des Übertragungsvorgangs für Volumes und Storage-VMs erforderlich ist.

Mit den Steuerelementen oben auf der Seite können Sie Suchvorgänge durchführen, um bestimmte Objekte zu finden, Filter erstellen und anwenden, um die Liste der angezeigten Daten einzugrenzen, Spalten auf der Seite hinzufügen/entfernen/neu anordnen und die Daten auf der Seite in eine CSV-, PDF- oder XLSX-Datei exportieren. Nachdem Sie die Seite angepasst haben, können Sie die Ergebnisse als benutzerdefinierte Ansicht speichern und dann einen Bericht dieser Daten planen, der regelmäßig generiert und per E-Mail versendet wird. Wenn Sie beispielsweise Volume-Beziehungen anzeigen möchten, können Sie entweder auf das Menü **Speicher** > **Volumes** > **Beziehung: Übertragungsrate des letzten Monats** zugreifen oder auf das Menü **Schutz** > **Beziehungen** > **Beziehungen: Übertragungsrate des letzten Monats** und den **Filter** verwenden, um nur Daten für Volumes anzuzeigen.

- **Gesamtübertragungsgröße**

  Zeigt die Gesamtgröße der Volumeübertragung in Gigabyte an.

- **Tag**

  Zeigt den Tag an, an dem die Volumenübertragung initiiert wurde.

- **Endzeit**

  Zeigt die Endzeit der Volumenübertragung mit Datum an.

Verwandte Informationen

- Informationen zur Ansicht **Relationship: MetroCluster** finden Sie unter"Überwachung von MetroCluster -Konfigurationen" .
- Informationen zur Ansicht **Beziehung: Transferstatus des letzten Monats** finden Sie unter"Beziehung: Ansicht des Übertragungsstatus des letzten Monats" .
- Informationen zur Ansicht **Beziehung: Alle Beziehungen** finden Sie unter"Beziehung: Ansicht der Übertragungsrate des letzten Monats"

Erstellen Sie benutzerdefinierte Berichte

Einheitliche Manager-Berichterstellung

Active IQ Unified Manager (früher OnCommand Unified Manager) bietet die Möglichkeit, Berichte für Ihre ONTAP Speichersysteme anzuzeigen, anzupassen, herunterzuladen und zu planen. Die Berichte können Einzelheiten zu Kapazität, Zustand, Leistung, Sicherheit und Schutzbeziehungen des Speichersystems liefern.

Die neue Berichts- und Planungsfunktion von Unified Manager, die in Active IQ Unified Manager 9.6 eingeführt wurde, ersetzt die vorherige Berichts-Engine, die in Unified Manager Version 9.5 eingestellt wurde.

Die Berichterstellung bietet verschiedene Ansichten Ihres Netzwerks und liefert verwertbare Informationen zu Kapazität, Integrität, Leistung, Sicherheit und Schutzdaten. Sie können Ihre Ansichten anpassen, indem Sie Spalten ein- und ausblenden und neu anordnen, Daten filtern, Daten sortieren und die Ergebnisse durchsuchen. Sie können benutzerdefinierte Ansichten zur Wiederverwendung speichern, sie als Berichte herunterladen und sie als wiederkehrende Berichte zur Verteilung per E-Mail planen.

Sie können Ansichten im Microsoft® Excel-Format herunterladen und anpassen. Sie können erweiterte Excel-Funktionen wie komplexe Sortierungen, mehrschichtige Filter, Pivot-Tabellen und Diagramme verwenden. Wenn Sie mit dem resultierenden Excel-Bericht zufrieden sind, können Sie die Excel-Datei hochladen, um sie bei jeder Planung und Freigabe des Berichts zu verwenden.

Zusätzlich zum Erstellen von Berichten über die Benutzeroberfläche können Sie mithilfe dieser zusätzlichen Methoden Integritäts-, Sicherheits- und Leistungsdaten aus Unified Manager extrahieren:

- Verwenden von Open Database Connectivity (ODBC) und ODBC-Tools für den direkten Zugriff auf die Datenbank für Clusterinformationen
- Ausführen von Unified Manager REST-APIs, um die Informationen zurückzugeben, die Sie überprüfen möchten

Ab dieser Version von Active IQ Unified Manager wurden die folgenden Verbesserungen an den Berichten vorgenommen:

- Für einen Bericht wird gemäß dem konfigurierten Zeitplan eine E-Mail gesendet. Auch wenn Sie einen On-Demand-Bericht erstellen, erhalten Sie eine E-Mail.
- Der Dateiname des Berichts und die Metadaten des Berichts enthalten den Hostnamen, von dem aus der Bericht generiert wurde. Selbst wenn jemand den Dateinamen ändert, können Sie dank dieser Verbesserung immer noch den Hostnamen identifizieren, von dem der Bericht generiert wurde.

Zugriffspunkte zum Erstellen von Berichten

Sie können im Unified Manager Informationen zu Ihren Clustern sammeln, um Berichte aus der Benutzeroberfläche, MySQL-Datenbankabfragen und REST-APIs zu erstellen.

In diesen Abschnitten werden die Berichterstellung und Planung von Unified Manager über die Benutzeroberfläche beschrieben.

Es gibt drei Möglichkeiten, auf die Berichtsfunktionen von Unified Manager zuzugreifen:

- Extrahieren Sie Daten direkt von den Inventarseiten in der Benutzeroberfläche.

- Verwenden Sie Open Database Connectivity (ODBC) und ODBC-Tools, um auf alle verfügbaren Objekte zuzugreifen.
- Ausführen von Unified Manager REST-APIs, um die Informationen zurückzugeben, die Sie überprüfen möchten.

In diesen Abschnitten werden die Berichterstellung und Planung von Unified Manager über die Benutzeroberfläche beschrieben.

Unified Manager-Datenbanken für benutzerdefinierte Berichte zugänglich

Unified Manager verwendet eine MySQL-Datenbank, um Daten aus den Clustern zu speichern, die es überwacht. Daten werden in verschiedenen Schemata in der MySQL-Datenbank gespeichert.

Alle Tabellendaten stehen aus folgenden Datenbanken zur Verfügung:

Datenbank	Beschreibung
netapp_model	Daten zu den Objekten auf ONTAP -Controllern.
netapp_model_view	Daten zu den Objekten auf ONTAP -Controllern, geeignet für die Nutzung von Berichtstools.
netapp_performance	Clusterspezifische Leistungsindikatoren.
ocum	Unified Manager-Anwendungsdaten und -Informationen zur Unterstützung der UI-Filterung, Sortierung und Berechnung einiger abgeleiteter Felder.
ocum_report	Daten zur Bestandskonfiguration und kapazitätsbezogene Informationen.
ocum_report_birt	Ansichten für die Inventarkonfiguration und kapazitätsbezogene Daten, geeignet für die Nutzung von Berichtstools.
opm	Leistungskonfigurationseinstellungen und Schwellenwertinformationen.
Waagenmonitor	Daten zur Integrität und Leistungsproblemen der Unified Manager-Anwendung.
VMware-Modell	VMware-Objektdaten für auf NetApp -Speicher gehostete Datenspeicher.
vmware_model_view	Ansichten für VMware-Objektdaten für auf NetApp -Speicher gehostete Datenspeicher, geeignet für die Nutzung von Berichtstools.

Datenbank	Beschreibung
vmware_performance	VMware-Leistungsindikatordaten für auf NetApp -Speicher gehostete Datenspeicher.

Ein Berichtsbenutzer – ein Datenbankbenutzer mit der Rolle „Berichtsschema“ – kann auf die Daten in diesen Tabellen zugreifen. Dieser Benutzer hat schreibgeschützten Zugriff auf Berichte und andere Datenbankansichten direkt aus der Unified Manager-Datenbank. Beachten Sie, dass dieser Benutzer keine Berechtigung zum Zugriff auf Tabellen hat, die Benutzerdaten oder Cluster-Anmeldeinformationen enthalten.

Unified Manager REST-APIs, die für die Berichterstellung verwendet werden können

Sie können REST-APIs zur Verwaltung Ihrer Cluster verwenden, indem Sie die von Unified Manager erfassten Informationen zu Integrität, Kapazität, Leistung und Sicherheit anzeigen.

REST-APIs werden über die Swagger-Webseite bereitgestellt. Sie können auf die Swagger-Webseite zugreifen, um die Unified Manager REST-API-Dokumentation anzuzeigen und manuell einen API-Aufruf zu tätigen. Klicken Sie in der Unified Manager-Web-Benutzeroberfläche in der Menüleiste auf die Schaltfläche **Hilfe** und wählen Sie dann **API-Dokumentation** aus. Informationen zu Unified Manager REST-APIs finden Sie unter"Erste Schritte mit Active IQ Unified Manager REST-APIs" .

Sie müssen über die Rolle „Operator“, „Speicheradministrator“ oder „Anwendungsadministrator“ verfügen, um auf die REST-APIs zugreifen zu können.

Berichte verstehen

Berichte zeigen detaillierte Informationen zu Speicher, Netzwerk, Dienstqualität und Schutzbeziehungen an und helfen Ihnen, potenzielle Probleme zu erkennen und zu lösen, bevor sie auftreten.

Wenn Sie eine Ansicht anpassen, können Sie sie für die zukünftige Verwendung unter einem eindeutigen Namen speichern. Sie können einen auf dieser Ansicht basierenden Bericht so planen, dass er regelmäßig ausgeführt wird, und ihn mit anderen teilen. Sie können die Ansicht auch in Excel herunterladen, um sie mit erweiterten Excel-Funktionen anzupassen, und die Datei dann wieder in Unified Manager hochladen. Wenn Sie einen Bericht mit dieser Ansicht planen, wird die von Ihnen hochgeladene Excel-Datei verwendet, um aussagekräftige Berichte zu erstellen, die Sie weitergeben können.

Sie können alle geplanten Berichte auf der Seite „Berichtszeitpläne“ verwalten.

> Zum Verwalten von Berichten müssen Sie über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Sie können Berichte als durch Kommas getrennte Werte (CSV), Excel- oder PDF-Dateien herunterladen.

Verstehen der Ansichts- und Berichtsbeziehung

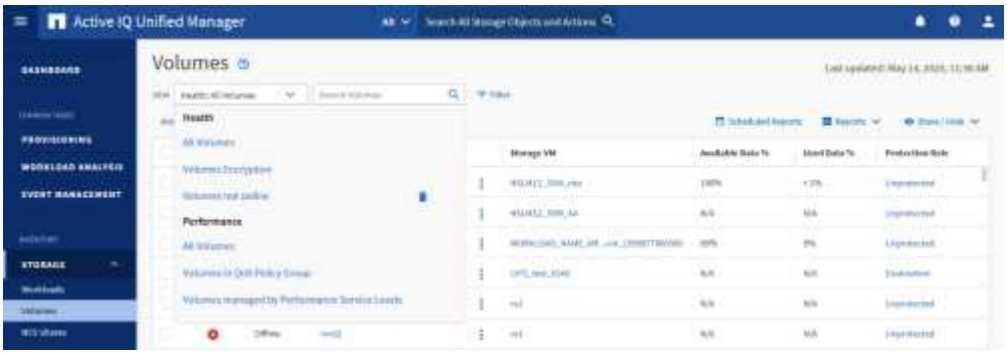
Ansichten und Inventarseiten werden zu Berichten, wenn Sie sie herunterladen oder planen.

Sie können Ansichten und Inventarseiten anpassen und zur Wiederverwendung speichern. Fast alles, was Sie

in Unified Manager anzeigen können, kann als Bericht gespeichert, wiederverwendet, angepasst, geplant und freigegeben werden.

In der Dropdown-Liste „Ansicht“ handelt es sich bei Elementen mit dem Löschsymbol um 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, wird die Änderung in Berichten, die diese Ansicht verwenden, beim nächsten Generieren des Berichts und Versenden per E-Mail gemäß dem Berichtszeitplan angezeigt. Achten Sie beim Ändern der Ansichten darauf, dass Ihre Änderungen mit allen zugehörigen Excel-Anpassungen funktionieren, die für die Berichte verwendet werden. 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 „Anwendungsadministrator“ oder „Speicheradministrator“ können das Löschsymbol sehen, eine Ansicht ändern oder löschen oder einen geplanten Bericht ändern oder löschen.

Berichtstypen

Diese Tabelle enthält eine umfassende Liste der Ansichten und Inventarseiten, die als Berichte verfügbar sind, die Sie anpassen, herunterladen und planen können.

Active IQ Unified Manager Berichte

Typ	Speicher- oder Netzwerkobjekt
Kapazität	Cluster Aggregate Bände Qtrees

Typ	Speicher- oder Netzwerkobjekt
Systemzustand	Cluster Nodes Aggregate Speicher-VMs Bände SMB/CIFS-Freigaben NFS-Freigaben
Performance	Cluster Nodes Aggregate Speicher-VMs Bände LUNs NVMe-Namespaces Netzwerkschnittstellen (LIFs) Häfen
Servicequalität	Herkömmliche QoS-Richtliniengruppen Adaptive QoS-Richtliniengruppen Richtliniengruppen für Leistungsservicelevel
Volume-Schutzbeziehungen (verfügbar auf der Seite „Volumes“)	Alle Beziehungen Transferstatus des letzten Monats Transferrate des letzten Monats
Sicherheit	Speicher-VMs Cluster

Berichtseinschränkungen

Es gibt einige Einschränkungen bei der neuen Berichtsfunktion von Active IQ Unified Manager, die Sie kennen sollten.

Vorhandene Berichte aus früheren Versionen von Unified Manager

Sie können den Zeitplan und die Empfänger nur für vorhandene Berichte bearbeiten, die in Unified Manager 9.5 und früheren Versionen erstellt und importiert wurden (als .rptdesign-Dateien). Wenn Sie einen der Standardberichte angepasst haben, die mit Unified Manager 9.5 oder früher bereitgestellt wurden, werden diese benutzerdefinierten Berichte nicht in das neue Berichtstool importiert.

Wenn Sie vorhandene Berichte bearbeiten müssen, die aus .rptdesign-Dateien importiert wurden, führen Sie einen der folgenden Schritte aus und entfernen Sie den importierten Bericht:

- Erstellen Sie eine neue Ansicht und planen Sie einen Bericht aus dieser Ansicht (bevorzugt)
- Bewegen Sie den Mauszeiger über den Bericht, kopieren Sie die SQL und ziehen Sie die Daten mit einem externen Tool

Die Standardansichten können ohne Anpassung als Berichte generiert werden. Mit der neuen Berichtslösung können Sie beliebige benutzerdefinierte Berichte neu erstellen.

Zeitplan- und Berichtsbeziehung

Sie können für jeden gespeicherten Bericht viele verschiedene Zeitpläne mit beliebigen Empfängerkombinationen erstellen. Sie können den Zeitplan jedoch nicht für mehrere Berichte wiederverwenden.

Berichtsschutz

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.

Veranstaltungsberichte

Obwohl Sie die Ereignisansicht anpassen und den resultierenden Bericht im CSV-Format herunterladen können, ist es nicht möglich, die Erstellung und Verteilung wiederkehrender Ereignisberichte zu planen.

Berichtsanhänge

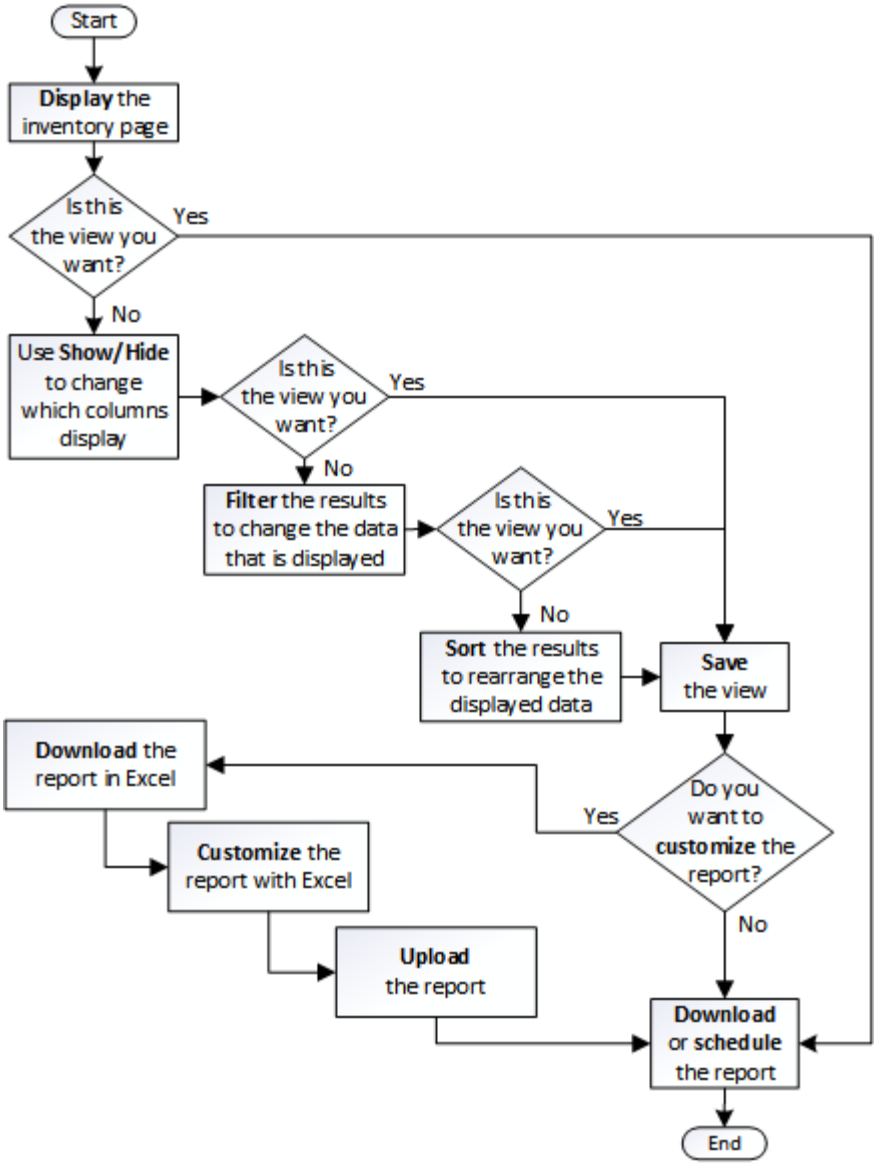
Berichte können nicht im Text einer E-Mail gesendet werden. Stattdessen werden Berichte nur als PDF-, Excel- oder CSV-Anhänge gesendet.

Arbeiten mit Berichten

Erfahren Sie, wie Sie Inventarseitenansichten finden und in gemeinsam nutzbare, geplante Berichte umwandeln.

Berichtsworkflow

Entscheidungsbaum, der den Berichts-Workflow beschreibt.



Schnellstart zur Berichterstellung

Erstellen Sie einen benutzerdefinierten Beispielbericht, um das Erkunden von Ansichten und Planen von Berichten zu erleben. Dieser Schnellstartbericht enthält eine Liste von Volumes, die Sie möglicherweise in die Cloud-Ebene verschieben möchten, da dort eine beträchtliche Menge inaktiver (kalter) Daten vorhanden ist. Sie öffnen die Ansicht „Leistung: Alle Volumes“, passen die Ansicht mithilfe von Filtern und Spalten an, speichern die benutzerdefinierte Ansicht als Bericht und planen die wöchentliche Freigabe des Berichts.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen FabricPool Aggregate konfiguriert haben und über Volumes auf diesen Aggregaten verfügen.

Führen Sie die folgenden Schritte aus, um:

- Öffnen der Standardansicht

- Passen Sie die Spalten an, indem Sie die Daten filtern und sortieren
- Speichern der Ansicht
- Planen Sie die Generierung eines Berichts für die benutzerdefinierte Ansicht

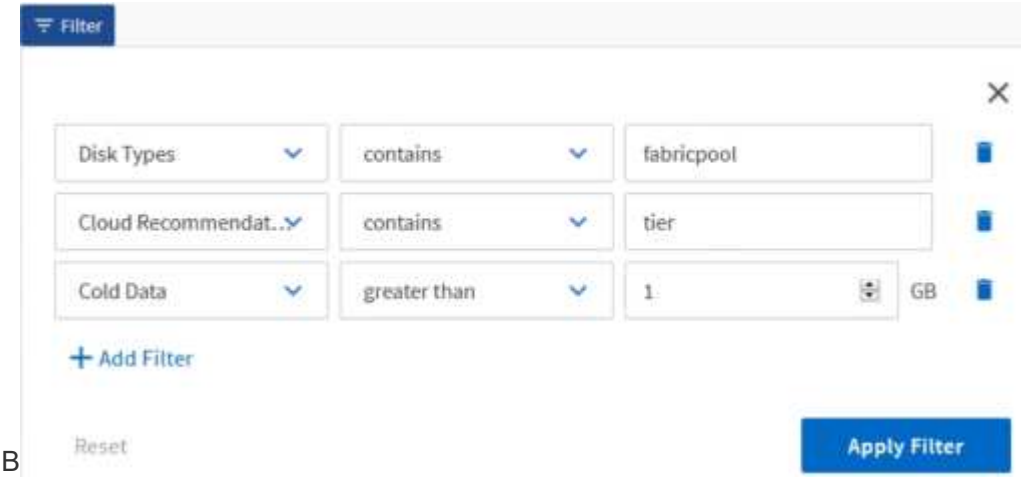
Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Leistung“ > „Alle Volumes“ aus.
3. Klicken Sie auf **Anzeigen/Ausblenden**, um sicherzustellen, dass die Spalte „Datenträgertypen“ in der Ansicht angezeigt wird.

   Fügen Sie weitere Spalten hinzu oder entfernen Sie sie, um eine Ansicht zu erstellen, die die für Ihren Bericht wichtigen Felder enthält.

4. Ziehen Sie die Spalte „Datenträgertypen“ neben die Spalte „Cloud-Empfehlung“.
5. Klicken Sie auf das Filtersymbol, um die folgenden drei Filter hinzuzufügen, und klicken Sie dann auf **Filter anwenden**:

   - Datenträgertypen enthalten FabricPool
   - Cloud-Empfehlung enthält Stufe
   - Kalte Daten größer als 10



GB

   Beachten Sie, dass jeder Filter mit einem logischen UND verknüpft ist, sodass alle zurückgegebenen Bände alle Kriterien erfüllen müssen. Sie können maximal fünf Filter hinzufügen.

6. Klicken Sie oben auf die Spalte „Kalte Daten“, um die Ergebnisse so zu sortieren, dass die Volumes mit den meisten kalten Daten oben in der Ansicht angezeigt werden.
7. Wenn die Ansicht angepasst ist, lautet der Ansichtsname „Nicht gespeicherte Ansicht“. Benennen Sie die Ansicht so, dass sie widerspiegelt, was in der Ansicht angezeigt wird, z. B. „Vols ändern Tiering-Richtlinie“. Wenn Sie fertig sind, klicken Sie auf das Häkchen oder drücken Sie die Eingabetaste, um die Ansicht unter dem neuen Namen zu speichern.

8. Laden Sie den Bericht als **CSV**-, **Excel**- oder **PDF**-Datei herunter, um die Ausgabe anzuzeigen, bevor Sie sie planen oder freigeben.

   Öffnen Sie die Datei mit einer installierten Anwendung, beispielsweise Microsoft Excel (CSV oder Excel) oder Adobe Acrobat (PDF), oder speichern Sie die Datei.

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, verwenden Sie die erweiterten Funktionen, um Ihren Bericht anzupassen. Wenn Sie zufrieden sind, laden Sie die Excel-Datei hoch. Diese Datei wird mit ihren Anpassungen auf die Ansicht angewendet, wenn der Bericht ausgeführt wird.

Weitere Informationen zum Anpassen von Berichten mit Excel finden Sie unter *Beispielberichte zu Microsoft Excel*.

9. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**. In der Liste werden alle geplanten Berichte angezeigt, die sich auf das Objekt, in diesem Fall Volumes, beziehen.

10. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
11. Geben Sie einen Namen für den Bericht ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

    Der folgende Beispielbericht liegt im CSV-Format vor:

    Der folgende Beispielbericht liegt im PDF-Format vor:

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise ONTAP System Manager oder die ONTAP CLI verwenden, um die Tiering-Richtlinie für bestimmte Volumes auf „auto“ oder „all“ zu ändern, um mehr kalte Daten in die Cloud-Ebene auszulagern.

Suchen nach einem geplanten Bericht

Sie können nach geplanten Berichten nach Name, Ansichtsname, Objekttyp oder Empfänger suchen.

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Berichtszeitpläne**.
2. Verwenden Sie das Textfeld **Geplante Berichte suchen**.

So finden Sie Berichte von …	Versuchen …
Zeitplanname	Geben Sie einen Teil des Berichtszeitplannamens ein.
Ansichtsname	Geben Sie einen Teil des Berichtsansichtsnamens ein. Standardansichten und benutzerdefinierte Ansichten werden in der Ansichtsliste angezeigt.
Empfänger	Geben Sie einen Teil der E-Mail-Adresse ein.

So finden Sie Berichte von …	Versuchen …
Dateityp	Geben Sie „PDF“, „CSV“ oder „XLSX“ ein.

3. Sie können auf eine Spaltenüberschrift klicken, um Berichte in aufsteigender oder absteigender Reihenfolge nach dieser Spalte zu sortieren, beispielsweise nach Zeitplanname oder Format.

Berichte anpassen

Es gibt viele Möglichkeiten, Ansichten anzupassen, sodass Sie einen Bericht erstellen können, der alle Informationen enthält, die Sie zur Verwaltung Ihrer ONTAP Cluster benötigen.

Beginnen Sie mit einer Standardinventarseite oder einer benutzerdefinierten Ansicht und passen Sie sie dann an, 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 in Excel herunterladen, um sie mit erweiterten Funktionen anzupassen. Wenn Sie fertig sind, laden Sie die angepasste Excel-Datei hoch. Wenn Sie einen Bericht mit dieser Ansicht planen, wird die angepasste Excel-Datei verwendet, um robuste Berichte zu erstellen, die Sie weitergeben können.

Weitere Informationen zum Anpassen von Berichten mit Excel finden Sie unter *Beispielberichte zu Microsoft Excel*.

Zum Verwalten von Berichten müssen Sie über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Spalten anpassen

Verwenden Sie **Anzeigen/Ausblenden**, um die Spalten auszuwählen, die Sie in Ihrem Bericht verwenden möchten. Ziehen Sie die Spalten auf der Inventarseite, um sie neu anzuordnen.

Schritte

1. Klicken Sie auf **Anzeigen/Ausblenden**, um Spalten hinzuzufügen oder zu entfernen.
2. Ziehen Sie auf der Inventarseite die Spalten, um sie in der gewünschten Reihenfolge für Ihren Bericht anzuordnen.
3. Benennen Sie die nicht gespeicherte Ansicht, um Ihre Änderungen zu speichern.

Daten filtern

Filtern Sie die Daten, um sicherzustellen, dass die Ergebnisse Ihren Berichtsanforderungen entsprechen. Durch Filtern können Sie nur die Daten anzeigen, die Sie interessieren.

Schritte

1. Klicken Sie auf das Filtersymbol, um Filter hinzuzufügen und die Ergebnisse einzugrenzen, die Sie

anzeigen möchten, und klicken Sie dann auf **Filter anwenden**.

2. Benennen Sie die nicht gespeicherte Ansicht, um Ihre Änderungen zu speichern.

Daten sortieren

Um die Ergebnisse zu sortieren, klicken Sie auf eine Spalte und geben Sie die aufsteigende oder absteigende Reihenfolge an. Durch das Sortieren der Daten werden die Informationen priorisiert, die Sie für den Bericht benötigen.

Schritte

1. Klicken Sie auf den oberen Rand einer Spalte, um die Ergebnisse so zu sortieren, dass die wichtigsten Informationen oben in der Ansicht angezeigt werden.
2. Benennen Sie die nicht gespeicherte Ansicht, um Ihre Änderungen zu speichern.

Verwenden der Suche zum Verfeinern Ihrer Ansicht

Nachdem Sie die gewünschte Ansicht erhalten haben, können Sie die Ergebnisse mithilfe des Suchfelds weiter verfeinern, um sich auf die Ergebnisse zu konzentrieren, die Sie in den Bericht aufnehmen möchten.

Schritte

1. Öffnen Sie die benutzerdefinierte oder Standardansicht, die Sie als Grundlage für Ihren Bericht verwenden möchten.
2. Geben Sie in das Suchfeld ein, um die in der Ansicht aufgelisteten Daten zu verfeinern. Sie können in jede der angezeigten Spalten Teildaten eingeben. Wenn Sie beispielsweise nach Knoten suchen möchten, deren Name „US_East“ enthält, können Sie die vollständige Liste der Knoten verfeinern.

   Die Ergebnisse Ihrer Suche werden in der benutzerdefinierten Ansicht gespeichert und im resultierenden geplanten Bericht verwendet.

3. Benennen Sie die nicht gespeicherte Ansicht, um Ihre Änderungen zu speichern.

Verwenden Sie Excel, um Ihren Bericht anzupassen

Nachdem Sie die Ansicht gespeichert haben, können Sie sie im Excel-Arbeitsmappenformat (.xlsx) herunterladen. Wenn Sie die Excel-Datei öffnen, können Sie erweiterte Excel-Funktionen verwenden, um Ihren Bericht anzupassen.

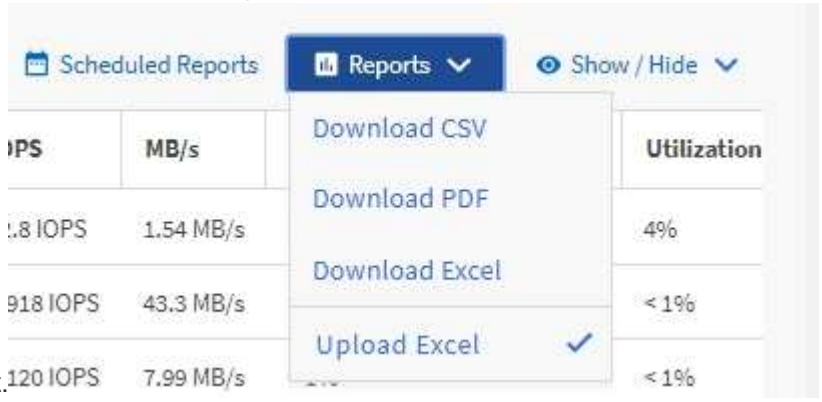
Bevor Sie beginnen

Sie können nur eine Excel-Arbeitsmappendatei mit der Erweiterung .xlsx hochladen.

Zu den erweiterten Excel-Funktionen, die Sie in Ihrem Bericht verwenden können, gehören beispielsweise:

- Mehrspaltige Sortierung
- Komplexe Filterung
- Pivot-Tabellen
- Diagramme

- Die heruntergeladene Excel-Datei verwendet den Standarddateinamen für die Ansicht, nicht Ihren gespeicherten Namen.
  - Das Format ist `<View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx`.
  - Beispielsweise eine benutzerdefinierte gespeicherte Ansicht mit dem Namen `Volumes-not online` hat einen Dateinamen von `health-volumes-05-May-2020-19-18-00.xlsx` wenn an diesem Tag und zu dieser Uhrzeit gespeichert.
- Sie können der Excel-Datei Blätter hinzufügen, vorhandene Blätter jedoch nicht ändern.
  - Verändern Sie die vorhandenen Blätter, Daten und Informationen nicht. Kopieren Sie die Daten stattdessen auf eine neue Seite, die Sie erstellen.
  - Eine Ausnahme von der obigen Regel besteht darin, dass Sie auf der Seite „Daten“ Formeln erstellen können. Verwenden Sie die Datenseitenformeln, um Diagramme auf neuen Seiten zu erstellen.
  - Geben Sie einem neuen Blatt keine Daten oder Informationen.
- Wenn eine benutzerdefinierte Excel-Datei vorhanden ist, ist neben dem Menüpunkt **Berichte** > **Excel hochladen** ein Häkchen angezeigt. Beim Download der Excel-Datei wird die Version mit den Anpassungen



verwendet.

Schritte

1. Öffnen Sie die Standardansicht, die benutzerdefinierte oder die gespeicherte Ansicht, die Sie als Grundlage für Ihren Bericht verwenden möchten.
2. Wählen Sie **Berichte** > **Excel herunterladen**.
3. Speichern Sie die Datei. Die Datei wird in Ihrem Download-Ordner gespeichert.
4. Öffnen Sie die gespeicherte Datei in Excel. Verschieben Sie die Datei nicht an einen neuen Speicherort. Wenn Sie Ihre Arbeit an einem anderen Ort erledigen, speichern Sie die Datei vor dem Hochladen unter dem ursprünglichen Dateinamen wieder am ursprünglichen Speicherort.
5. Passen Sie die Datei mithilfe von Excel-Funktionen wie komplexen Sortierungen, mehrschichtigen Filtern, Pivot-Tabellen oder Diagrammen an. Weitere Informationen finden Sie in der Microsoft® Excel-Dokumentation.
6. Wählen Sie **Berichte** > **Excel hochladen** und wählen Sie die Datei aus, die Sie geändert haben. Die zuletzt heruntergeladene Datei wird vom selben Dateispeicherort hochgeladen.
7. Senden Sie sich selbst einen Testbericht mit der Funktion **Geplante Berichte**.

Berichte herunterladen

Sie können Berichte herunterladen und die Daten als CSV-Datei (Comma-Separated Values), Microsoft Excel-Datei (.XLSX) oder PDF-Datei auf einem lokalen Laufwerk oder einem Netzwerklaufwerk speichern. Sie können CSV- und XLSX-Dateien mit Tabellenkalkulationsprogrammen wie Microsoft Excel und PDF-Dateien mit Leseprogrammen wie Adobe Acrobat öffnen.

Schritte

1. Klicken Sie auf die Schaltfläche **Berichte**, um den Bericht auf eine der folgenden Arten herunterzuladen:

Wählen	Zu…
CSV herunterladen	Speichern Sie den Bericht als CSV-Datei (Comma-Separated Values).
PDF herunterladen	Speichern Sie den Bericht als PDF-Datei.
Excel herunterladen	Speichern Sie den Bericht als Microsoft Excel-Datei (XLSX).

Berichte planen

Nachdem Sie eine Ansicht erstellt haben, die Sie wiederverwenden und als Bericht freigeben möchten, können Sie sie mit Active IQ Unified Manager planen. Sie können geplante Berichte verwalten und die Empfänger und die Verteilungshäufigkeit für jeden Berichtszeitplan ändern.

Sie können die meisten Ansichten oder Inventarseiten im Unified Manager planen. Ausnahmen sind Ereignisse. Dabei handelt es sich um Berichte, die Sie als CSV-Dateien herunterladen können. Sie können jedoch keine Ereignisse zur Neugenerierung und Freigabe planen. Sie können die Dashboards, Favoriten oder Konfigurationsseiten auch nicht herunterladen oder planen.

Ab Active IQ Unified Manager 9.8 können Sie Ansichten im Microsoft® Excel-Format herunterladen und anpassen. Sie können erweiterte Excel-Funktionen wie komplexe Sortierungen, Ebenenfilter, Pivot-Tabellen und Diagramme verwenden. Wenn Sie mit dem resultierenden Excel-Bericht zufrieden sind, können Sie die Excel-Datei hochladen, um sie bei jeder Planung und Freigabe des Berichts zu verwenden.

Sie können die integrierten Ansichten oder die von Ihnen angepassten Ansichten planen. Sie können den zu sendenden Dateityp auswählen: CSV, PDF oder XSLX. Wenn Sie einen Bericht zum ersten Mal planen, können Sie ihn herunterladen und sich selbst als einzigen Empfänger festlegen, der den Bericht sehen kann, so wie ihn auch Ihre Empfänger sehen werden.

Planen eines Berichts

Nachdem Sie eine Ansicht oder Excel-Datei erstellt haben, deren regelmäßige Generierung und Verteilung Sie planen möchten, können Sie den Bericht planen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen die SMTP-Servereinstellungen auf der Seite **Allgemein** > **Benachrichtigungen** konfiguriert haben, damit die Berichts-Engine Berichte als E-Mail-Anhänge vom Unified Manager-Server an die Empfängerliste senden kann.
- Der E-Mail-Server muss so konfiguriert sein, dass das Senden von Anhängen mit den generierten E-Mails möglich ist.

Führen Sie die folgenden Schritte aus, um einen für eine Ansicht zu erstellenden Bericht zu testen und zu planen. Wählen Sie die gewünschte Ansicht aus oder passen Sie sie an. Das folgende Verfahren verwendet eine Netzwerkansicht, die die Leistung Ihrer Netzwerkschnittstellen anzeigt. Sie können jedoch jede beliebige Ansicht verwenden.

Schritte

1. Öffnen Sie Ihre Ansicht. In diesem Beispiel wird die Standardnetzwerkansicht verwendet, die die LIF-Leistung zeigt. Klicken Sie im linken Navigationsbereich auf **Netzwerk > Netzwerkschnittstellen**.
2. Passen Sie die Ansicht nach Bedarf mit den integrierten Unified Manager-Funktionen an.
3. Nachdem Sie die Ansicht angepasst haben, können Sie im Feld **Ansicht** einen eindeutigen Namen eingeben und auf das Häkchen klicken, um sie zu speichern.
4. Sie können die erweiterten Funktionen von Microsoft® Excel verwenden, um Ihren Bericht anzupassen. Weitere Einzelheiten finden Sie unter"Verwenden von Excel zum Anpassen Ihres Berichts" .
5. So sehen Sie sich die Ausgabe an, bevor Sie sie planen oder freigeben:

Option	Beschreibung
Wenn Sie Excel zum Anpassen des Berichts verwendet haben	Zeigen Sie die vorhandene heruntergeladene Excel-Datei an.
Wenn Sie Excel nicht zum Anpassen des Berichts verwendet haben	Laden Sie den Bericht als **CSV**-, **PDF**- oder **XLSX** -Datei herunter.

   Öffnen Sie die Datei mit einer installierten Anwendung, beispielsweise Microsoft Excel (CSV/XSLX) oder Adobe Acrobat (PDF).

6. Wenn Sie mit dem Bericht zufrieden sind, klicken Sie auf **Geplante Berichte**.
7. Klicken Sie auf der Seite „Berichtszeitpläne“ auf **Zeitplan hinzufügen**.
8. Akzeptieren Sie den Standardnamen, der eine Kombination aus Ansichtsname und Häufigkeit ist, oder passen Sie den **Zeitplannamen** an.
9. Um den geplanten Bericht das erste Mal zu testen, fügen Sie sich selbst nur als **Empfänger** hinzu. Wenn Sie zufrieden sind, fügen Sie die E-Mail-Adressen aller Berichtsempfänger hinzu.
10. Geben Sie an, wie oft der Bericht erstellt und an die Empfänger gesendet werden soll. Sie können **Täglich**, **Wöchentlich** oder **Monatlich** wählen.
11. Wählen Sie das Format aus, entweder **PDF**, **CSV** oder **XSLX**.

> Wählen Sie für Berichte, bei denen Sie Excel zum Anpassen des Inhalts verwendet haben, immer **XSLX** aus.

12. Klicken Sie auf das Häkchen ( ), um den Berichtszeitplan zu speichern.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht erstellt und in der geplanten Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Planen Sie importierte .rptdesign-Berichte

Sie können vorhandene Berichte planen, die in einer früheren Version von Unified Manager erstellt und importiert wurden.

Für die Planung importierter Berichte ist Folgendes erforderlich:

- importierte BIRT-entworfene .rptdesign-Dateiberichte 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 auf der Seite „Berichtszeitpläne“ die importierten Berichte aufgelistet. Sie können den Zeitplan für diese Berichte bearbeiten, um die E-Mail-Adressen der Empfänger, die Häufigkeit und das Format (PDF oder CSV) anzugeben. Andernfalls können diese Berichte in der Unified Manager-Benutzeroberfläche nicht bearbeitet oder angezeigt werden.

Schritte

1. Öffnen Sie die Seite „Berichtszeitpläne“. Wenn Sie Berichte importiert haben, wird eine Meldung angezeigt.
2. Klicken Sie auf den Namen **Ansicht**, um die SQL-Abfrage anzuzeigen, die zum Generieren des Berichts verwendet wird.
3. Klicken Sie auf das Symbol „Mehr“ , klicken Sie auf **Bearbeiten**, definieren Sie die Details des Berichtszeitplans und speichern Sie den Bericht.

   Sie können auch alle unerwünschten Berichte über das Symbol „Mehr“ löschen. .

Berichtszeitpläne verwalten

Sie können Ihre Berichtszeitpläne auf der Seite „Berichtszeitpläne“ verwalten. Sie können vorhandene Zeitpläne anzeigen, ändern oder löschen.

Bevor Sie beginnen

Sie können auf der Seite „Berichtszeitpläne“ keine neuen Berichte planen. Sie können geplante Berichte nur von den Objektinventarseiten hinzufügen.

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Berichtszeitpläne**.
2. Auf der Seite „Berichtszeitpläne“:

Wenn Sie wollen…	Dann…
Einen vorhandenen Zeitplan anzeigen	Blättern Sie mithilfe der Bildlaufleisten und Seitensteuerelemente durch die Liste der vorhandenen Berichte.
Bearbeiten eines vorhandenen Zeitplans	a. Klicken Sie auf das Symbol „Mehr“ für den Zeitplan, den Sie verwenden möchten. b. Klicken Sie auf **Bearbeiten**. c. Nehmen Sie die erforderlichen Änderungen vor. d. Klicken Sie auf das Häkchen, um Ihre Änderungen zu speichern.
Löschen eines vorhandenen Zeitplans	a. Klicken Sie auf das Symbol „Mehr“ für den Zeitplan, den Sie verwenden möchten. b. Klicken Sie auf **Löschen**. c. Bestätigen Sie Ihre Entscheidung.

Geplante Berichte bearbeiten

Nachdem Berichte geplant wurden, können Sie sie auf der Seite „Berichtszeitpläne“ bearbeiten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Berichtszeitpläne**.

> Wenn Sie über die entsprechenden Berechtigungen verfügen, können Sie jeden Bericht und seinen Zeitplan im System ändern.

2. Klicken Sie auf das Symbol „Mehr“ für den Zeitplan, den Sie ändern möchten.
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, klicken Sie auf das Häkchen, um Ihre Änderungen zu speichern.

Geplante Berichte löschen

Nachdem Berichte geplant wurden, können Sie sie auf der Seite „Berichtszeitpläne“ löschen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicherverwaltung** > **Berichtszeitpläne**.

   Wenn Sie über die entsprechenden Berechtigungen verfügen, können Sie jeden Bericht und seinen Zeitplan im System entfernen.

2. Klicken Sie auf das Symbol „Mehr“ für den Zeitplan, den Sie entfernen möchten.
3. Klicken Sie auf **Löschen**.
4. Bestätigen Sie Ihre Entscheidung.

   Der geplante Bericht wird aus der Liste entfernt und nicht mehr gemäß 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.

Beispiele für benutzerdefinierte Berichte

Diese benutzerdefinierten Beispielberichte werden häufig verwendet, um Ihnen dabei zu helfen, potenzielle Probleme zu erkennen und auf potenzielle Probleme zu reagieren, bevor sie auftreten.

Die Liste der Berichte in diesem Abschnitt ist nicht vollständig und wird mit der Zeit erweitert. Sie können benutzerdefinierte Berichte vorschlagen, die diesem Abschnitt hinzugefügt werden sollen, indem Sie Feedback zur Dokumentation geben.

Zum Verwalten von Berichten müssen Sie über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Anpassen von Cluster-Speicherberichten

Die Beispielberichte zum Clusterspeicher in diesem Abschnitt sind lediglich Beispiele, die Ihnen dabei helfen sollen, zu verstehen, wie Sie Berichte zur Clusterkapazität erstellen, die Ihnen bei der Überwachung Ihrer Speichersystemressourcen helfen.

Erstellen Sie einen Bericht, um die Kapazität nach Clustermodell anzuzeigen

Sie können einen Bericht erstellen, um die Speicherkapazität und Auslastung von Clustern basierend auf dem Speichersystemmodell zu analysieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die die Kapazität nach

Clustermodell anzeigt, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Cluster**.
2. Wählen Sie im Menü „Ansicht“ die Option „Kapazität“ > „Alle Cluster“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten, z. B. „Cluster-FQDN“ und „Betriebssystemversion“.
4. Ziehen Sie die „Gesamtrohkapazität“, das „Modell/Familie“ und die drei aggregierten Spalten in die Nähe der Spalte „Cluster“.
5. Klicken Sie oben auf die Spalte „Modell/Familie“, um die Ergebnisse nach Clustertyp zu sortieren.
6. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Kapazität nach Clustermodell“.
7. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
8. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtszeitpläne** eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
9. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise bestimmten Clustern mehr Kapazität hinzufügen oder ältere Clustermodelle aktualisieren.

Erstellen Sie einen Bericht, um Cluster mit der größten nicht zugewiesenen LUN-Kapazität zu identifizieren

Sie können einen Bericht erstellen, um die Cluster mit der größten nicht zugewiesenen LUN-Kapazität (über 0,5 TB) zu ermitteln und so zu ermitteln, wo Sie zusätzliche Workloads hinzufügen können.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die Cluster mit der größten nicht zugewiesenen LUN-Kapazität anzeigt, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Cluster**.
2. Wählen Sie im Menü „Ansicht“ die Option „Kapazität“ > „Alle Cluster“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Ziehen Sie die Spalte „Nicht zugewiesene LUN-Kapazität“ in die Nähe der Spalte „HA-Paar“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Nicht zugewiesene LUN-Kapazität größer als 0,5 TB

6. Klicken Sie oben auf die Spalte „Nicht zugewiesene LUN-Kapazität“, um die Ergebnisse nach der größten Menge nicht zugewiesener LUN-Kapazität zu sortieren.
7. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Größte nicht zugewiesene LUN-Kapazität“, und klicken Sie auf das Häkchen ( ).
8. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise die nicht zugewiesene LUN-Kapazität des Clusters verwenden.

Erstellen Sie einen Bericht, um HA-Paare mit der größten verfügbaren Kapazität anzuzeigen

Sie können einen Bericht erstellen, um die Hochverfügbarkeitspaare (HA) mit der größten Kapazität zum Bereitstellen neuer Volumes und LUNs zu finden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, in der HA-Paare nach der größten verfügbaren Kapazität sortiert angezeigt werden, um neue Volumes und LUNs bereitzustellen. Planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Cluster**.
2. Wählen Sie im Menü „Ansicht“ die Option „Kapazität“ > „Alle Cluster“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Ziehen Sie die Spalte „Aggregierte ungenutzte Kapazität“ in die Nähe der Spalte „HA-Paar“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
    - Gesamte ungenutzte Kapazität größer als 0,5 TB
6. Klicken Sie oben auf die Spalte „Ungenutzte Gesamtkapazität“, um die Ergebnisse nach der größten ungenutzten Gesamtkapazität zu sortieren.
7. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Am wenigsten genutzte Gesamtkapazität“, und klicken Sie auf das Häkchen ( ).
8. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der

angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise HA-Paare basierend auf der Gesamtkapazität ausgleichen.

Erstellen Sie einen Bericht, um Knoten anzuzeigen, auf denen ältere Versionen von ONTAP ausgeführt werden

Sie können einen Bericht erstellen, um die Version der ONTAP -Software anzuzeigen, die auf allen Clusterknoten installiert ist, sodass Sie sehen können, welche Knoten Sie aktualisieren sollten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die Knoten mit älteren Versionen von ONTAP anzeigt, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Knoten**.
2. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
3. Ziehen Sie die Spalte „Betriebssystemversion“ in die Nähe der Spalte „Knoten“.
4. Klicken Sie oben auf die Spalte „Betriebssystemversion“, um die Ergebnisse nach der ältesten ONTAP-Version zu sortieren.
5. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Knoten nach ONTAP -Version“.
6. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
7. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
8. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise Knoten aktualisieren, auf denen ältere Versionen von ONTAP ausgeführt werden.

Anpassen aggregierter Kapazitätsberichte

Diese benutzerdefinierten Beispielberichte sollen Ihnen dabei helfen, potenzielle Probleme im Zusammenhang mit der Gesamtspeicherkapazität zu erkennen und darauf zu reagieren.

Die Berichte in diesem Abschnitt sind lediglich Beispiele, die Ihnen dabei helfen sollen, zu verstehen, wie Sie Berichte über die Gesamtkapazität erstellen, um die Ressourcen Ihres Speichersystems zu überwachen.

Erstellen Sie einen Bericht, um anzuzeigen, wann Aggregate ihre volle Kapazität erreichen

Sie können einen Bericht erstellen, um die Aggregate zu ermitteln, die ihre volle Kapazität erreichen, sodass Sie mehr Kapazität hinzufügen oder Arbeitslasten auf andere Aggregate verschieben können.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die Aggregate anzeigt, die ihre volle Kapazität erreichen, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.
2. Wählen Sie im Menü „Ansicht“ die Option „Kapazität“ > „Alle Aggregate“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Tage bis zur vollständigen Fertigstellung weniger als 45 Tage
5. Klicken Sie oben auf die Spalte „Tage bis zur vollen Kapazität“, um die Ergebnisse nach der geringsten Anzahl von Tagen zu sortieren, die bis zum Erreichen der vollen Kapazität verbleiben.
6. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Tage bis zur vollen Gesamtkapazität“, und klicken Sie auf das Häkchen ( ).
7. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
8. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtszeitpläne** eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
9. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise den Speicher auf Aggregaten erhöhen, die ihre volle Kapazität erreichen. Darüber hinaus möchten Sie möglicherweise den Schwellenwert „Tage bis zur vollen Kapazität“ auf mehr als die standardmäßigen 7 Tage erhöhen, damit Sie Ereignisse erhalten, die Ihnen mehr Zeit geben, auf knapp werdenden Speicherplatz in Aggregaten zu reagieren.

Erstellen Sie einen Bericht, 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

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die Aggregate anzeigt, die zu 80 % oder mehr gefüllt sind, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.
2. Wählen Sie im Menü „Ansicht“ die Option „Kapazität“ > „Alle Aggregate“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Ziehen Sie die Spalten „Verfügbare Daten %“ und „Verwendete Daten %“ in die Nähe der Spalte „Aggregat“.
5. Klicken Sie auf das Filtersymbol, fügen Sie die folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Der Prozentsatz der verwendeten Daten liegt über 80 %
6. Klicken Sie oben auf die Spalte „Verwendete Daten %“, um die Ergebnisse nach Kapazitätsprozentsatz zu sortieren.
7. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Aggregate fast voll“, und klicken Sie auf das Häkchen ( ) .
8. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise einige Daten aus bestimmten Aggregaten verschieben.

Erstellen Sie einen Bericht, um überbelegte Aggregate anzuzeigen

Sie können einen Bericht erstellen, um die Speicherkapazität und die Verwendung von Aggregaten zu analysieren und überbelegte Aggregate anzuzeigen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die Aggregate anzeigt, die den Überlastungsschwellenwert überschreiten, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.
2. Wählen Sie im Menü „Ansicht“ die Option „Kapazität“ > „Alle Aggregate“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Ziehen Sie die Spalte „Überbelegte Kapazität %“ in die Nähe der Spalte „Aggregat“.
5. Klicken Sie auf das Filtersymbol, fügen Sie die folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Überbelegte Kapazität in % ist größer als 100 %

6. Klicken Sie oben auf die Spalte „Überbelegte Kapazität %“, um die Ergebnisse nach Kapazitätsprozentsatz zu sortieren.
7. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Aggregate überbelegt“, und klicken Sie auf das Häkchen ( ).
8. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise die Kapazität der Aggregate erhöhen oder einige Daten aus bestimmten Aggregaten verschieben.

Anpassen von Volume-Kapazitätsberichten

Diese benutzerdefinierten Beispielberichte sollen Ihnen dabei helfen, potenzielle Probleme im Zusammenhang mit der Volumekapazität und -leistung zu erkennen und darauf zu reagieren.

Erstellen Sie einen Bericht, um Volumes zu identifizieren, die sich der vollen Kapazität nähern und bei denen die automatische Löschung von Snapshots deaktiviert ist.

Sie können einen Bericht erstellen, der die Liste der Volumes enthält, die sich der vollen Kapazität nähern, wenn die Funktion „Automatisches Löschen von Snapshots“ deaktiviert ist. Die Ergebnisse können dabei helfen, Volumes zu identifizieren, bei denen Sie möglicherweise Snapshot Autodelete konfigurieren möchten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, in der die erforderlichen Spalten in der richtigen Reihenfolge angezeigt werden, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Kapazität“ > „Alle Volumes“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Ziehen Sie die Spalten „Snapshot Autodelete“ und „Days To Full“ per Drag & Drop in die Nähe der Spalte „Verfügbare Datenkapazität“.
5. Klicken Sie auf das Filtersymbol, fügen Sie die folgenden zwei Filter hinzu und klicken Sie dann auf **Filter anwenden**:
    - Tage bis zur vollständigen Fertigstellung weniger als 30 Tage
    - Automatisches Löschen von Snapshots ist deaktiviert

6. Klicken Sie oben auf die Spalte **Tage bis zur Vollendung**, sodass die Datenträger mit den wenigsten verbleibenden Tagen oben in der Liste angezeigt werden.
7. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Vols near capacity“.
8. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
9. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise die automatische Löschung von Snapshots auf den Volumes aktivieren oder eine Möglichkeit finden, den verfügbaren Speicherplatz zu erhöhen.

Erstellen Sie einen Bericht, um den Speicherplatz zu ermitteln, der von Volumes mit deaktiviertem Thin Provisioning verwendet wird

Wenn für ein Volume kein Thin Provisioning durchgeführt wird, nimmt es den gesamten Speicherplatz auf der Festplatte ein, der bei der Erstellung des Volumes definiert wurde. Durch die Identifizierung von Volumes, bei denen Thin Provisioning deaktiviert ist, können Sie leichter entscheiden, ob Sie Thin Provisioning auf bestimmten Volumes aktivieren möchten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, in der die erforderlichen Spalten in der richtigen Reihenfolge angezeigt werden, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Kapazität“ > „Alle Volumes“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Ziehen Sie die Spalten „Verwendete Daten %“ und „Thin Provisioned“ per Drag & Drop in die Nähe der Spalte „Verfügbare Datenkapazität“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu: **Thin Provisioning** ist **Nein**, und klicken Sie dann auf **Filter anwenden**.
6. Klicken Sie oben auf die Spalte „Verwendete Daten %“, um die Ergebnisse so zu sortieren, dass die Datenträger mit dem höchsten Prozentsatz oben in der Liste angezeigt werden.
7. Speichern Sie die Ansicht unter einem Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Vols no thin provisioning“.
8. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtszeitpläne** eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken

Sie dann auf das Häkchen ( ) am Ende der Zeile.

Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise Thin Provisioning auf bestimmten Volumes aktivieren.

Erstellen Sie einen Bericht, um Volumes auf FabricPool -Aggregaten zu identifizieren, die Daten in die Cloud-Ebene verschieben sollen

Sie können einen Bericht erstellen, der die Liste der Volumes enthält, die sich derzeit auf FabricPool -Aggregaten befinden, die eine Cloud-Empfehlung der Stufe „Tier“ haben und die eine große Menge kalter Daten enthalten. Dieser Bericht kann Ihnen bei der Entscheidung helfen, ob Sie die Tiering-Richtlinie für bestimmte Volumes auf „auto“ oder „all“ ändern sollten, um mehr kalte (inaktive) Daten in die Cloud-Ebene auszulagern.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.
- Sie müssen FabricPool Aggregate konfiguriert haben und über Volumes auf diesen Aggregaten verfügen.

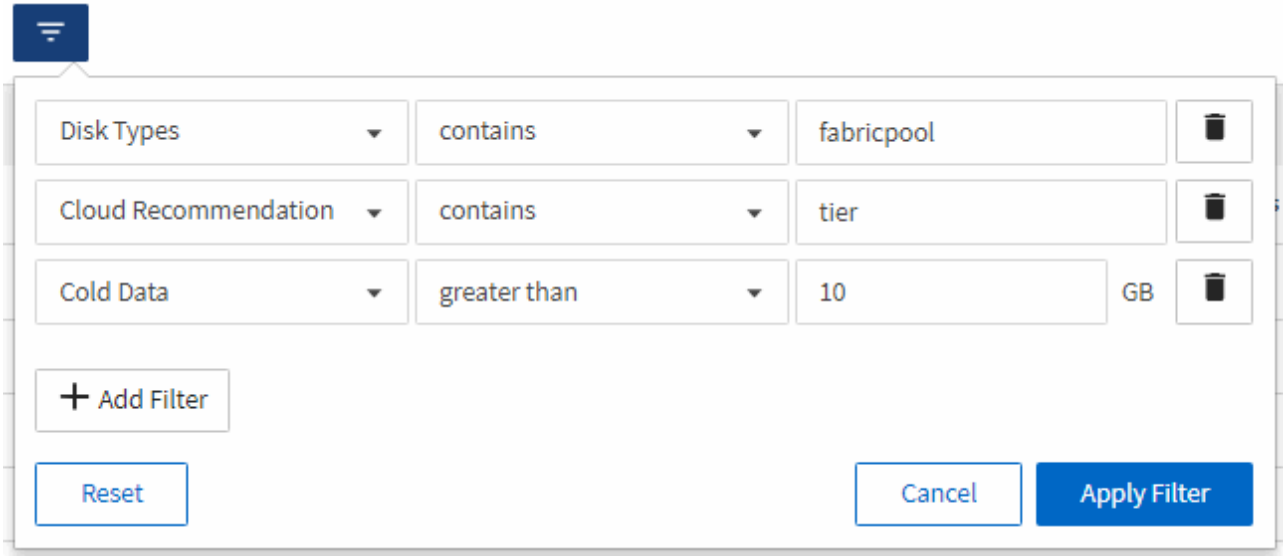
Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, in der die erforderlichen Spalten in der richtigen Reihenfolge angezeigt werden, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

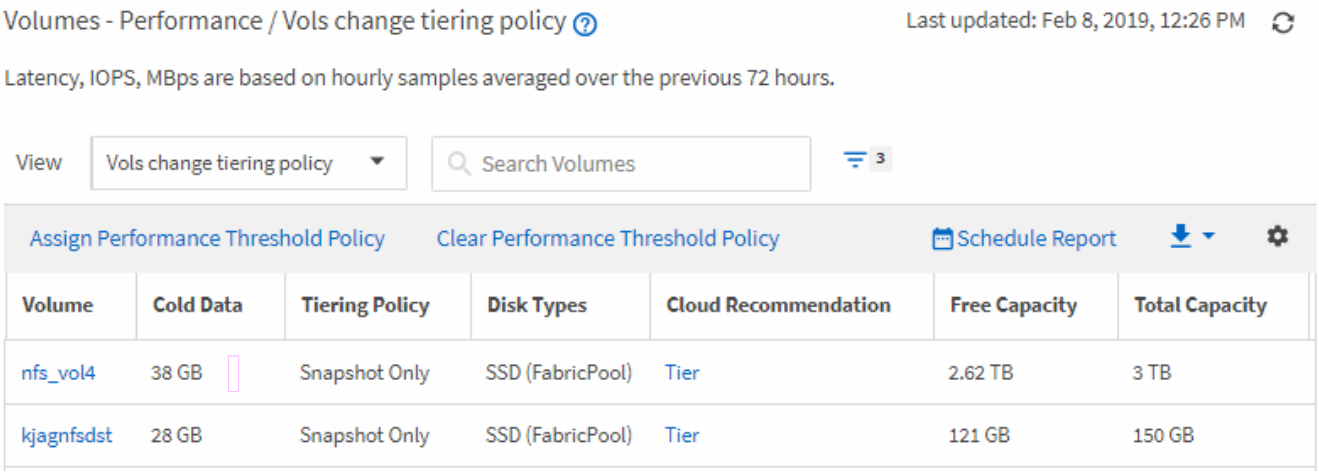
1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Leistung“ > „Alle Volumes“ aus.
3. Stellen Sie in der Spaltenauswahl sicher, dass die Spalte „Datenträgertyp“ in der Ansicht angezeigt wird.

   Fügen Sie weitere Spalten hinzu oder entfernen Sie sie, um eine für Ihren Bericht wichtige Ansicht zu erstellen.

4. Ziehen Sie die Spalte „Datenträgertyp“ per Drag & Drop in die Nähe der Spalte „Cloud-Empfehlung“.
5. Klicken Sie auf das Filtersymbol, fügen Sie die folgenden drei Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Der Datenträgertyp enthält FabricPool
   - Cloud-Empfehlung enthält Stufe
   - Kalte Daten größer als 10 GB



6. Klicken Sie oben auf die Spalte „Kalte Daten“, sodass die Volumes mit den meisten kalten Daten oben in der Ansicht angezeigt werden.
7. Speichern Sie die Ansicht unter einem Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Vols ändern Tiering-
Richtlinie“.



Volume	Cold Data	Tiering Policy	Disk Types	Cloud Recommendation	Free Capacity	Total Capacity
nfs_vol4	38 GB	Snapshot Only	SSD (FabricPool)	Tier	2.62 TB	3 TB
kjagnfsdst	28 GB	Snapshot Only	SSD (FabricPool)	Tier	121 GB	150 GB

8. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
9. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
10. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise System Manager oder die ONTAP CLI verwenden, um die Tiering-Richtlinie für bestimmte Volumes auf „auto“ oder „all“ zu ändern, um mehr kalte Daten in die Cloud-Ebene auszulagern.

Passen Sie Qtree-Kapazitätsberichte an

Diese benutzerdefinierten Beispielberichte sollen Ihnen dabei helfen, potenzielle

Probleme im Zusammenhang mit der Qtree-Kapazität zu erkennen und darauf zu reagieren.

Erstellen Sie einen Bericht, um fast volle Qtrees anzuzeigen

Sie können einen Bericht erstellen, um die Speicherkapazität und Auslastung von Qtrees zu analysieren und fast volle Qtrees anzuzeigen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die fast volle Qtrees anzeigt, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Qtrees**.
2. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
3. Ziehen Sie die Spalte „Disk Used %“ in die Nähe der Spalte „Qtrees“.
4. Klicken Sie auf das Filtersymbol, fügen Sie die folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Der Prozentsatz der Festplattennutzung liegt über 75 %
5. Klicken Sie oben auf die Spalte „Verwendeter Datenträger %“, um die Ergebnisse nach Kapazitätsprozentsatz zu sortieren.
6. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „`Qtrees fast voll`“, und klicken Sie auf das Häkchen ( ).
7. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
8. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtszeitpläne** eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
9. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise die harten und weichen Festplattenlimits (sofern festgelegt) anpassen oder die Daten über die Qtrees verteilen.

Anpassen von NFS-Freigabeberichten

Sie können NFS-Freigabeberichte anpassen, um Informationen zu NFS-Exportrichtlinien und -Regeln für Volumes auf Ihren Speichersystemen zu analysieren. Sie können beispielsweise Berichte anpassen, um Volumes mit nicht zugänglichen Bereitstellungspfaden und Volumes mit der Standardexportrichtlinie anzuzeigen.

Erstellen Sie einen Bericht, um Volumes anzuzeigen, deren Mount-Pfad nicht zugänglich ist

Sie können einen Bericht erstellen, um Volumes zu finden, deren Bereitstellungspfad

nicht zugänglich ist.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht für Volumes mit einem unzugänglichen Bereitstellungspfad zu erstellen und dann die Erstellung eines Berichts für diese Ansicht zu planen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **NFS-Freigaben**.
2. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
3. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Mount Path Active ist Nein
4. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Volumes mit einem nicht zugänglichen Mount-Pfad“, und klicken Sie auf das Häkchen ( ).
5. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
6. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
7. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise die nicht zugänglichen Mount-Pfade korrigieren.

Erstellen Sie einen Bericht, um Volumes anzuzeigen, die die Standardexportrichtlinie verwenden

Sie können einen Bericht erstellen, um Volumes zu finden, die die Standardexportrichtlinie verwenden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht für Volumes zu erstellen, die die Standardexportrichtlinie verwenden, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **NFS-Freigaben**.
2. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
3. Ziehen Sie die Spalte „Exportrichtlinie“ in die Nähe der Spalte „Volumen“.
4. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Exportrichtlinie enthält Standard

5. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Volumes mit einer Standardexportrichtlinie“, und klicken Sie auf das Häkchen ( ).
6. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
7. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
8. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise eine benutzerdefinierte Exportrichtlinie konfigurieren.

Anpassen von Speicher-VM-Berichten

Sie können Speicher-VM-Berichte erstellen, um Volume-Informationen zu analysieren und den Gesamtzustand und die Speicherverfügbarkeit anzuzeigen. Sie können beispielsweise Berichte erstellen, um anzuzeigen, dass SVMs die maximale Volumeanzahl erreichen, und um gestoppte SVMs zu analysieren.

Erstellen Sie einen Bericht, um Speicher-VMs anzuzeigen, die das maximale Volumenlimit erreichen

Sie können einen Bericht erstellen, um SVMs zu finden, die das maximale Volumenlimit erreichen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die Speicher-VMs anzeigt, die das maximale Volumenlimit erreichen, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Speicher-VMs**.
2. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
3. Ziehen Sie die Spalten „Volume Count“ und „Maximum Allowed Volumes“ in die Nähe der Spalte „Storage VM“.
4. Klicken Sie oben auf die Spalte „Maximal zulässige Volumes“, um die Ergebnisse nach der höchsten Volumeanzahl zu sortieren.
5. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „`SVMs erreichen maximale Volumes`“, und klicken Sie auf das Häkchen ( ).
6. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
7. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtszeitpläne** eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
8. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise die den Speicher-VMs zugewiesenen Volumes ausgleichen oder, falls möglich, den ONTAP System Manager verwenden, um die maximal zulässigen Volumes zu ändern.

Erstellen Sie einen Bericht zum Anzeigen gestoppter Speicher-VMs

Sie können einen Bericht erstellen, um eine Liste aller gestoppten SVMs anzuzeigen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die gestoppte Speicher-VMs anzeigt, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Speicher-VMs**.
2. Wählen Sie im Menü „Ansicht“ die Option „Integrität“ > „Alle Speicher-VMs“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Ziehen Sie die Spalte „Status“ in die Nähe der Spalte „Speicher-VM“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Status ist „Gestoppt“
6. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Gestoppte SVMs“, und klicken Sie auf das Häkchen ( ).
7. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
8. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtszeitpläne** eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
9. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise untersuchen, warum die SVM gestoppt wurde, um festzustellen, ob Sie die gestoppten SVMs neu starten sollten.

Anpassen von Volumenbeziehungsberichten

Mit dem Bericht „Volume Relationships Inventory“ können Sie die Speicherinventardetails in einem Cluster analysieren, den für Volumes erforderlichen Schutzgrad ermitteln und die Volumedetails basierend auf Fehlerquelle, Muster und Zeitplänen filtern.

Erstellen Sie einen Bericht, um Volumenbeziehungen nach Fehlerquelle zu gruppieren

Sie können einen Bericht erstellen, der Volumes nach dem Grund gruppiert, warum die Beziehung in einem fehlerhaften Zustand ist.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die Volumes nach Fehlerquelle gruppiert, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Beziehung“ > „Alle Beziehungen“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um sicherzustellen, dass die Spalten „Beziehungsgesundheit“ und „Grund für Ungesundheit“ in der Ansicht angezeigt werden.

   Fügen Sie weitere Spalten hinzu oder entfernen Sie sie, um eine für Ihren Bericht wichtige Ansicht zu erstellen.

4. Ziehen Sie die Spalten „Beziehungsgesundheit“ und „Grund für Ungesundheit“ in die Nähe der Spalte „Status“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Die Beziehungsgesundheit ist schlecht
6. Klicken Sie oben auf die Spalte „Fehlerursache“, um die Volumebeziehungen nach Fehlerquelle zu gruppieren.
7. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Vol-Beziehungen nach Fehler“.
8. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
9. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht angezeigten Ergebnisse können Sie die Quelle und die Auswirkungen der einzelnen Fehlertypen untersuchen.

Erstellen Sie einen Bericht, um Volumenbeziehungen nach Problem zu gruppieren

Sie können einen Bericht erstellen, der Volumenbeziehungen nach Ausgabe gruppiert.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die Volumenbeziehungen nach Ausgabe gruppiert, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Beziehung“ > „Alle Beziehungen“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Ziehen Sie die Spalte „Unhealthy Reason“ in die Nähe der Spalte „State“.
5. Klicken Sie oben auf die Spalte „Unhealthy Reason“, um die Bände nach Problem zu gruppieren.
6. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Vol-Beziehungen nach Problem“.
7. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
8. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht angezeigten Ergebnisse können Sie die Quelle und die Auswirkungen jedes Problemtyps untersuchen.

Erstellen Sie einen Bericht, um Volumenübertragungstrends in bestimmten Zeitintervallen anzuzeigen

Sie können einen Bericht erstellen, der Volumenübertragungstrends in bestimmten Zeitintervallen anzeigt.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht für Volumes in bestimmten Zeitintervallen zu erstellen und dann die Erstellung eines Berichts für diese Ansicht zu planen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Beziehung“ > „Übertragungsstatus des letzten Monats“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Ziehen Sie die Spalte „Übertragungsdauer“ in die Nähe der Spalte „Betriebsergebnis“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Transfer-Endzeit in den letzten 7 Tagen
6. Klicken Sie oben auf die Spalte „Übertragungsdauer“, um die Datenträger nach Zeitintervall zu sortieren.
7. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Volumes nach Dauer“.
8. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
9. Geben Sie einen Namen für den Berichtszeitplan ein, legen Sie die Häufigkeit auf **Wöchentlich** fest, füllen Sie die anderen Berichtsfelder aus und klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht angezeigten Ergebnisse können Sie die Übertragungszeitintervalle untersuchen.

Erstellen Sie einen Bericht, um fehlgeschlagene oder erfolgreiche Volumeübertragungen anzuzeigen

Sie können einen Bericht erstellen, der den Status von Volumenübertragungen anzeigt. In diesem Bericht können Sie sowohl fehlgeschlagene als auch erfolgreiche Volumenübertragungen anzeigen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht zu erstellen, die anzeigt, welche Übertragungen fehlgeschlagen und welche erfolgreich waren, und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Beziehung“ > „Übertragungsstatus des letzten Monats“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um alle Spalten zu entfernen, die Sie nicht im Bericht haben möchten.
4. Ziehen Sie die Spalte „Operationsergebnis“ in die Nähe der Spalte „Status“.
5. Klicken Sie oben auf die Spalte „Operationsergebnis“, um die Volumes nach Status zu sortieren.
6. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Volumes nach Übertragungsstatus“.
7. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
8. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht angezeigten Ergebnisse können Sie den Übertragungsstatus untersuchen.

Erstellen Sie einen Bericht, um Volumenübertragungen basierend auf der Übertragungsgröße anzuzeigen

Sie können einen Bericht erstellen, um Volumenübertragungen basierend auf der Übertragungsgröße anzuzeigen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht für Volumenübertragungen basierend auf der Übertragungsgröße zu erstellen und planen Sie dann die Generierung eines Berichts für diese Ansicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Beziehung“ > „Übertragungsrate des letzten Monats“ aus.

3. Klicken Sie oben auf die Spalte „Gesamtübertragungsgröße“, um die Volumenübertragungen nach Größe zu sortieren.
4. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Volumes nach Übertragungsgröße“.
5. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
6. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht angezeigten Ergebnisse können Sie die Volumenbeziehungen nach Übertragungsgröße untersuchen.

Erstellen Sie einen Bericht, um Volumenübertragungen gruppiert nach Tag anzuzeigen

Sie können einen Bericht erstellen, um Volumenübertragungen nach Tag gruppiert anzuzeigen.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht für nach Tag gruppierte Volumenübertragungen zu erstellen und dann die Erstellung eines Berichts für diese Ansicht zu planen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Beziehung“ > „Übertragungsrate des letzten Monats“ aus.
3. Klicken Sie oben auf die Spalte „Tag“, um die Volumenübertragungen nach Tag zu sortieren.
4. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „Volumenübertragungen nach Tag“.
5. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
6. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht angezeigten Ergebnisse können Sie die Volumenübertragungen nach Tagen untersuchen.

Anpassen von Volume-Leistungsberichten

Diese benutzerdefinierten Beispielberichte sollen Ihnen dabei helfen, potenzielle Probleme im Zusammenhang mit der Lautstärkeleistung zu erkennen und darauf zu reagieren.

Erstellen Sie einen Bericht, um Volumes mit einer großen Menge kalter Daten auf einem Aggregat anzuzeigen, das nicht FabricPool-fähig ist.

Sie können einen Bericht erstellen, um Volumes mit einer großen Menge kalter Daten auf einem Nicht- FabricPool -Aggregat anzuzeigen. Dies kann Ihnen dabei helfen, Volumes zu identifizieren, die in ein FabricPool Aggregat verschoben werden sollten.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine benutzerdefinierte Ansicht für Volumes mit einer großen Menge kalter Daten auf einem nicht FabricPool-fähigen Aggregat zu erstellen und dann die Generierung eines Berichts für diese Ansicht zu planen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie im Menü „Ansicht“ die Option „Leistung“ > „Alle Volumes“ aus.
3. Wählen Sie **Anzeigen/Ausblenden**, um sicherzustellen, dass die Spalte „Datenträgertyp“ in der Ansicht angezeigt wird.

   Fügen Sie weitere Spalten hinzu oder entfernen Sie sie, um eine für Ihren Bericht wichtige Ansicht zu erstellen.

4. Ziehen Sie die Spalte „Datenträgertyp“ in die Nähe der Spalte „Kalte Daten“.
5. Klicken Sie auf das Filtersymbol, fügen Sie den folgenden Filter hinzu und klicken Sie dann auf **Filter anwenden**:
   - Kalte Daten größer als 100 GB
   - Der Datenträgertyp enthält SSD
6. Klicken Sie oben auf die Spalte „Datenträgertyp“, um die Volumes nach Datenträgertyp zu sortieren, sodass der Datenträgertyp SSD (FabricPool) unten angezeigt wird.
7. Speichern Sie die Ansicht unter einem bestimmten Namen, der widerspiegelt, was die Ansicht anzeigt, z. B. „`Cold data vols not FabricPool`“.
8. Klicken Sie auf der Inventarseite auf die Schaltfläche **Geplante Berichte**.
9. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

   Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Anhand der im Bericht angezeigten Ergebnisse können Sie Volumes finden, die sich gut für die Verschiebung in FabricPool Aggregate eignen.

Beispiele für Microsoft Excel-Berichte

Diese Beispielberichte zu Microsoft Excel sollen die Berichtsoptionen vorstellen, die mit den erweiterten Funktionen von Excel verfügbar sind.

Mit den erweiterten Funktionen von Excel können Sie eine große Bandbreite an Berichten erstellen, die

speziell auf Ihre Anforderungen zugeschnitten sind. Ausführliche Informationen zur Verwendung von Excel finden Sie in der Produktdokumentation.

Zum Verwalten von Berichten müssen Sie über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Erstellen Sie einen Bericht, um eine Tabelle und ein Diagramm zur Gesamtkapazität anzuzeigen

Sie können einen Bericht zur Kapazitätsanalyse in einer Excel-Datei erstellen, indem Sie Summen und das gruppierte Säulendiagrammformat verwenden.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine Ansicht „Integrität: Alle Aggregate“ zu öffnen, die Ansicht in Excel herunterzuladen, ein Diagramm der verfügbaren Kapazität zu erstellen, die angepasste Excel-Datei hochzuladen und den Abschlussbericht zu planen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.
2. Wählen Sie **Berichte** > **Excel herunterladen**.

   Abhängig von Ihrem Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.

3. Klicken Sie bei Bedarf auf **Bearbeitung aktivieren**.
4. Öffnen Sie die heruntergeladene Datei in Excel.
5. Erstellen Sie ein neues Blatt (⊕) nach dem `data` Blatt und nennen Sie es **Gesamtdatenkapazität**.
6. Fügen Sie dem neuen Blatt „Gesamtdatenkapazität“ die folgenden Spalten hinzu:
   a. Gesamtdatenkapazität (GB)
   b. Zugesicherte Kapazität (GB)
   c. Verwendete Datenkapazität (GB)
   d. Verfügbare Datenkapazität (GB)
7. Geben Sie in die erste Zeile jeder Spalte die folgende Formel ein und achten Sie darauf, dass sie auf das Datenblatt (Daten!) verweist und auf die richtigen Spalten- und Zeilenbezeichner für die erfassten Daten verweist (Total Data Capacity zieht Daten aus Spalte E, Zeilen 2 bis 20).

   a. =SUMME(Daten!E$2:Daten!E$20)
   b. =SUMME(Daten!F$2:Daten!F$50)
   c. =SUMME(Daten!G$2:Daten!G$50)
   d. =SUMME(Daten!H$2:Daten!H$50)

   Die Formel summiert jede Spalte basierend auf den aktuellen Daten.

1. Wählen Sie im Datenblatt die Spalten **Gesamtdatenkapazität (GB)** und **Zugesicherte Kapazität (GB)** aus.

2. Wählen Sie **Empfohlene Diagramme** aus dem Menü **Einfügen** und wählen Sie das Diagramm **Gruppierte Säulen**.
3. Klicken Sie mit der rechten Maustaste auf das Diagramm und wählen Sie **Diagramm verschieben**, um das Diagramm in die `Total Data Capacity` Blatt.
4. Mithilfe der Menüs **Entwurf** und **Format**, die bei Auswahl des Diagramms verfügbar sind, können Sie das Aussehen des Diagramms anpassen.
5. Wenn Sie zufrieden sind, speichern Sie die Datei mit Ihren Änderungen. Ändern Sie weder den Dateinamen noch den Speicherort.

6. Wählen Sie im Unified Manager **Berichte** > **Excel hochladen**.

   Stellen Sie sicher, dass Sie sich in derselben Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

7. Wählen Sie die Excel-Datei aus, die Sie geändert haben.
8. Klicken Sie auf **Öffnen**.
9. Klicken Sie auf **Senden**.

   Neben dem Menüpunkt **Berichte** > **Excel hochladen** wird ein Häkchen angezeigt.

10. Klicken Sie auf **Geplante Berichte**.
11. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.

    Wählen Sie das **XLSX**-Format für den Bericht.

12. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise untersuchen, wie Sie die verfügbare Kapazität in Ihrem Netzwerk am besten nutzen können.

Erstellen Sie einen Bericht, um Diagramme mit der Gesamtsumme und der verfügbaren Kapazität anzuzeigen

Sie können einen Bericht erstellen, um die Gesamtspeicherkapazität und die zugesagte Kapazität in einem Excel-Diagrammformat zu analysieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine Ansicht „Integrität: Alle Aggregate“ zu öffnen, die Ansicht in Excel herunterzuladen, ein Diagramm mit der Gesamt- und der zugesagten Kapazität zu erstellen, die angepasste Excel-Datei hochzuladen und den Abschlussbericht zu planen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.
2. Wählen Sie **Berichte** > **Excel herunterladen**.

   Abhängig von Ihrem Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.

3. Öffnen Sie die heruntergeladene Datei in Excel.
4. Klicken Sie bei Bedarf auf **Bearbeitung aktivieren**.
5. Klicken Sie im Datenblatt mit der rechten Maustaste auf die Spalte Typ und wählen Sie **Sortieren** > **Sortieren von A bis Z**.

   Dadurch werden Ihre Daten nach Speichertyp sortiert, beispielsweise:

   - Festplatte
   - Hybrid
   - SSD
   - SSD (FabricPool)

6. Wählen Sie die `Type, Total Data Capacity,` Und `Available Data Capacity` Spalten.
7. Wählen Sie im Menü **Einfügen** eine `3-D column` Diagramm.

   Das Diagramm erscheint auf dem Datenblatt.

8. Klicken Sie mit der rechten Maustaste auf das Diagramm und wählen Sie **Diagramm verschieben**.
9. Wählen Sie **Neues Blatt** und benennen Sie das Blatt **Total Storage Charts**.

   Achten Sie darauf, dass das neue Blatt nach den Info- und Datenblättern erscheint.

10. Benennen Sie das Diagramm mit **Gesamtkapazität im Vergleich zur verfügbaren Kapazität**.
11. Mithilfe der Menüs **Entwurf** und **Format**, die verfügbar sind, wenn das Diagramm ausgewählt ist, können Sie das Aussehen des Diagramms anpassen.
12. Wenn Sie zufrieden sind, speichern Sie die Datei mit Ihren Änderungen. Ändern Sie weder den Dateinamen noch den Speicherort.
13. Wählen Sie im Unified Manager **Berichte** > **Excel hochladen**.

    Stellen Sie sicher, dass Sie sich in derselben Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

14. Wählen Sie die Excel-Datei aus, die Sie geändert haben.
15. Klicken Sie auf **Öffnen**.
16. Klicken Sie auf **Senden**.

    Neben dem Menüpunkt **Berichte** > **Excel hochladen** wird ein Häkchen angezeigt.

17. Klicken Sie auf **Geplante Berichte**.
18. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtszeitpläne** eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.

    Wählen Sie das **XLSX**-Format für den Bericht.

19. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise die Last Ihrer Aggregate ausgleichen.

Erstellen Sie einen Bericht, um Diagramme zur verfügbaren Datenträgerkapazität anzuzeigen

Sie können einen Bericht erstellen, um die verfügbare Datenträgerkapazität in einem Excel-Diagramm zu analysieren.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine Ansicht „Integrität: Alle Volumes“ zu öffnen, die Ansicht in Excel herunterzuladen, ein Diagramm der verfügbaren Kapazität zu erstellen, die benutzerdefinierte Excel-Datei hochzuladen und den Abschlussbericht zu planen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Volumes**.
2. Wählen Sie **Berichte** > **Excel herunterladen**.

   Abhängig von Ihrem Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.

3. Klicken Sie bei Bedarf auf **Bearbeitung aktivieren**.
4. Öffnen Sie die heruntergeladene Datei in Excel.
5. Auf der `data` wählen Sie die Daten aus, die Sie im `Volume` Und `Available Data` % Spalten.
6. Wählen Sie im Menü **Einfügen** eine `3-D piechart.`

   Das Diagramm zeigt, welche Volumes über den größten verfügbaren Speicherplatz verfügen. Das Diagramm erscheint auf dem Datenblatt.

   Abhängig von Ihrer Netzwerkkonfiguration kann die Auswahl ganzer Spalten oder zu vieler Datenzeilen dazu führen, dass Ihr Kreisdiagramm unleserlich wird. In diesem Beispiel wird das 3D-Kreisdiagramm verwendet, Sie können jedoch jeden Diagrammtyp verwenden. Verwenden Sie das Diagramm, das die Daten, die Sie erfassen möchten, am besten darstellt.

7. Benennen Sie den Diagrammtitel mit **Verfügbare Kapazität**.
8. Klicken Sie mit der rechten Maustaste auf das Diagramm und wählen Sie **Diagramm verschieben**.
9. Wählen Sie **Neues Blatt** und benennen Sie das Blatt **Storage Volume Charts**.

   Achten Sie darauf, dass das neue Blatt nach den Info- und Datenblättern erscheint.

10. Mithilfe der Menüs **Entwurf** und **Format**, die verfügbar sind, wenn das Diagramm ausgewählt ist, können Sie das Aussehen des Diagramms anpassen.
11. Wenn Sie zufrieden sind, speichern Sie die Datei mit Ihren Änderungen.
12. Wählen Sie im Unified Manager **Berichte** > **Excel hochladen**.

    Stellen Sie sicher, dass Sie sich in derselben Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

13. Wählen Sie die Excel-Datei aus, die Sie geändert haben.
14. Klicken Sie auf **Öffnen**.
15. Klicken Sie auf **Senden**.

    Neben dem Menüpunkt **Berichte** > **Excel hochladen** wird ein Häkchen angezeigt.

16. Klicken Sie auf **Geplante Berichte**.
17. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite **Berichtszeitpläne** eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.
18. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

    Wählen Sie das **XLSX**-Format für den Bericht.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise die Last auf Ihren Datenträgern ausgleichen.

Erstellen Sie einen Bericht, um Aggregate mit den meisten verfügbaren IOPS anzuzeigen

Dieser Bericht zeigt, welche Aggregate die meisten verfügbaren IOPS pro Aggregattyp haben, auf denen Sie neue Workloads bereitstellen können.

Bevor Sie beginnen

- Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Führen Sie die folgenden Schritte aus, um eine Ansicht „Integrität: Alle Volumes“ zu öffnen, die Ansicht in Excel herunterzuladen, ein Diagramm der verfügbaren Kapazität zu erstellen, die benutzerdefinierte Excel-Datei hochzuladen und den Abschlussbericht zu planen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speicher** > **Aggregate**.
2. Wählen Sie **Leistung: Alle Aggregate** aus der Dropdown-Liste **Ansicht**.
3. Wählen Sie **Anzeigen/Ausblenden**, um die `Available IOPS` Spalte und blenden Sie die `Cluster FQDN, Inactive Data Reporting,` Und `Threshold Policy` Spalten.
4. Ziehen Sie die `Available IOPS` Und `Free Capacity` Spalten neben dem `Type` Spalte.
5. Benennen und speichern Sie die benutzerdefinierte Ansicht `Available IOPS Per Aggr.`
6. Wählen Sie **Berichte** > **Excel herunterladen**.

   Abhängig von Ihrem Browser müssen Sie möglicherweise auf **OK** klicken, um die Datei zu speichern.

7. Klicken Sie bei Bedarf auf **Bearbeitung aktivieren**.
8. Öffnen Sie die heruntergeladene Datei in Excel.
9. Klicken Sie im Datenblatt auf das kleine Dreieck oben links, um das gesamte Blatt auszuwählen.
10. Wählen Sie im Menüband **Daten** die Option **Sortieren** aus dem `Sort & Filter area.`
11. Legen Sie die folgenden Sortierebenen fest:
    a. Geben Sie **Sortieren nach** als `Available IOPS` (IOPS), die **Sort On** als `Cell Values,` und die **Bestellung** als `Largest to Smallest.`
    b. Klicken Sie auf **Ebene hinzufügen**.
    c. Geben Sie **Sortieren nach** als `Type` , die **Sortieren nach** als `Cell Values,` und die **Bestellung** als `Z to A.`
    d. Klicken Sie auf **Ebene hinzufügen**.
    e. Geben Sie **Sortieren nach** als `Free Capacity (GB),` das **Sortieren nach** als `Cell Values,` und die **Bestellung** als `Largest to Smallest.`
    f. Klicken Sie auf **OK**.
12. Speichern und schließen Sie die Excel-Datei.
13. Wählen Sie im Unified Manager **Berichte** > **Excel hochladen**.

    Stellen Sie sicher, dass Sie sich in derselben Ansicht befinden, in der Sie die Excel-Datei heruntergeladen haben.

14. Wählen Sie die Excel-Datei aus, die Sie geändert haben. In diesem Fall `performance-aggregates-<date>.xlsx.`
15. Klicken Sie auf **Öffnen**.
16. Klicken Sie auf **Senden**.

    Neben dem Menüpunkt **Berichte** > **Excel hochladen** wird ein Häkchen angezeigt.

17. Klicken Sie auf **Geplante Berichte**.
18. Klicken Sie auf **Zeitplan hinzufügen**, um der Seite „Berichtszeitpläne“ eine neue Zeile hinzuzufügen, damit Sie die Zeitplanmerkmale für den neuen Bericht definieren können.

19. Geben Sie einen Namen für den Berichtszeitplan ein und füllen Sie die anderen Berichtsfelder aus. Klicken Sie dann auf das Häkchen ( ) am Ende der Zeile.

    Wählen Sie das **XLSX**-Format für den Bericht.

    Der Bericht wird sofort testweise versendet. Anschließend wird der Bericht generiert und in der angegebenen Häufigkeit per E-Mail an die aufgeführten Empfänger gesendet.

Basierend auf den im Bericht angezeigten Ergebnissen möchten Sie möglicherweise neue Workloads auf den Aggregaten bereitstellen, die über die größten verfügbaren IOPS verfügen.

Verwalten des Speichers mithilfe von REST-APIs

Erste Schritte mit Active IQ Unified Manager REST-APIs

Active IQ Unified Manager bietet eine Reihe von APIs zur Verwaltung Ihrer Speicherressourcen auf den unterstützten Speichersystemen über eine RESTful-Webdienstschnittstelle für jede Drittanbieterintegration.

In diesen Themen finden Sie Informationen zu Unified Manager-APIs, Beispiel-Workflows zur Lösung bestimmter Probleme und einige Beispielcodes. Mithilfe dieser Informationen können Sie RESTful-Clients von NetApp Manageability-Softwarelösungen zum Verwalten von NetApp -Systemen erstellen. Die APIs basieren auf dem Architekturstil Representational State Transfer (REST). Alle vier REST-Operationen Erstellen, Lesen, Aktualisieren und Löschen (auch als CRUD bekannt) werden unterstützt.

Sehen"Active IQ Unified Manager" für zusätzliche Ressourcen und Details zu den Vorteilen der Active IQ Unified Manager REST API.

Zielgruppe für diesen Inhalt

Die hier behandelten Themen richten sich an Entwickler, die Anwendungen erstellen, die über REST-APIs mit der Active IQ Unified Manager -Software interagieren.

Speicheradministratoren und -architekten können diese Informationen zu Rate ziehen, um ein grundlegendes Verständnis dafür zu erlangen, wie die Unified Manager REST-APIs zum Erstellen von Clientanwendungen zum Verwalten und Überwachen von NetApp -Speichersystemen verwendet werden können.

Sie sollten diese Informationen verwenden, wenn Sie den Speicheranbieter, den ONTAP Cluster und die Verwaltungs-APIs zur Verwaltung Ihres Speichers verwenden möchten.

> Sie müssen eine der folgenden Rollen innehaben: Operator, Speicheradministrator oder Anwendungsadministrator. Sie müssen die IP-Adresse oder den vollqualifizierten Domänennamen des Unified Manager-Servers kennen, auf dem Sie die REST-APIs ausführen möchten.

Active IQ Unified Manager API-Zugriff und Kategorien

Mit den Active IQ Unified Manager -APIs können Sie Speicherobjekte in Ihrer Umgebung verwalten und bereitstellen. Sie können auch auf die Web-Benutzeroberfläche von Unified Manager zugreifen, um einige dieser Funktionen auszuführen.

Erstellen Sie eine URL für den direkten Zugriff auf REST-APIs

Sie können über eine Programmiersprache wie Python, C#, C++, JavaScript usw. direkt auf die REST-APIs zugreifen. Geben Sie den Hostnamen oder die IP-Adresse und die URL für den Zugriff auf die REST-APIs im Format

https://<Hostname>/api

> Der Standardport ist 443. Sie können den Port entsprechend den Anforderungen Ihrer Umgebung konfigurieren.

Greifen Sie auf die Online-API-Dokumentationsseite zu

Sie können auf die Referenzinhaltsseite „API-Dokumentation“ zugreifen, die zusammen mit dem Produkt geliefert wird, um die API-Dokumentation anzuzeigen und manuell einen API-Aufruf zu tätigen (auf der Schnittstelle, beispielsweise Swagger). Sie können auf diese Dokumentation zugreifen, indem Sie auf die **Menüleiste** > **Hilfe-Schaltfläche** > **API-Dokumentation** klicken.

Alternativ geben Sie den Hostnamen oder die IP-Adresse und die URL für den Zugriff auf die REST-API-Seite im Format

https://<Hostname>/docs/api/

Kategorien

Die API-Aufrufe sind funktional nach Bereichen oder Kategorien organisiert. Um eine bestimmte API zu finden, klicken Sie auf die entsprechende API-Kategorie.

Die mit Unified Manager bereitgestellten REST-APIs unterstützen Sie bei der Durchführung von Verwaltungs-, Überwachungs- und Bereitstellungsfunktionen. Die APIs sind in die folgenden Kategorien eingeteilt.

- **Rechenzentrum**

  Diese Kategorie enthält die APIs, die Sie bei der Speicherverwaltung und -analyse im Rechenzentrum mithilfe von Tools wie Work Flow Automation und Ansible unterstützen. Die REST-APIs in dieser Kategorie bieten Informationen zu Clustern, Knoten, Aggregaten, Volumes, LUNs, Dateifreigaben, Namespaces und anderen Elementen in Ihrem Rechenzentrum.

- **Verwaltungsserver**

  Die APIs unter der Kategorie **Management-Server** enthalten die `jobs, system,` Und `events` APIs. Jobs sind Vorgänge, die für die asynchrone Ausführung im Zusammenhang mit der Verwaltung von Speicherobjekten oder Workloads auf Unified Manager geplant sind. Der `events` API gibt Ereignisse in Ihrem Rechenzentrum zurück und die `system` Die API gibt die Details der Unified Manager-Instanz zurück.

- **Speicheranbieter**

  Diese Kategorie enthält alle Bereitstellungs-APIs, die für die Verwaltung und Bereitstellung von Dateifreigaben, LUNs, Leistungsserviceleveln und Speichereffizienzrichtlinien erforderlich sind. Mit den APIs können Sie außerdem Zugriffsendpunkte und Active Directorys konfigurieren sowie Leistungsservicelevel und Speichereffizienzrichtlinien für Speicher-Workloads zuweisen.

- **Verwaltung**

  Diese Kategorie enthält die APIs, die zum Ausführen administrativer Aufgaben verwendet werden, z. B. zum Verwalten von Sicherungseinstellungen, zum Anzeigen von Trust Store-Zertifikaten für die Unified Manager-Datenquellen und zum Verwalten von ONTAP Clustern als Datenquellen für Unified Manager.

- **Tor**

  Mit Unified Manager können Sie ONTAP REST-APIs über die APIs in der Gateway-Kategorie aufrufen und die Speicherobjekte in Ihrem Rechenzentrum verwalten.

- **Sicherheit**

  Diese Kategorie enthält APIs zum Verwalten von Unified Manager-Benutzern.

Im Active IQ Unified Manager angebotene REST-Dienste

Sie sollten sich über die angebotenen REST-Dienste und -Vorgänge im Klaren sein, bevor Sie mit der Verwendung der Active IQ Unified Manager -APIs beginnen.

Die Bereitstellungs- und Verwaltungs-APIs, die zum Konfigurieren des API-Servers verwendet werden, unterstützen Lese- (GET) oder Schreibvorgänge (POST, PATCH, DELETE). Im Folgenden finden Sie einige Beispiele für die von den APIs unterstützten Vorgänge GET, PATCH, POST und DELETE:

- Beispiel für GET: `GET /datacenter/cluster/clusters` ruft Clusterdetails in Ihrem Rechenzentrum ab. Die maximale Anzahl von Datensätzen, die vom `GET` Operation ist 1000.

  Mit den APIs können Sie die Datensätze nach unterstützten Attributen filtern, sortieren und 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 aus einer LUN, SVM oder Dateifreigabe mithilfe seines eindeutigen Schlüssels.

Die REST-Vorgänge, die mithilfe der APIs ausgeführt werden können, hängen von der Rolle des Operator-, Speicheradministrator- oder Anwendungsadministrator-Benutzers ab.

Benutzerrolle	Unterstützte REST-Methode
Operator	Nur Lesezugriff auf Daten. Benutzer mit dieser Rolle können alle GET-Anfragen ausführen.
Speicheradministrator	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 Verwalten von Speicherdienstobjekten und Speicherverwaltungsoptionen.
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-Vorgängen finden Sie in der *Online-API-Dokumentation*.

API-Version im Active IQ Unified Manager

Die REST-API-URIs in Active IQ Unified Manager geben eine Versionsnummer an. 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 sie eine Antwort zurücksendet, die der Client verarbeiten kann.

Der numerische Teil dieser Versionsnummer ist in Bezug auf die Releases inkrementell. URIs mit einer Versionsnummer bieten eine konsistente Schnittstelle, die die Abwärtskompatibilität in zukünftigen Versionen gewährleistet. Sie finden die gleichen APIs auch ohne Versionsangabe, zum Beispiel `/datacenter/svm/svms`, die die Basis-APIs ohne Version angeben. Bei den Basis-APIs handelt es sich immer um 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 Version einer bestimmten API (in Bezug auf die inkrementelle Ganzzahl) zu verwenden, die in Ihrer Unified Manager-Instanz verfügbar ist.

Bei allen Anfragen müssen Sie explizit die API-Version anfordern, die Sie verwenden möchten. Wenn die Versionsnummer angegeben ist, gibt der Dienst keine Antwortelemente zurück, für deren Verarbeitung Ihre Anwendung nicht ausgelegt ist. In REST-Anfragen sollten Sie den Versionsparameter einschließen. Die früheren Versionen der APIs werden nach einigen Veröffentlichungen möglicherweise verworfen. In dieser Version `v1` Version der APIs ist veraltet.

Speicherressourcen in ONTAP

Die Speicherressourcen in ONTAP können grob in *physische Speicherressourcen* und *logische Speicherressourcen* unterteilt werden. Um Ihre ONTAP Systeme mithilfe der in Active IQ Unified Manager bereitgestellten APIs effektiv zu verwalten, müssen Sie das Speicherressourcenmodell und die Beziehung zwischen verschiedenen Speicherressourcen verstehen.

- **Physische Speicherressourcen**

  Bezieht sich auf die von ONTAP bereitgestellten physischen Speicherobjekte. Zu den physischen Speicherressourcen gehören Festplatten, Cluster, Speichercontroller, Knoten und Aggregate.

- **Logische Speicherressourcen**

  Bezieht sich auf die von ONTAP bereitgestellten Speicherressourcen, die nicht an eine physische Ressource gebunden sind. Diese Ressourcen sind mit einer virtuellen Speichermaschine (SVM, früher als VServer bezeichnet) verknüpft und existieren unabhängig von bestimmten physischen Speicherressourcen wie einer Festplatte, einem Array-LUN oder einem Aggregat.

  Zu den logischen Speicherressourcen gehören Volumes aller Typen und Qtrees sowie die Funktionen und Konfigurationen, die Sie mit diesen Ressourcen verwenden können, wie z. B. Snapshot-Kopien, Deduplizierung, Komprimierung und Kontingente.

Die folgende Abbildung zeigt die Speicherressourcen in einem 2-Knoten-Cluster:

REST-API-Zugriff und Authentifizierung im Active IQ Unified Manager

Auf die Active IQ Unified Manager REST-API kann über jeden REST-Client oder jede Programmierplattform zugegriffen werden, die HTTP-Anfragen mit einem grundlegenden HTTP-Authentifizierungsmechanismus ausgeben kann.

Eine Beispielanfrage 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 der vollqualifizierte Domänenname (FQDN) des API-Servers.
- Port 443

  443 ist der Standard-HTTPS-Port. Sie können den HTTPS-Port bei Bedarf anpassen.

Um HTTP-Anfragen von einem Webbrowser aus zu stellen, müssen Sie REST-API-Browser-Plugins verwenden. Sie können auch über Skriptplattformen wie cURL und Perl auf die REST-API zugreifen.

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 Serverüberprüfung ein selbstsigniertes SSL-Zertifikat zur Verfügung. Dieses Zertifikat kann durch ein benutzerdefiniertes Zertifikat (oder CA-Zertifikat) ersetzt werden.

Sie müssen den Benutzerzugriff auf den API-Server konfigurieren, um die REST-APIs aufzurufen. Bei den Benutzern kann es sich um lokale Benutzer (in der lokalen Datenbank gespeicherte Benutzerprofile) oder LDAP-Benutzer handeln (wenn Sie den API-Server für die Authentifizierung über LDAP konfiguriert haben). Sie können den Benutzerzugriff verwalten, indem Sie sich bei der Benutzeroberfläche der Unified Manager-Verwaltungskonsole anmelden.

Im Active IQ Unified Manager verwendete HTTP-Statuscodes

Beim Ausführen der APIs oder bei der Fehlerbehebung sollten Sie sich der verschiedenen HTTP-Statuscodes und Fehlercodes bewusst sein, die von den Active IQ Unified Manager -APIs verwendet werden.

In der folgenden Tabelle sind die Fehlercodes im Zusammenhang mit der Authentifizierung aufgeführt:

HTTP-Statuscode	Titel des Statuscodes	Beschreibung
200	OK	Wird bei erfolgreicher Ausführung synchroner API-Aufrufe zurückgegeben.
201	Erstellt	Erstellung neuer Ressourcen durch synchrone Aufrufe, beispielsweise Konfiguration von Active Directory.

HTTP-Statuscode	Titel des Statuscodes	Beschreibung
202	Akzeptiert	Wird bei erfolgreicher Ausführung asynchroner Aufrufe für Bereitstellungsfunktionen wie dem Erstellen von LUNs und Dateifreigaben zurückgegeben.
400	Ungültige Anfrage	Zeigt einen Fehler bei der Eingabevalidierung an. Der Benutzer muss die Eingaben korrigieren, beispielsweise gültige Schlüssel in einem Anforderungstext.
401	Nicht autorisierte Anfrage	Sie sind nicht berechtigt, die Ressource anzuzeigen/Nicht autorisiert.
403	Verbotene Anfrage	Der Zugriff auf die Ressource, die Sie erreichen wollten, ist verboten.
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.
500	Interner Serverfehler	Interner Serverfehler. Die Antwort vom Server konnte nicht abgerufen werden. Dieser interne Serverfehler kann dauerhaft sein, muss es aber nicht. Wenn Sie beispielsweise eine `GET` oder `GET ALL` Wenn Sie den Vorgang ausführen und diesen Fehler erhalten, wird empfohlen, diesen Vorgang mindestens fünfmal zu wiederholen. Handelt es sich um einen permanenten Fehler, lautet der zurückgegebene Statuscode weiterhin 500. Wenn der Vorgang erfolgreich ist, lautet der zurückgegebene Statuscode 200.

Empfehlungen zur Verwendung der APIs für Active IQ Unified Manager

Wenn Sie die APIs in Active IQ Unified Manager verwenden, sollten Sie bestimmte empfohlene Vorgehensweisen befolgen.

- Für eine gültige Ausführung müssen alle Antwortinhaltstypen das folgende Format aufweisen:

```
application/json
```

- Die API-Versionsnummer hat nichts mit der Produktversionsnummer zu tun. Sie sollten die neueste Version der API verwenden, die für Ihre Unified Manager-Instanz verfügbar ist. Weitere Informationen zu den API-Versionen von Unified Manager finden Sie im Abschnitt „REST-API-Versionierung in Active IQ Unified Manager“.
- Beim Aktualisieren von Array-Werten mithilfe einer Unified Manager-API müssen Sie die gesamte Wertezeichenfolge aktualisieren. Sie können einem Array keine Werte anhängen. Sie können nur ein vorhandenes Array ersetzen.
- Sie können Filteroperatoren wie Pipe (|) und Platzhalter (*) für alle Abfrageparameter verwenden, mit Ausnahme von Doppelwerten, beispielsweise IOPS und Leistung in den Metrik-APIs.
- Vermeiden Sie die Abfrage von Objekten, indem Sie eine Kombination der Filteroperatoren Platzhalter (*) und Pipe (|) verwenden. Möglicherweise wird eine falsche Anzahl von Objekten abgerufen.
- Bei der Verwendung von Werten für Filter ist darauf zu achten, dass der Wert keine `?` Charakter. Dies dient dazu, das Risiko einer SQL-Injection zu verringern.
- Beachten Sie, dass die `GET` (Alle) Anfragen für eine beliebige API geben maximal 1000 Datensätze zurück. Auch wenn Sie die Abfrage ausführen, indem Sie die `max_records` auf einen Wert über 1000 setzen, werden nur 1000 Datensätze zurückgegeben.
- Für die Durchführung administrativer Funktionen wird die Verwendung der Unified Manager-Benutzeroberfläche empfohlen.

Protokolle zur Fehlerbehebung

Mithilfe von Systemprotokollen können Sie die Ursachen von Fehlern analysieren und Probleme beheben, die beim Ausführen der APIs auftreten können.

Rufen Sie die Protokolle vom folgenden Speicherort ab, um Probleme im Zusammenhang mit den API-Aufrufen zu beheben.

Protokollspeicherort	Verwenden
`/var/log/ocie/access_log.log`	Enthält alle API-Aufrufdetails, wie etwa den Benutzernamen des Benutzers, der die API aufruft, Startzeit, Ausführungszeit, Status und URL. Sie können diese Protokolldatei verwenden, um die häufig verwendeten APIs zu überprüfen oder Fehler in jedem GUI-Workflow zu beheben. Sie können es auch verwenden, um Analysen basierend auf der Ausführungszeit zu skalieren.

Protokollspeicherort	Verwenden
`/var/log/ocum/ocumserver.log`	Enthält alle API-Ausführungsprotokolle. Sie können diese Protokolldatei zur Fehlerbehebung und zum Debuggen der API-Aufrufe verwenden.
`/var/log/ocie/server.log`	Enthält alle Wildfly-Serverbereitstellungen und Protokolle zum Starten/Stoppen des Dienstes. Mithilfe dieser Protokolldatei können Sie die Grundursache aller Probleme ermitteln, die beim Starten, Stoppen oder Bereitstellen des Wildfly-Servers auftreten.
`/var/log/ocie/au.log`	Enthält Protokolle zur Erfassungseinheit. Sie können diese Protokolldatei verwenden, wenn Sie Objekte in ONTAP erstellt, geändert oder gelöscht haben, diese jedoch nicht für die Active IQ Unified Manager REST-APIs berücksichtigt werden.

Jobobjekte asynchrone Prozesse

Active IQ Unified Manager bietet die `jobs` API, die Informationen zu den Jobs abruft, die während der Ausführung anderer APIs ausgeführt werden. Sie müssen wissen, wie die asynchrone Verarbeitung mithilfe des Job-Objekts funktioniert.

Die Ausführung einiger API-Aufrufe, insbesondere jener zum Hinzufügen oder Ändern von Ressourcen, kann länger dauern als die Ausführung anderer Aufrufe. Unified Manager verarbeitet diese lang andauernden Anfragen asynchron.

Asynchrone Anforderungen, beschrieben mithilfe des Job-Objekts

Nach einem asynchron ausgeführten API-Aufruf zeigt der HTTP-Antwortcode 202 an, 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 weiterläuft. Die Antwort enthält das Job-Objekt, das die Anfrage verankert, einschließlich seiner eindeutigen Kennung.

Abfragen des mit einer API-Anforderung verknüpften Job-Objekts

Das in der HTTP-Antwort zurückgegebene Job-Objekt enthält mehrere Eigenschaften. Sie können die Statuseigenschaft abfragen, um festzustellen, ob die Anforderung erfolgreich abgeschlossen wurde. Ein Job-Objekt kann einen der folgenden Zustände aufweisen:

- `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):

- Standard-Polling-Anfrage: Der aktuelle Jobstatus wird sofort zurückgegeben.
- Lange Polling-Anforderung: Wenn der Job-Status wechselt zu `NORMAL, ERROR,` oder `PARTIAL_FAILURES.`

Schritte in einer asynchronen Anfrage

Sie können das folgende allgemeine Verfahren verwenden, um einen asynchronen API-Aufruf abzuschließen:

1. Führen Sie den asynchronen API-Aufruf aus.
2. Erhalten Sie eine HTTP-Antwort 202, die die erfolgreiche Annahme der Anfrage anzeigt.
3. Extrahieren Sie die Kennung für das Job-Objekt aus dem Antworttext.
4. Warten Sie innerhalb einer Schleife, bis das Job-Objekt den Endzustand erreicht `NORMAL, ERROR,` oder `PARTIAL_FAILURES.`
5. Überprüfen Sie den Endstatus des Jobs und rufen Sie das Jobergebnis ab.

Hallo API-Server

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 Ihnen grundlegende Details zum API-Server im JSON-Format (der Server unterstützt nur `application/json` Format).

Die verwendete URI lautet: `https://<hostname>/api/datacenter/svm/svms`. Dieser Beispielcode verwendet 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. Beachten Sie die folgenden Hinweise zum Beispielcode:

- Verwendet eine HTTPS-Verbindung zum Active IQ Unified Manager, um die angegebene REST-URI aufzurufen
- Ignoriert das vom Active IQ Unified Manager bereitgestellte Zertifikat
- Überspringt die Hostnamenüberprüfung während des Handshakes
- Anwendung `javax.net.ssl.HttpsURLConnection` für eine URI-Verbindung
- Verwendet eine Drittanbieterbibliothek(`org.apache.commons.codec.binary.Base64`) zum Erstellen der Base64-codierten Zeichenfolge, die in der HTTP-Basisauthentifizierung verwendet wird

Zum Kompilieren und Ausführen des Beispielcodes müssen Sie den Java-Compiler 1.8 oder höher verwenden.

```
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

Die REST-APIs für Active IQ Unified Manager sind in diesem Abschnitt nach Kategorien aufgelistet.

Sie können die Online-Dokumentationsseite Ihrer Unified Manager-Instanz anzeigen, die die Details jedes REST-API-Aufrufs enthält. Dieses Dokument wiederholt nicht die Details der Online-Dokumentation. 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 überprüfen, einschließlich der Eingabeparameter, Ausgabeformate, HTTP-Statuscodes und des Anforderungsverarbeitungstyps.

Die folgenden Informationen sind für jeden API-Aufruf innerhalb eines Workflows enthalten, um das Auffinden des Aufrufs auf der Dokumentationsseite zu erleichtern:

- Kategorie

  Die API-Aufrufe sind auf der Dokumentationsseite in funktional verwandte Bereiche oder Kategorien unterteilt. Um einen bestimmten API-Aufruf zu finden, scrollen Sie zum Ende der Seite und klicken Sie dann auf die entsprechende API-Kategorie.

- HTTP-Verb (Aufruf)

  Das HTTP-Verb identifiziert die an einer Ressource ausgeführte Aktion. Jeder API-Aufruf wird über ein einzelnes HTTP-Verb ausgeführt.

- Weg

  Der Pfad bestimmt die spezifische Ressource, die die Aktion im Rahmen der Ausführung eines Aufrufs verwendet. Die Pfadzeichenfolge wird an die Kern-URL angehängt, um die vollständige URL zur Identifizierung der Ressource zu bilden.

Verwalten von Speicherobjekten in einem Rechenzentrum mithilfe von APIs

Die REST-APIs unter dem `datacenter` Mit der Kategorie „Speicherobjekte“ können Sie die Speicherobjekte in Ihrem Rechenzentrum verwalten, z. B. Cluster, Knoten, Aggregate, Speicher-VMs, Volumes, LUNs, Dateifreigaben und Namespaces. Diese APIs stehen zum Abfragen der Konfiguration der Objekte zur Verfügung, während einige von ihnen Ihnen das Ausführen von Vorgängen zum Hinzufügen, Löschen oder Ändern dieser Objekte ermöglichen.

Bei den meisten dieser APIs handelt es sich um GET-Aufrufe, die eine clusterübergreifende Aggregation mit Filter-, Sortier- und Paginierungsunterstützung bieten. Beim Ausführen dieser APIs geben sie Daten aus der Datenbank zurück. Daher müssen die neu erstellten Objekte im nächsten Erfassungszyklus erkannt werden, damit sie in der Antwort erscheinen.

Wenn Sie die Details eines bestimmten Objekts abfragen möchten, müssen Sie die eindeutige ID dieses Objekts eingeben, um dessen Details anzuzeigen. Beispielsweise finden Sie die Metriken und Analyseinformationen der Speicherobjekte unter"Anzeigen von Leistungsmetriken" .

```
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 an die APIs sind auf Ihrer Swagger-API-Schnittstelle verfügbar. Sie können die Ergebnisse nach bestimmten Parametern filtern und sortieren, wie auf Swagger angegeben. Mit diesen APIs können Sie die Ergebnisse nach bestimmten Speicherobjekten filtern, beispielsweise nach Cluster, Volume oder Speicher-VM.

APIs für Speicherobjekte in Ihrem Rechenzentrum

HTTP-Verb	Weg	Beschreibung

`GET`	`/datacenter/cluster/clusters`
	
	`/datacenter/cluster/clusters/{key}`
		Mit dieser Methode können Sie die Details der ONTAP Cluster im gesamten Rechenzentrum anzeigen. Die API gibt Informationen zurück, wie etwa die IPv4- oder IPv6-Adresse des Clusters, Informationen zum Knoten, wie etwa Knotenzustand, Leistungskapazität und Hochverfügbarkeitspaar (HA), und gibt an, ob es sich bei dem Cluster um ein reines SAN-Array handelt.

HTTP-Verb	Weg	Beschreibung
GET	`/datacenter/cluster/licensing/licenses` `/datacenter/cluster/licensing/licenses/{key}`	Gibt die Details der auf den Clustern in Ihrem Rechenzentrum installierten Lizenzen zurück. Sie können Ihre Ergebnisse anhand der erforderlichen Kriterien filtern. Es werden Informationen wie Lizenzschlüssel, Clusterschlüssel, Ablaufdatum und Lizenzumfang zurückgegeben. 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 Rechenzentrum anzeigen. Sie können Informationen zum Cluster, zur Knotenintegrität, zur Leistungskapazität und zum Hochverfügbarkeitspaar (HA) für den Knoten anzeigen.

GET	`/datacenter/protocols/cifs/shares`
	
	`/datacenter/protocols/cifs/shares/{key}`
		Mit dieser Methode können Sie die Details der CIFS-Freigaben im Rechenzentrum anzeigen. Neben Cluster-, SVM- und Volume-Details werden auch Informationen zur Access Control List (ACL) zurückgegeben.

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-Dienste anzeigen.
		
		Sie können die Exportrichtlinien für einen Cluster oder eine Speicher-VM abfragen und den Exportrichtlinienschlüssel für die Bereitstellung von NFS-Dateifreigaben wiederverwenden. Weitere Informationen zum Zuweisen und Wiederverwenden von Exportrichtlinien für Workloads finden Sie unter „Bereitstellung von CIFS- und NFS-Dateifreigaben“.

HTTP-Verb	Weg	Beschreibung
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	Mit dieser Methode können Sie die Sammlung von Aggregaten im Rechenzentrum oder ein bestimmtes Aggregat anzeigen, um Workloads darauf bereitzustellen oder zu überwachen. Es werden Informationen wie Cluster- und Knotendetails, genutzte Leistungskapazität, verfügbarer und genutzter Speicherplatz sowie Speichereffizienz zurückgegeben.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	Mit dieser Methode können Sie die LUN-Sammlung im gesamten Rechenzentrum anzeigen. Sie können Informationen zur LUN anzeigen, z. B. Cluster- und SVM-Details, QoS-Richtlinien und igroups.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	Mit dieser Methode können Sie die Details aller QoS-Richtlinien anzeigen, die für die Speicherobjekte im Rechenzentrum gelten. Es werden Informationen wie Cluster- und SVM-Details, die festen oder adaptiven Richtliniendetails und die Anzahl der für diese Richtlinie geltenden Objekte zurückgegeben.
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	Mit dieser Methode können Sie die Qtree-Details im gesamten Rechenzentrum für alle FlexVol Volumes oder FlexGroup -Volumes anzeigen. Es werden Informationen wie Cluster- und SVM-Details, FlexVol volume und Exportrichtlinie zurückgegeben.

HTTP-Verb	Weg	Beschreibung

`GET`	`/datacenter/storage/volumes`
	
	`/datacenter/storage/volumes/{key}`
		Mit dieser Methode können Sie die Volume-Sammlung im Rechenzentrum anzeigen. Es werden Informationen zu den Volumes zurückgegeben, beispielsweise SVM- und Clusterdetails, QoS- und Exportrichtlinien sowie Angaben dazu, ob das Volume vom Typ „Lese-/Schreibzugriff“, „Datenschutz“ oder „Lastverteilung“ ist.
		
		Für FlexVol und FlexClone -Volumes können Sie die Informationen zu den jeweiligen Aggregaten anzeigen. Für ein FlexGroup -Volume gibt die Abfrage die Liste der Bestandteilaggregate zurück.

HTTP-Verb	Weg	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. Wenn eine vorhandene Igroup vorhanden ist, können Sie sie zuweisen. Sie können auch igroups erstellen und sie den LUNs zuweisen.
		
		Mit diesen Methoden können Sie igroups abfragen, erstellen, löschen und ändern.
		
		Zu beachtende Punkte:
		
		• `POST:`Beim Erstellen einer igroup können Sie die Speicher-VM angeben, auf die Sie Zugriff zuweisen möchten.
		• `DELETE:`Sie müssen den Igroup-Schlüssel als Eingabeparameter angeben, um eine bestimmte Igroup zu löschen. Wenn Sie einer LUN bereits eine Igroup zugewiesen haben, können Sie diese Igroup nicht löschen.
		• `PATCH:`Sie müssen den Igroup-Schlüssel als Eingabeparameter angeben, um eine bestimmte Igroup zu ändern. Sie müssen außerdem die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben.

HTTP-Verb	Weg	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 Speicher-VM-Objekt, das Sie erstellen möchten, als Eingabeparameter eingeben. Sie können eine benutzerdefinierte Speicher-VM erstellen und ihr dann die erforderlichen Eigenschaften zuweisen.
		• `DELETE:`Sie müssen den Speicher-VM-Schlüssel angeben, um eine bestimmte Speicher-VM zu löschen.
		• `PATCH:`Sie müssen den Speicher-VM-Schlüssel angeben, um eine bestimmte Speicher-VM zu ändern. Sie müssen außerdem die Eigenschaften, die Sie aktualisieren möchten, zusammen mit ihren Werten eingeben.

Zu beachtende Punkte:

Wenn Sie in Ihrer Umgebung die SLO-basierte Workloadbereitstellung aktiviert haben, stellen Sie beim Erstellen der Speicher-VM sicher, dass sie alle für die Bereitstellung von LUNs und Dateifreigaben darauf erforderlichen Protokolle unterstützt, z. B. CIFS oder SMB, NFS, FCP und iSCSI. Die Bereitstellungs-Workflows können fehlschlagen, wenn die Speicher-VM die erforderlichen Dienste nicht unterstützt. Es wird empfohlen, die Dienste für die jeweiligen Arten von Workloads auch auf der Storage-VM zu aktivieren.

Wenn Sie die SLO-basierte Workloadbereitstellung in Ihrer Umgebung aktiviert haben, können Sie die Speicher-VM, auf der Speicher-Workloads bereitgestellt wurden, nicht löschen. Wenn Sie eine Speicher-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 CIFS- oder SMB-Servername bleibt jedoch in der Active Directory-Konfiguration erhalten und muss manuell vom Active Directory-Server gelöscht werden.

APIs für Netzwerkelemente in Ihrem Rechenzentrum

Die folgenden APIs in der Kategorie „Rechenzentrum“ rufen Informationen zu den Ports und Netzwerkschnittstellen in Ihrer Umgebung ab, insbesondere zu den FC-Ports, FC-Schnittstellen, Ethernet-Ports und IP-Schnittstellen.

HTTP-Verb	Weg	Beschreibung
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	Ruft Informationen zu allen Ethernet-Ports in Ihrer Rechenzentrumsumgebung ab. Mit einem Portschlüssel als Eingabeparameter können Sie die Informationen zu diesem bestimmten Port anzeigen. Es werden Informationen wie Clusterdetails, Broadcastdomäne, Portdetails wie Status, Geschwindigkeit und Typ sowie die Angabe, ob der Port aktiviert ist, abgerufen.
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	Mit dieser Methode können Sie die Details der FC-Schnittstellen in Ihrer Rechenzentrumsumgebung anzeigen. Mit einem Schnittstellenschlüssel als Eingabeparameter können Sie die Informationen zu dieser bestimmten Schnittstelle anzeigen. Es werden Informationen wie Clusterdetails, Home-Knotendetails und Home-Portdetails abgerufen.
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	Ruft Informationen zu allen FC-Ports ab, die in den Knoten in Ihrer Rechenzentrumsumgebung verwendet werden. Mit einem Portschlüssel als Eingabeparameter können Sie die Informationen zu diesem bestimmten Port anzeigen. Es werden Informationen wie Clusterdetails, Portbeschreibung, unterstütztes Protokoll und der Status des Ports abgerufen.

HTTP-Verb	Weg	Beschreibung
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	Mit dieser Methode können Sie die Details der IP-Schnittstellen in Ihrer Rechenzentrumsumgebung anzeigen. Mit einem Schnittstellenschlüssel als Eingabeparameter können Sie die Informationen zu dieser bestimmten Schnittstelle anzeigen. Es werden Informationen wie Clusterdetails, IPspace-Details, Home-Node-Details und ob Failover aktiviert ist, abgerufen.

Greifen Sie über Proxy-Zugriff auf ONTAP -APIs zu

Die Gateway-APIs bieten Ihnen den Vorteil, dass Sie die Active IQ Unified Manager Anmeldeinformationen zum Ausführen von ONTAP REST-APIs und zum Verwalten von Speicherobjekten verwenden können. Diese APIs sind verfügbar, wenn die API-Gateway-Funktion über die Unified Manager-Web-Benutzeroberfläche aktiviert ist.

Unified Manager REST-APIs unterstützen nur eine ausgewählte Reihe von Aktionen, die auf den Unified Manager-Datenquellen, d. h. ONTAP Clustern, ausgeführt werden können. Sie können die anderen Funktionen über ONTAP -APIs nutzen. Die Gateway-APIs ermöglichen es Unified Manager, als Pass-Through-Schnittstelle zum Tunneln aller API-Anfragen zu fungieren, die auf den von ihm verwalteten ONTAP Clustern ausgeführt werden sollen, ohne dass eine Anmeldung bei jedem Rechenzentrumscluster einzeln erforderlich ist. Es fungiert als zentraler Verwaltungspunkt für die Ausführung der APIs in den ONTAP Clustern, die von Ihrer Unified Manager-Instanz verwaltet werden. Die API-Gateway-Funktion ermöglicht es Unified Manager, eine einzige Steuerebene zu sein, von der aus Sie mehrere ONTAP Cluster verwalten können, ohne sich einzeln bei ihnen anmelden zu müssen. Mit den Gateway-APIs können Sie bei Unified Manager angemeldet bleiben und die ONTAP Cluster verwalten, indem Sie ONTAP REST-API-Operationen ausführen.

Alle Benutzer können mithilfe der GET-Operation eine Abfrage ausführen. Anwendungsadministratoren können alle ONTAP REST-Vorgänge ausführen.

Das Gateway fungiert als Proxy zum Tunneln der API-Anfragen, indem es die Header- und Body-Anfragen im gleichen Format wie in den ONTAP -APIs verwaltet. Sie können Ihre Unified Manager-Anmeldeinformationen verwenden und die spezifischen Vorgänge ausführen, um auf die ONTAP -Cluster zuzugreifen und sie zu verwalten, ohne einzelne Cluster-Anmeldeinformationen weiterzugeben. Es verwaltet weiterhin die Clusterauthentifizierung und das Clustermanagement, leitet die API-Anfragen jedoch um, sodass sie direkt auf dem jeweiligen Cluster ausgeführt werden. Die von den APIs zurückgegebene Antwort ist dieselbe wie die Antwort, die von den jeweiligen ONTAP REST-APIs zurückgegeben wird, die direkt von ONTAP ausgeführt werden.

HTTP-Verb	Pfad (URL)	Beschreibung
GET	/gateways	Diese GET-Methode ruft die Liste aller von Unified Manager verwalteten Cluster ab, die ONTAP REST-Aufrufe unterstützen. Sie können die Clusterdetails überprüfen und basierend auf der Cluster-UUID oder der Universal Unique Identifier (UUID) andere 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. Stellen Sie außerdem sicher, dass die UUID zum Cluster gehört, der von ONTAP 9.5 oder höher unterstützt wird, und über HTTPS zu Unified Manager hinzugefügt wurde. {path} muss durch die ONTAP REST-URL ersetzt werden. Sie müssen entfernen `/api/` aus der URL.
		Dies ist eine Single-Point-Proxy-API, die POST-, DELETE-, PATCH-Operationen und GET für alle ONTAP REST-APIs unterstützt. Für die API gelten keine Einschränkungen, solange sie von ONTAP unterstützt wird. Die Tunnel- oder Proxy-Funktionalität kann nicht deaktiviert werden.
		
		Der `OPTIONS` Die Methode gibt alle von einer ONTAP REST-API unterstützten Vorgänge zurück. Wenn beispielsweise eine ONTAP -API nur die `GET` Betrieb, Ausführen der `OPTIONS` Methode durch Verwendung dieser Gateway-API gibt `GET` als Antwort. Diese Methode wird von Swagger nicht unterstützt, kann aber mit anderen API-Tools ausgeführt werden.
		
		Der `OPTIONS` Methode ermittelt, ob eine Ressource verfügbar ist. Mit diesem Vorgang können die Metadaten zu einer Ressource in den HTTP-Antwortheadern angezeigt werden. Diese Methode wird von Swagger nicht unterstützt, kann aber mit anderen API-Tools ausgeführt werden.

Verstehen Sie das API Gateway-Tunneling

Mit den Gateway-APIs können Sie ONTAP Objekte über Unified Manager verwalten. Unified Manager verwaltet die Cluster und Authentifizierungsdetails und leitet die Anfragen an den ONTAP REST-Endpunkt weiter. Die Gateway-API transformiert die URL und Hypermedia als Engine of Application State (HATEOAS)-Links im Header und Antworttext mit der Basis-URL des API-Gateways. Die Gateway-API fungiert als Proxy-Basis-URL, an die Sie die ONTAP REST-URL anhängen und den erforderlichen ONTAP REST-Endpunkt ausführen.

Damit eine ONTAP -API erfolgreich über das API-Gateway ausgeführt werden kann, muss die API von der Version des ONTAP Clusters unterstützt werden, auf dem sie ausgeführt wird. Das Ausführen 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 ist: `/storage/volumes` . Sie müssen die ONTAP API REST-URL als Wert für den Pfadparameter hinzufügen.

Achten Sie beim Hinzufügen des Pfads darauf, dass Sie das “/” symbol at the beginning of the URL. For the API `/storage/volumes`, hinzufügen `storage/volumes`.

Die angehängte URL lautet: `/gateways/{uuid}/storage/volumes`

Beim Ausführen des `GET` Bei dieser Operation lautet die generierte URL wie folgt: `GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes`

Der `/api` Tag der ONTAP REST-URL wird in der angehängten URL entfernt und der für die Gateway-API bleibt erhalten.

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 Speichervolumes in diesem Cluster zurück. Das Antwortformat ist dasselbe, das Sie erhalten, wenn Sie dieselbe API von ONTAP ausführen. Die zurückgegebenen Statuscodes sind die ONTAP REST-Statuscodes.

API-Bereich festlegen

Für alle APIs ist ein Kontext innerhalb des Clusterbereichs festgelegt. APIs, die auf Basis von Storage-VMs arbeiten, haben ebenfalls den Cluster als Geltungsbereich, d. h. die API-Operationen werden auf einer bestimmten Storage-VM innerhalb eines verwalteten Clusters ausgeführt. Wenn Sie das `/gateways/{uuid}/{path}` API: Stellen Sie sicher, dass Sie die Cluster-UUID (Unified Manager-Datenquellen-UUID) für den Cluster eingeben, auf dem Sie den Vorgang ausführen. Um den Kontext auf eine bestimmte Speicher-VM innerhalb dieses Clusters festzulegen, geben Sie den Speicher-VM-Schlüssel als Parameter X-Dot-SVM-UUID oder den Speicher-VM-Namen als Parameter X-Dot-SVM-Name ein. Der Parameter wird als Filter im String-Header hinzugefügt und der Vorgang wird im Rahmen dieser Speicher-VM innerhalb dieses Clusters 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 unterhttps://docs.netapp.com/us-en/ontap-automation/index.html["ONTAP REST API-Automatisierung"]

Ausführen von Verwaltungsaufgaben mithilfe von APIs

Sie können die APIs unter dem `administration` Kategorie zum Ändern der Sicherungseinstellungen, Überprüfen der Sicherungsdateiinformationen und Clusterzertifikate sowie zum Verwalten von ONTAP Clustern als Active IQ Unified

Manager -Datenquellen.

Zum Ausführen dieser Vorgänge müssen Sie über die Rolle „Anwendungsadministrator“ verfügen. Sie können zum Konfigurieren dieser Einstellungen auch die Web-Benutzeroberfläche von Unified Manager verwenden.

HTTP-Verb	Weg	Beschreibung

`GET`
 	
`PATCH`
	`/admin/backup-settings`
	
	`/admin/backup-settings`
		Sie können die `GET` Methode zum Anzeigen der Einstellungen des Sicherungszeitplans, der standardmäßig in Unified Manager konfiguriert ist. Sie können Folgendes überprüfen:
		• Ob der Zeitplan aktiviert oder deaktiviert ist
		• Häufigkeit der geplanten Sicherung (täglich oder wöchentlich)
		• Zeitpunkt der Sicherung
		• Maximale Anzahl von Sicherungsdateien, die in der Anwendung aufbewahrt werden sollen
		
		Die Uhrzeit der Sicherung entspricht der Zeitzone des Servers.
		
		Die Datenbanksicherungseinstellungen sind standardmäßig im Unified Manager verfügbar und Sie können keinen Sicherungszeitplan erstellen. Sie können jedoch die `PATCH` Methode zum Ändern der Standardeinstellungen.

`GET`	`/admin/backup-file-info`	Bei jeder Änderung des Sicherungszeitplans für Unified Manager wird eine Sicherungsdumpdatei erstellt. Mit dieser Methode können Sie überprüfen, ob die Sicherungsdatei gemäß den geänderten Sicherungseinstellungen erstellt wird und ob die Informationen in der Datei mit den geänderten Einstellungen übereinstimmen.

HTTP-Verb	Weg	Beschreibung
GET	/admin/datasource-certificate	Mit dieser Methode können Sie das Datenquellenzertifikat (Cluster) aus dem Trust Store anzeigen. Vor dem Hinzufügen eines ONTAP Clusters als Unified Manager-Datenquelle ist die Validierung des Zertifikats erforderlich.
GET POST PATCH DELETE	/admin/datasources/clusters /admin/datasources/clusters/{key}	Sie können die GET Methode zum Abrufen der Details der von Unified Manager verwalteten Datenquellen (ONTAP Cluster). Sie können Unified Manager auch einen neuen Cluster als Datenquelle hinzufügen. Zum Hinzufügen eines Clusters müssen Sie dessen Hostnamen, Benutzernamen und Kennwort kennen. Verwenden Sie zum Ändern und Löschen eines Clusters, der von Unified Manager als Datenquelle verwaltet wird, den ONTAP Clusterschlüssel.

Verwalten von Benutzern mithilfe von APIs

Sie können die APIs in der security Kategorie zur Steuerung des Benutzerzugriffs auf ausgewählte Clusterobjekte im Active IQ Unified Manager. Sie können lokale Benutzer oder Datenbankbenutzer hinzufügen. Sie können auch Remotebenutzer oder -gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Basierend auf den Berechtigungen der Rollen, die Sie den Benutzern zuweisen, können diese die Speicherobjekte verwalten oder die Daten in Unified Manager anzeigen.

Zum Ausführen dieser Vorgänge müssen Sie über die Rolle „Anwendungsadministrator“ verfügen. Sie können zum Konfigurieren dieser Einstellungen auch die Web-Benutzeroberfläche von Unified Manager verwenden.

Die APIs unter der security Kategorie verwenden Sie den Benutzerparameter, also den Benutzernamen und nicht den Schlüsselparameter als eindeutige Kennung für die Benutzerentität.

HTTP-Verb	Weg	Beschreibung

`GET`
 	
`POST`
	`/security/users`
	
	`/security/users`
		Sie können diese Methoden verwenden, um die Details von Benutzern abzurufen oder neue Benutzer zu Unified Manager hinzuzufügen.
		
		Sie können den Benutzern basierend auf ihren Benutzertypen bestimmte Rollen zuweisen. Beim Hinzufügen von Benutzern müssen Sie Kennwörter für den lokalen Benutzer, den Wartungsbenutzer und den Datenbankbenutzer angeben.

`GET`
 	
`PATCH`
 	
`DELETE`
	`/security/users/{name}`	Mit der GET-Methode können Sie alle Details eines Benutzers abrufen, z. B. Name, E-Mail-Adresse, Rolle und Autorisierungstyp. Mit der PATCH-Methode können Sie die Details aktualisieren. Mit der DELETE-Methode können Sie den Benutzer entfernen.

Anzeigen von Leistungsmetriken mithilfe von APIs

Active IQ Unified Manager bietet Ihnen eine Reihe von APIs unter dem `/datacenter` Kategorie, mit der Sie die Leistungsdaten Ihrer Cluster und Speicherobjekte in einem Rechenzentrum anzeigen können. Diese APIs rufen die Leistungsdaten der verschiedenen Speicherobjekte ab, z. B. Cluster, Knoten, LUNs, Volumes, Aggregate, Speicher-VMs, FC-Schnittstellen, FC-Ports, Ethernet-Ports und IP-Schnittstellen.

Der `/metrics` Und `/analytics` APIs bieten verschiedene Ansichten der Leistungsmetriken, mit denen Sie für die folgenden Speicherobjekte in Ihrem Rechenzentrum auf verschiedenen Detailebenen tiefer gehen können:

- Cluster
- Knoten
- Speicher-VMs
- Aggregate
- Bände
- LUNs
- FC-Schnittstellen
- FC-Ports
- Ethernet-Anschlüsse

- IP-Schnittstellen

Die folgende Tabelle vergleicht die `/metrics` Und `/analytics` APIs hinsichtlich der Einzelheiten der abgerufenen Leistungsdaten.

Metriken	Analyse
Leistungsdetails für ein einzelnes Objekt. Zum Beispiel die `/datacenter/cluster/clusters/{key}/metrics` Für die API muss der Clusterschlüssel als Pfadparameter eingegeben werden, um die Metriken für diesen bestimmten Cluster abzurufen.	Leistungsdetails für mehrere Objekte desselben Typs in einem Rechenzentrum. Zum Beispiel die `/datacenter/cluster/clusters/analytics` Die API ruft die kollektiven Metriken aller Cluster in einem Rechenzentrum ab.
Beispiel für Leistungsmetriken für ein Speicherobjekt basierend auf dem Zeitintervallparameter für den Abruf.	Der aggregierte Leistungswert auf hoher Ebene für einen bestimmten Typ von Speicherobjekt für einen bestimmten Zeitraum (über 72 Stunden).
Es werden grundlegende Details des Objekts abgerufen, beispielsweise Details eines Knotens oder Clusters.	Es werden keine spezifischen Details abgerufen.
Für ein einzelnes Objekt werden kumulierte Zähler wie Minimum, Maximum, 95. Perzentil und die durchschnittlichen Leistungswerte über einen bestimmten Zeitraum abgerufen, beispielsweise Lese-, Schreib-, Gesamt- und andere Zähler.	Für alle Objekte desselben Typs wird ein einzelner aggregierter Wert angezeigt.

Metriken	Analyse
Der Zeitbereich und die Beispieldaten basieren auf dem folgenden Zeitplan: Der Zeitbereich für die Daten. Beispiele können 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m sein. Sie erhalten 1-Stunden-Proben, wenn der Bereich mehr als 3 Tage (72 Stunden) beträgt, andernfalls sind es 5-Minuten-Proben. Der Zeitraum für jeden Zeitbereich ist wie folgt: • 1h: Messwerte der letzten Stunde, abgetastet über 5 Minuten. • 12h: Messwerte der letzten 12 Stunden, abgetastet über 5 Minuten. • 1d: Messwerte des letzten Tages, abgetastet über 5 Minuten. • 2d: Messwerte der letzten 2 Tage, abgetastet über 5 Minuten. • 3d: Messwerte der letzten 3 Tage, abgetastet über 5 Minuten. • 15d: Messwerte der letzten 15 Tage, abgetastet über 1 Stunde. • 1w: Messwerte der letzten Woche, abgetastet über 1 Stunde. • 1 Min.: Messwerte des letzten Monats, abgetastet über 1 Stunde. • 2 m: Messwerte der letzten 2 Monate, erfasst über 1 Stunde. • 3 m: Messwerte der letzten 3 Monate, erfasst über 1 Stunde. • 6 m: Messwerte der letzten 6 Monate, abgetastet über 1 Stunde. Verfügbare Werte: 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m Standardwert: 1 h	Über 72 Stunden. Die Dauer, über die diese Stichprobe berechnet wird, wird im Standardformat ISO-8601 dargestellt.

Ausgabebeispiel für Metrik-APIs

Zum Beispiel die `/datacenter/cluster/nodes/{key}/metrics` Die API ruft (unter anderem) die folgenden Details für einen Knoten ab:

Das 95. Perzentil im Zusammenfassungswert gibt an, dass 95 % der für den Zeitraum gesammelten Proben einen Zählerwert haben, der unter dem als 95. Perzentil angegebenen Wert liegt.

```
{
     "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
      }
    },
```

Ausgabebeispiel für Analyse-APIs

Zum Beispiel die `/datacenter/cluster/nodes/analytics` Die API ruft (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 Leistungsmetriken sind doppelte Werte, zum Beispiel `100.53` . Das Filtern dieser Gleitkommawerte durch Pipe-Zeichen (|) und Platzhalterzeichen (*) wird nicht unterstützt.

HTTP-Verb	Weg	Beschreibung
GET	/datacenter/cluster/clusters/{key}/metrics	Ruft Leistungsdaten (Beispiel und Zusammenfassung) für einen Cluster ab, der durch den Eingabeparameter des Clusterschlüssels angegeben ist. Es werden Informationen wie Clusterschlüssel und UUID, Zeitbereich, IOPS, Durchsatz und Anzahl der Samples zurückgegeben.
GET	/datacenter/cluster/clusters/analytics	Ruft Leistungsmetriken auf hoher Ebene für alle Cluster in einem Rechenzentrum ab. Sie können Ihre Ergebnisse anhand der erforderlichen Kriterien filtern. Es werden Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) zurückgegeben.
GET	/datacenter/cluster/nodes/{key}/metrics	Ruft Leistungsdaten (Beispiel und Zusammenfassung) für einen Knoten ab, der durch den Eingabeparameter des Knotenschlüssels angegeben ist. Es werden Informationen wie die Knoten-UUID, der Zeitbereich, eine Zusammenfassung der IOPS, des Durchsatzes, der Latenz und der Leistung, die Anzahl der gesammelten Samples und der genutzte Prozentsatz zurückgegeben.
GET	/datacenter/cluster/nodes/analytics	Ruft Leistungsmetriken auf hoher Ebene für alle Knoten in einem Rechenzentrum ab. Sie können Ihre Ergebnisse anhand der erforderlichen Kriterien filtern. Es werden Informationen wie Knoten- und Clusterschlüssel sowie Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) zurückgegeben.

HTTP-Verb	Weg	Beschreibung
GET	`/datacenter/storage/aggregates/{key}/metrics`	Ruft Leistungsdaten (Beispiel und Zusammenfassung) für ein Aggregat ab, das durch den Eingabeparameter des Aggregatschlüssels angegeben wird. Es werden Informationen wie der Zeitbereich, eine Zusammenfassung der IOPS, Latenz, Durchsatz und Leistungskapazität, die Anzahl der für jeden Zähler erfassten Stichproben und der genutzte Prozentsatz zurückgegeben.
GET	`/datacenter/storage/aggregates/analytics`	Ruft Leistungsmetriken auf hoher Ebene für alle Aggregate in einem Rechenzentrum ab. Sie können Ihre Ergebnisse anhand der erforderlichen Kriterien filtern. Es werden Informationen wie Aggregat- und Clusterschlüssel sowie Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) zurückgegeben.

GET	`/datacenter/storage/luns/{key}/metrics`
	
	`/datacenter/storage/volumes/{key}/metrics`
		Ruft Leistungsdaten (Beispiel und Zusammenfassung) für eine LUN oder eine Dateifreigabe (Volume) ab, die durch den Eingabeparameter des LUN- oder Volume-Schlüssels angegeben ist. Es werden Informationen wie die Zusammenfassung der Mindest-, Höchst- und Durchschnittswerte der Lese-, Schreib- und Gesamt-IOPS, der Latenz und des Durchsatzes sowie die Anzahl der für jeden Zähler erfassten Stichproben zurückgegeben.

HTTP-Verb	Weg	Beschreibung

GET	`/datacenter/storage/luns/analytics`
	
	`/datacenter/storage/volumes/analytics`
		Ruft Leistungsmetriken auf hoher Ebene für alle LUNs oder Volumes in einem Rechenzentrum ab. Sie können Ihre Ergebnisse anhand der erforderlichen Kriterien filtern. Es werden Informationen wie Speicher-VM- und Clusterschlüssel sowie Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) zurückgegeben.

GET	`/datacenter/svm/svms/{key}/metrics`	Ruft Leistungsdaten (Beispiel und Zusammenfassung) für eine Speicher-VM ab, die durch den Eingabeparameter des Speicher-VM-Schlüssels angegeben ist. Zusammenfassung der IOPS basierend auf jedem unterstützten Protokoll, wie z. B. `nvmf, fcp, iscsi,` Und `nfs` , Durchsatz, Latenz und die Anzahl der gesammelten Samples werden zurückgegeben.
GET	`/datacenter/svm/svms/analytics`	Ruft Leistungsmetriken auf hoher Ebene für alle Speicher-VMs in einem Rechenzentrum ab. Sie können Ihre Ergebnisse anhand der erforderlichen Kriterien filtern. Es werden Informationen wie die UUID der Speicher-VM, aggregierte IOPS, Latenz, Durchsatz und der Erfassungszeitraum (in Stunden) zurückgegeben.
GET	`/datacenter/network/ethernet/ports/{key}/metrics`	Ruft die Leistungsmetriken für einen bestimmten Ethernet-Port ab, der durch den Eingabeparameter des Portschlüssels angegeben wird. Wenn ein Intervall (Zeitbereich) aus dem unterstützten Bereich angegeben wird, gibt die API die kumulierten Zähler zurück, z. B. die minimalen, maximalen und durchschnittlichen Leistungswerte über den Zeitraum.

HTTP-Verb	Weg	Beschreibung
GET	/datacenter/network/ethernet/ports/analytics	Ruft die Leistungsmetriken auf hoher Ebene für alle Ethernet-Ports in Ihrer Rechenzentrumsumgebung ab. Es werden Informationen wie Cluster- und Knotenschlüssel und UUID, Durchsatz, Erfassungszeitraum und Auslastung in Prozent für die Ports zurückgegeben. Sie können das Ergebnis nach den verfügbaren Parametern filtern, z. B. nach Portschlüssel, Auslastung in Prozent, Cluster- und Knotenname und UUID usw.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Ruft die Leistungsmetriken 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 kumulierten Zähler zurück, z. B. die minimalen, maximalen und durchschnittlichen Leistungswerte über den Zeitraum.
GET	/datacenter/network/fc/interfaces/analytics	Ruft die Leistungsmetriken auf hoher Ebene für alle Ethernet-Ports in Ihrer Rechenzentrumsumgebung ab. Es werden Informationen wie Cluster- und FC-Schnittstellenschlüssel und UUID, Durchsatz, IOPS, Latenz und Speicher-VM zurückgegeben. Sie können das Ergebnis nach den verfügbaren Parametern filtern, z. B. nach Cluster- und FC-Schnittstellenname und UUID, Speicher-VM, Durchsatz usw.

HTTP-Verb	Weg	Beschreibung
GET	/datacenter/network/fc/ports/{key}/metrics	Ruft die Leistungsmetriken für einen bestimmten FC-Port ab, der durch den Eingabeparameter des Portschlüssels angegeben wird. Wenn ein Intervall (Zeitbereich) aus dem unterstützten Bereich angegeben wird, gibt die API die kumulierten Zähler zurück, z. B. die minimalen, maximalen und durchschnittlichen Leistungswerte über den Zeitraum.
GET	/datacenter/network/fc/ports/analytics	Ruft die Leistungsmetriken auf hoher Ebene für alle FC-Ports in Ihrer Rechenzentrumsumgebung ab. Es werden Informationen wie Cluster- und Knotenschlüssel und UUID, Durchsatz, Erfassungszeitraum und Auslastung in Prozent für die Ports zurückgegeben. Sie können das Ergebnis nach den verfügbaren Parametern filtern, z. B. nach Portschlüssel, Auslastung in Prozent, Cluster- und Knotenname und UUID usw.
GET	/datacenter/network/ip/interfaces/{key}/metrics	Ruft die Leistungsmetriken für eine Netzwerk-IP-Schnittstelle ab, wie durch den Eingabeparameter des Schnittstellenschlüssels angegeben. Wenn ein Intervall (Zeitbereich) aus dem unterstützten Bereich angegeben wird, gibt die API Informationen zurück, wie etwa die Anzahl der Samples, die kumulierten Zähler, den Durchsatz und die Anzahl der empfangenen und gesendeten Pakete.

HTTP-Verb	Weg	Beschreibung
GET	/datacenter/network/ip/interfaces/analytics	Ruft die Leistungsmetriken auf hoher Ebene für alle Netzwerk-IP-Schnittstellen in Ihrer Rechenzentrumsumgebung ab. Es werden Informationen wie Cluster- und IP-Schnittstellenschlüssel und UUID, Durchsatz, IOPS und Latenz zurückgegeben. Sie können das Ergebnis nach den verfügbaren Parametern filtern, z. B. nach Cluster- und IP-Schnittstellenname und UUID, IOPS, Latenz, Durchsatz usw.

Anzeigen von Jobs und Systemdetails

Sie können die `jobs` API unter der `management-server` Kategorie, um die Ausführungsdetails asynchroner Vorgänge anzuzeigen. Der `system` API unter der `management-server` Mit der Kategorie können Sie die Instanzdetails in Ihrer Active IQ Unified Manager Umgebung anzeigen.

Jobs anzeigen

In Active IQ Unified Manager werden Vorgänge wie das Hinzufügen und Ändern von Ressourcen durch synchrone und asynchrone API-Aufrufe ausgeführt. Aufrufe, die für die asynchrone Ausführung geplant sind, können durch ein für diesen Aufruf erstelltes Job-Objekt verfolgt werden. Jedes Job-Objekt verfügt über einen eindeutigen Schlüssel zur Identifizierung. Jedes Job-Objekt gibt die Job-Objekt-URI zurück, damit Sie auf den Job zugreifen und seinen Fortschritt verfolgen können. Sie können diese API verwenden, um die Details jeder Ausführung abzurufen.

Mithilfe dieser API können Sie alle Jobobjekte für Ihr Rechenzentrum abfragen, einschließlich historischer Daten. Wenn Sie alle Jobs abfragen, werden standardmäßig die Details der letzten 20 Jobs zurückgegeben, die über die Web-Benutzeroberfläche und die API-Schnittstelle ausgelöst wurden. Verwenden Sie die integrierten Filter, um bestimmte Jobs anzuzeigen. Sie können den Job-Schlüssel auch verwenden, um die Details eines bestimmten Jobs abzufragen und die nächsten Operationen für die Ressourcen auszuführen.

Kategorie	HTTP-Verb	Weg	Beschreibung
Management-Server	ERHALTEN	/management-server/jobs	Gibt die Auftragsdetails aller Aufträge zurück. Ohne Sortierreihenfolge wird das zuletzt übermittelte Job-Objekt oben zurückgegeben.

Kategorie	HTTP-Verb	Weg	Beschreibung
Management-Server	ERHALTEN	`/management-server/jobs/{key}` Geben Sie den Jobschlüssel des Jobobjekts ein, um die spezifischen Details dieses Jobs anzuzeigen.	Gibt die Details des spezifischen Jobobjekts zurück.

Systemdetails anzeigen

Mithilfe der `/management-server/system` API können Sie die instanzspezifischen Details Ihrer Unified Manager-Umgebung abfragen. Die API gibt Informationen zu den Produkten und Diensten zurück, beispielsweise die auf Ihrem System installierte Version von Unified Manager, UUID, Herstellername, Host-Betriebssystem sowie Name, Beschreibung und Status der auf der Unified Manager-Instanz ausgeführten Dienste.

Kategorie	HTTP-Verb	Weg	Beschreibung
Management-Server	ERHALTEN	`/management-server/system`	Zum Ausführen dieser API sind keine Eingabeparameter erforderlich. Standardmäßig werden die Systemdetails der aktuellen Unified Manager-Instanz zurückgegeben.

Verwalten von Ereignissen und Warnungen mithilfe von APIs

Der `events` , `alerts` , Und `scripts` APIs unter der `management-server` Mit der Kategorie „Ereignisse, Warnungen und die mit den Warnungen verknüpften Skripte“ können Sie in Ihrer Active IQ Unified Manager Umgebung verwalten.

Anzeigen und Ändern von Ereignissen

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 und sie auflösen und aktualisieren.

Durch Ausführen des `GET` Methode für die `/management-server/events` API können Sie die Ereignisse in Ihrem Rechenzentrum abfragen, einschließlich historischer Daten. Verwenden Sie die integrierten Filter, z. B. Name, Auswirkungsstufe, Auswirkungsbereich, Schweregrad, Status, Ressourcenname und Ressourcentyp, um bestimmte Ereignisse anzuzeigen. Die Ressourcentyp- und Bereichsparameter geben Informationen über das Speicherobjekt zurück, bei dem das Ereignis aufgetreten ist, und der Auswirkungsbereich gibt Informationen über das Problem zurück, aufgrund dessen das Ereignis ausgelöst wurde, beispielsweise Verfügbarkeit, Kapazität, Konfiguration, Sicherheit, Schutz und Leistung.

Durch Ausführen des PATCH-Vorgangs für diese API können Sie den Lösungsworkflow für das Ereignis aktivieren. Sie können sich selbst oder einem anderen Benutzer ein Ereignis zuweisen und den Empfang des Ereignisses bestätigen. Wenn Sie die Schritte für die Ressourcen ausführen, um das Problem zu beheben, das das Ereignis ausgelöst hat, können Sie diese API verwenden, um das Ereignis als behoben zu markieren.

Weitere Informationen zu Veranstaltungen finden Sie unter"Ereignisse verwalten" .

Kategorie	HTTP-Verb	Weg	Beschreibung
Management-Server	ERHALTEN	`/management-server/events` `/management-server/events/{key}`	Wenn Sie die Methode „Get ALL“ ausführen, besteht der Antworttext aus den Ereignisdetails aller Ereignisse in Ihrem Rechenzentrum. Wenn Sie die Ereignisdetails mit einem bestimmten Schlüssel abrufen, können Sie die Details eines bestimmten Ereignisses anzeigen und die nächsten Vorgänge für die Ressourcen ausführen. Der Antworttext besteht aus den Details dieses Ereignisses.
Management-Server	PATCH	`management-server/events/{key}`	Führen Sie diese API aus, um ein Ereignis zuzuweisen oder den Status in „Bestätigt“ oder „Gelöst“ zu ändern. Mit dieser Methode können Sie das Ereignis auch sich selbst oder einem anderen Benutzer zuweisen. Es handelt sich um eine synchrone Operation.

Verwalten von Warnungen

Ereignisse werden automatisch und kontinuierlich generiert. Unified Manager generiert nur dann eine Warnung, wenn ein Ereignis bestimmte Filterkriterien erfüllt. Sie können die Ereignisse auswählen, für die Warnungen generiert werden sollen. Mithilfe der `/management-server/alerts` API können Sie Warnungen so konfigurieren, dass automatisch Benachrichtigungen gesendet werden, wenn bestimmte Ereignisse oder Ereignisse mit einem bestimmten Schweregrad auftreten.

Weitere Informationen zu Warnungen finden Sie unter"Verwalten von Warnungen" .

Kategorie	HTTP-Verb	Weg	Beschreibung
Management-Server	ERHALTEN	`/management-server/alerts` `/management-server/alerts/{key}`	Fragen Sie alle vorhandenen Warnungen in Ihrer Umgebung oder eine bestimmte Warnung ab, indem Sie den Warnungsschlüssel verwenden. Sie können die Informationen zu den in Ihrer Umgebung generierten Warnungen anzeigen, z. B. die Warnungsbeschreibung, die Aktion, die E-Mail-ID, an die die Benachrichtigung gesendet wird, das Ereignis und den Schweregrad.
Management-Server	POST	`/management-server/alerts`	Mit dieser Methode können Sie Warnungen für bestimmte Ereignisse hinzufügen. Sie müssen den Alarmnamen, die physische oder logische Ressource oder das Ereignis hinzufügen, auf das der Alarm anwendbar ist, ob der Alarm aktiviert ist und ob Sie SNMP-Traps ausgeben. Sie können zusätzliche Details hinzufügen, für die Sie die Warnung generieren möchten, z. B. die Aktion, die Benachrichtigungs-E-Mail-ID, die Skriptdetails, falls Sie ein Warnungsskript hinzufügen usw.

Kategorie	HTTP-Verb	Weg	Beschreibung
Management-Server	PATCH und DELETE	`management-server/events/{key}`	Mit diesen Methoden können Sie bestimmte Warnungen ändern und löschen. Sie können verschiedene Attribute ändern, z. B. Beschreibung, Name sowie das Aktivieren und Deaktivieren der Warnung. Sie können eine Warnung löschen, wenn sie nicht mehr benötigt wird.

Beachten Sie beim Auswählen einer Ressource zum Hinzufügen einer Warnung, dass durch die Auswahl eines Clusters als Ressource nicht automatisch die Speicherobjekte innerhalb dieses Clusters ausgewählt werden. 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.

Skripte verwalten

Mithilfe der `/management-server/scripts` API können Sie eine Warnung auch mit einem Skript verknüpfen, das ausgeführt wird, wenn eine Warnung ausgelöst wird. Sie können Skripte verwenden, um mehrere Speicherobjekte in Unified Manager automatisch zu ändern oder zu aktualisieren. Das Skript ist mit einer Warnung verknüpft. Wenn ein Ereignis eine Warnung auslöst, wird das Skript ausgeführt. Sie können benutzerdefinierte Skripte hochladen und deren Ausführung testen, wenn eine Warnung generiert wird. Sie können Ihrem Skript eine Warnung zuordnen, sodass das Skript ausgeführt wird, wenn für ein Ereignis in Unified Manager eine Warnung ausgelöst wird.

Weitere Informationen zu Skripten finden Sie unter"Skripte verwalten" .

Kategorie	HTTP-Verb	Weg	Beschreibung
Management-Server	ERHALTEN	`/management-server/scripts`	Verwenden Sie diese API, um alle vorhandenen Skripte in Ihrer Umgebung abzufragen. Verwenden Sie den Standardfilter und sortieren Sie nach Vorgängen, um nur bestimmte Skripte anzuzeigen.

Kategorie	HTTP-Verb	Weg	Beschreibung
Management-Server	POST	`/management-server/scripts`	Verwenden Sie diese API, um eine Beschreibung für das Skript hinzuzufügen und die mit einer Warnung verknüpfte Skriptdatei hochzuladen.

Verwalten von Workloads mithilfe von APIs

Die hier beschriebenen APIs decken verschiedene Funktionen der Speicherverwaltung ab, z. B. das Anzeigen von Speicher-Workloads, das Erstellen von LUNs und Dateifreigaben, das Verwalten von Leistungsserviceleveln und Speichereffizienzrichtlinien sowie das Zuweisen der Richtlinien zu Speicher-Workloads.

Anzeigen von Speicherworkloads mithilfe von APIs

Mit den hier aufgeführten APIs können Sie eine konsolidierte Liste der Speicher-Workloads für alle ONTAP Cluster in Ihrem Rechenzentrum anzeigen. Die APIs bieten außerdem eine Übersicht über die Anzahl der in Ihrer Active IQ Unified Manager Umgebung bereitgestellten Speicher-Workloads sowie deren Kapazitäts- und Leistungsstatistiken (IOPS).

Speicher-Workloads anzeigen

Mit der folgenden Methode können Sie alle Speicher-Workloads in allen Clustern Ihres Rechenzentrums anzeigen. Informationen zum Filtern der Antwort basierend auf bestimmten Spalten finden Sie in der API-Referenzdokumentation, die in Ihrer Unified Manager-Instanz verfügbar ist.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/workloads`

Zusammenfassung der Speicherarbeitslasten anzeigen

Mit der folgenden Methode können Sie die genutzte Kapazität, die verfügbare Kapazität, die genutzten IOPS, die verfügbaren IOPS und die Anzahl der von jedem Performance Service Level verwalteten Speicher-Workloads ermitteln. Die angezeigten Speicherarbeitslasten können für jede LUN, NFS-Dateifreigabe oder CIFS-Freigabe gelten. Die API bietet eine Übersicht über Speicher-Workloads, eine Übersicht über die vom Unified Manager bereitgestellten Speicher-Workloads, eine Übersicht über das Rechenzentrum, eine Übersicht über den gesamten, genutzten und verfügbaren Speicherplatz und die IOPS im Rechenzentrum im Hinblick auf die zugewiesenen Performance Service Levels. Die als Antwort auf diese API empfangenen Informationen werden verwendet, um das Dashboard in der Unified Manager-Benutzeroberfläche zu füllen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/workloads-summary`

Verwalten von Zugriffsendpunkten mithilfe von APIs

Sie müssen Zugriffsendpunkte oder logische Schnittstellen (LIFs) erstellen, die für die Bereitstellung von Storage Virtual Machines (SVMs), LUNs und Dateifreigaben erforderlich sind. Sie können die Zugriffsendpunkte für die SVMs, LUNs oder Dateifreigaben in Ihrer Active IQ Unified Manager Umgebung anzeigen, erstellen, ändern und löschen.

Zugriffsendpunkte anzeigen

Sie können eine Liste der Zugriffsendpunkte in Ihrer Unified Manager-Umgebung mithilfe der folgenden Methode anzeigen. Um eine Liste der Zugriffsendpunkte einer bestimmten SVM, LUN oder Dateifreigabe abzufragen, müssen Sie die eindeutige Kennung für die SVM, LUN oder Dateifreigabe eingeben. Sie können auch den eindeutigen Zugriffsendpunktschlüssel eingeben, um die Details des jeweiligen Zugriffsendpunkts abzurufen.

Kategorie	HTTP-Verb	Weg

Speicheranbieter	ERHALTEN	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

Hinzufügen von Zugriffsendpunkten

Sie können benutzerdefinierte Zugriffsendpunkte erstellen und ihnen die erforderlichen Eigenschaften zuweisen. Sie müssen die Details des Zugriffsendpunkts, den Sie erstellen möchten, als Eingabeparameter eingeben. Sie können diese API oder den System Manager oder die ONTAP CLI verwenden, um auf jedem Knoten einen Zugriffsendpunkt zu erstellen. Für die Erstellung von Zugriffsendpunkten werden sowohl IPv4- als auch IPv6-Adressen unterstützt.

Sie müssen Ihre SVM mit einer Mindestanzahl von Zugriffsendpunkten pro Knoten konfigurieren, um die Bereitstellung von LUNs und Dateifreigaben erfolgreich zu gestalten. Sie sollten Ihre SVM mit mindestens zwei Zugriffsendpunkten pro Knoten konfigurieren, von denen einer das CIFS- und/oder NFS-Protokoll und der andere das iSCSI- oder FCP-Protokoll unterstützt.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	POST	`/storage-provider/access-endpoints`

Löschen von Zugriffsendpunkten

Sie können einen bestimmten Zugriffsendpunkt mit der folgenden Methode löschen. Sie müssen den Zugriffsendpunktschlüssel als Eingabeparameter angeben, um einen bestimmten Zugriffsendpunkt zu löschen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	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 Zugriffsendpunktschlüssel angeben, um einen bestimmten Zugriffsendpunkt zu ändern. Sie müssen außerdem die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	PATCH	`/storage-provider/access-endpoints/{key}`

Verwalten der Active Directory-Zuordnung mithilfe von APIs

Mit den hier aufgeführten APIs können Sie Active Directory-Zuordnungen auf der SVM verwalten, die für die Bereitstellung von CIFS-Freigaben auf den SVMs erforderlich sind. Für die Zuordnung der SVMs zu ONTAP müssen Active Directory-Zuordnungen konfiguriert werden.

Anzeigen von Active Directory-Zuordnungen

Sie können die Konfigurationsdetails der Active Directory-Zuordnungen für eine SVM mithilfe der folgenden Methode anzeigen. Um die Active Directory-Zuordnungen auf einer SVM anzuzeigen, müssen Sie den SVM-Schlüssel eingeben. Um die Details einer bestimmten Zuordnung abzufragen, müssen Sie den Zuordnungsschlüssel eingeben.

Kategorie	HTTP-Verb	Weg

Speicheranbieter	ERHALTEN	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

Active Directory-Zuordnung hinzufügen

Sie können Active Directory-Zuordnungen auf einer SVM mithilfe der folgenden Methode erstellen. Sie müssen die Zuordnungsdetails als Eingabeparameter eingeben.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	POST	`/storage-provider/active-directories-mappings`

Verwalten von Dateifreigaben mithilfe von APIs

Sie können die `/storage-provider/file-shares` API zum Anzeigen, Hinzufügen, Ändern und Löschen der CIFS- und NFS-Dateifreigabevolumes in Ihrer Rechenzentrumsumgebung.

Stellen Sie vor der Bereitstellung der Dateifreigabevolumes sicher, dass die SVM mit den unterstützten Protokollen erstellt und bereitgestellt wurde. Wenn Sie während der Bereitstellung Performance Service Levels (PSLs) oder Storage Efficiency Policies (SEPs) zuweisen, sollten die PSLs oder SEPs vor dem Erstellen der Dateifreigaben erstellt werden.

Dateifreigaben anzeigen

Mit der folgenden Methode können Sie die in Ihrer Unified Manager-Umgebung verfügbaren Dateifreigabevolumes anzeigen. Wenn Sie einen ONTAP Cluster als Datenquelle zu Active IQ Unified Manager hinzugefügt haben, werden die Speicher-Workloads für diese Cluster automatisch zu Ihrer Unified Manager-Instanz hinzugefügt. Diese API ruft die Dateifreigaben automatisch ab und wird manuell zu Ihrer Unified Manager-Instanz hinzugefügt. Sie können die Details einer bestimmten Dateifreigabe anzeigen, indem Sie diese API mit dem Dateifreigabeschlüssel ausführen.

Kategorie	HTTP-Verb	Weg

Speicheranbieter	ERHALTEN	`/storage-provider/file-shares`
		
		`/storage-provider/file-shares/{key}`

Dateifreigaben hinzufügen

Mit der folgenden Methode können Sie CIFS- und NFS-Dateifreigaben in Ihrem SVM hinzufügen. Sie müssen die Details der Dateifreigabe, die Sie erstellen möchten, als Eingabeparameter eingeben. Sie können diese API nicht zum Hinzufügen von FlexGroup -Volumes verwenden.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	POST	`/storage-provider/file-shares`

Je nachdem, ob die Parameter der Zugriffskontrollliste (ACL) oder der Exportrichtlinienparameter angegeben sind, werden CIFS-Freigaben oder NFS-Dateifreigaben erstellt. Wenn Sie die Werte für die ACL-Parameter nicht 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 gemounteten Volumes standardmäßig `rw` (Lesen/Schreiben). Geben Sie zum Erstellen von Datensicherungsvolumes (DP) Folgendes an: `dp` als Wert für die `type` Parameter.

Dateifreigaben löschen

Mit der folgenden Methode können Sie eine bestimmte Dateifreigabe löschen. Sie müssen den Dateifreigabeschlüssel als Eingabeparameter eingeben, um eine bestimmte Dateifreigabe zu löschen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	LÖSCHEN	`/storage-provider/file-shares/{key}`

Ändern von Dateifreigaben

Mit der folgenden Methode können Sie eine Dateifreigabe ändern und ihre Eigenschaften aktualisieren.

Sie müssen den Dateifreigabeschlüssel angeben, um eine bestimmte Dateifreigabe zu ändern. Darüber hinaus müssen Sie die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben.

Beachten Sie, dass Sie bei einem einzelnen Aufruf dieser API nur eine Eigenschaft aktualisieren können. Für mehrere Updates müssen Sie diese API genauso oft ausführen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	PATCH	`/storage-provider/file-shares/{key}`

Verwalten von LUNs mithilfe von APIs

Sie können die `/storage-provider/luns` API zum Anzeigen, Hinzufügen, Ändern und Löschen der LUNs in Ihrer Rechenzentrumsumgebung.

Stellen Sie vor der Bereitstellung der LUNs sicher, dass die SVM mit den unterstützten Protokollen erstellt und bereitgestellt wurde. Wenn Sie während der Bereitstellung Performance Service Levels (PSLs) oder Storage Efficiency Policies (SEPs) zuweisen, sollten die PSLs oder SEPs vor der Erstellung der LUN erstellt werden.

LUNs anzeigen

Sie können die folgende Methode verwenden, um die LUNs in Ihrer Unified Manager-Umgebung anzuzeigen. Wenn Sie einen ONTAP Cluster als Datenquelle zu Active IQ Unified Manager hinzugefügt haben, werden die Speicher-Workloads für diese Cluster automatisch zu Ihrer Unified Manager-Instanz hinzugefügt. Diese API ruft alle LUNs ab, die Ihrer Unified Manager-Instanz automatisch und manuell hinzugefügt wurden. Sie können die Details einer bestimmten LUN anzeigen, indem Sie diese API mit dem LUN-Schlüssel ausführen.

Kategorie	HTTP-Verb	Weg

Speicheranbieter	ERHALTEN	`/storage-provider/luns`
		
		`/storage-provider/luns/{key}`

LUNs hinzufügen

Sie können die folgende Methode verwenden, um Ihren SVMs LUNs hinzuzufügen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	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. Mit diesem Tag lässt sich das Volumen einfach suchen. Wenn Sie den Lautstärkeschlüssel in der Anfrage angeben, wird die Markierung übersprungen.

Löschen von LUNs

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 ein Volume in ONTAP erstellt und dann LUNs über Unified Manager auf diesem Volume bereitgestellt haben, wird das Volume beim Löschen aller LUNs mithilfe dieser API auch aus dem ONTAP Cluster gelöscht.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	LÖSCHEN	`/storage-provider/luns/{key}`

LUNs ändern

Mit der folgenden Methode können Sie eine LUN ändern und ihre Eigenschaften aktualisieren. Sie müssen den LUN-Schlüssel angeben, um eine bestimmte LUN zu ändern. Sie müssen außerdem die LUN-Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben. Zum Aktualisieren von LUN-Arrays mithilfe dieser API sollten Sie die Empfehlungen unter „Empfehlungen zur Verwendung der APIs“ lesen.

Sie können bei einem einzelnen Aufruf dieser API nur eine Eigenschaft aktualisieren. Für mehrere Updates müssen Sie diese API genauso oft ausführen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	PATCH	`/storage-provider/luns/{key}`

Verwalten von Leistungsservicelevels mithilfe von APIs

Sie können Performance-Service-Levels anzeigen, erstellen, ändern und löschen, indem Sie die APIs des Speicheranbieters für Ihren Active IQ Unified Manager verwenden.

Leistungsservicelevel anzeigen

Mit der folgenden Methode können Sie die Performance-Service-Levels anzeigen, um sie Speicher-Workloads zuzuweisen. Die API listet alle systemdefinierten und benutzererstellten Performance Service Levels auf und ruft die Attribute aller Performance Service Levels ab. Wenn Sie ein bestimmtes Performance Service Level abfragen möchten, müssen Sie die eindeutige ID des Performance Service Levels eingeben, um dessen Details abzurufen.

Kategorie	HTTP-Verb	Weg

Speicheranbieter	ERHALTEN	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

Performance-Service-Levels hinzufügen

Mit der folgenden Methode können Sie benutzerdefinierte Performance-Service-Levels erstellen und sie Ihren Speicher-Workloads zuweisen, wenn die systemdefinierten Performance-Service-Levels die erforderlichen Service Level Objectives (SLOs) für die Speicher-Workloads nicht erfüllen. Geben Sie die Details für das Performance-Service-Level ein, das Sie erstellen möchten. Stellen Sie bei den IOPS-Eigenschaften sicher, dass Sie einen gültigen Wertebereich eingeben.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	POST	`/storage-provider/performance-service-levels`

Leistungsservicelevel löschen

Mit der folgenden Methode können Sie einen bestimmten Performance-Service-Level löschen. Sie können einen Performance-Service-Level nicht löschen, wenn er einer Arbeitslast zugewiesen ist oder wenn es sich um den einzigen verfügbaren Performance-Service-Level handelt. Sie müssen die eindeutige ID des Performance-Service-Levels als Eingabeparameter angeben, um ein bestimmtes Performance-Service-Level zu löschen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	LÖSCHEN	`/storage-provider/performance-service-levels/{key}`

Leistungsservicelevel ändern

Mit der folgenden Methode können Sie einen Performance-Service-Level ändern und seine Eigenschaften aktualisieren. Sie können einen Performance-Service-Level, der systemdefiniert ist oder einer Arbeitslast zugewiesen ist, nicht ändern. Sie müssen die eindeutige ID angeben, um ein bestimmtes Performance-Service-Level zu ändern. Sie müssen außerdem die IOPS-Eigenschaft, die Sie aktualisieren möchten, zusammen mit einem gültigen Wert eingeben.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	PATCH	`/storage-provider/performance-service-levels/{key}`

Anzeigen aggregierter Funktionen basierend auf Performance Service Levels

Mit der folgenden Methode können Sie die aggregierten Funktionen basierend auf Performance-Service-Levels abfragen. Diese API gibt die Liste der in Ihrem Rechenzentrum verfügbaren Aggregate zurück und gibt die Funktionen in Bezug auf die Leistungsservicelevel an, die in diesen Aggregaten unterstützt werden können. Während Sie Workloads auf einem Volume bereitstellen, können Sie die Fähigkeit eines Aggregats zur Unterstützung eines bestimmten Performance Service Levels anzeigen und Workloads basierend auf dieser Fähigkeit bereitstellen. Sie können das Aggregat nur angeben, wenn Sie eine Arbeitslast mithilfe von APIs bereitstellen. Diese Funktion ist in der Unified Manager-Web-Benutzeroberfläche nicht verfügbar.

Kategorie	HTTP-Verb	Weg

Speicheranbieter	ERHALTEN	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

Verwalten von Speichereffizienzrichtlinien mithilfe von APIs

Sie können Speichereffizienzrichtlinien mithilfe der APIs des Speicheranbieters anzeigen, erstellen, ändern und löschen.

Beachten Sie die folgenden Punkte:

- Es ist nicht zwingend erforderlich, beim Erstellen einer Arbeitslast auf Unified Manager eine Speichereffizienzrichtlinie zuzuweisen.
- Sie können die Zuweisung einer Speichereffizienzrichtlinie zu einer Arbeitslast nicht mehr aufheben, nachdem ihr eine Richtlinie zugewiesen wurde.
- Wenn für eine Arbeitslast einige Speichereinstellungen auf ONTAP Volumes angegeben sind, z. B. Deduplizierung und Komprimierung, können diese Einstellungen durch die in der Speichereffizienzrichtlinie angegebenen Einstellungen überschrieben werden, die Sie anwenden, wenn Sie die Speicherarbeitslasten zu Unified Manager hinzufügen.

Richtlinien zur Speichereffizienz anzeigen

Mit der folgenden Methode können Sie die Speichereffizienzrichtlinien anzeigen, bevor Sie sie Speicher-Workloads zuweisen. Diese API listet alle systemdefinierten und benutzererstellten Speichereffizienzrichtlinien auf und ruft die Attribute aller Speichereffizienzrichtlinien ab. Wenn Sie eine bestimmte Speichereffizienzrichtlinie abfragen möchten, müssen Sie die eindeutige ID der Richtlinie eingeben, um ihre Details abzurufen.

Kategorie	HTTP-Verb	Weg

Speicheranbieter	ERHALTEN	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

Hinzufügen von Richtlinien zur Speichereffizienz

Mit der folgenden Methode können Sie benutzerdefinierte Speichereffizienzrichtlinien erstellen und diese Ihren Speicher-Workloads zuweisen, wenn die systemdefinierten Richtlinien die Bereitstellungsanforderungen für Ihre Speicher-Workloads nicht erfüllen. Geben Sie die Details der Speichereffizienzrichtlinie, die Sie erstellen möchten, als Eingabeparameter ein.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	POST	`/storage-provider/storage-efficiency-policies`

Richtlinien zur Speichereffizienz löschen

Sie können die folgende Methode verwenden, um eine bestimmte Speichereffizienzrichtlinie zu löschen. Sie können eine Speichereffizienzrichtlinie nicht löschen, wenn sie einer Arbeitslast zugewiesen ist oder wenn es sich um die einzige verfügbare Speichereffizienzrichtlinie handelt. Sie müssen die eindeutige ID der Speichereffizienzrichtlinie als Eingabeparameter angeben, um eine bestimmte Speichereffizienzrichtlinie zu löschen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	LÖSCHEN	`/storage-provider/storage-efficiency-policies/{key}`

Ändern Sie die Richtlinien zur Speichereffizienz

Mit der folgenden Methode können Sie eine Speichereffizienzrichtlinie ändern und ihre Eigenschaften aktualisieren. Sie können keine Speichereffizienzrichtlinie ändern, die systemdefiniert ist oder einer Arbeitslast zugewiesen ist. Sie müssen die eindeutige ID der Speichereffizienzrichtlinie angeben, um eine bestimmte Speichereffizienzrichtlinie zu ändern. Darüber hinaus müssen Sie die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert angeben.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	PATCH	`/storage-provider/storage-efficiency-policies/{key}`

Gängige API-Workflows für die Speicherverwaltung

Die allgemeinen Arbeitsabläufe bieten Entwicklern von Clientanwendungen Beispiele dafür, wie Active IQ Unified Manager -APIs von einer Clientanwendung aufgerufen werden können, um allgemeine Speicherverwaltungsfunktionen auszuführen. Dieser Abschnitt enthält einige dieser Beispiel-Workflows.

Die Arbeitsabläufe beschreiben einige der häufig verwendeten Anwendungsfälle der Speicherverwaltung zusammen mit Beispielcodes, die Sie verwenden können. Jede der Aufgaben wird mithilfe eines Workflow-Prozesses beschrieben, der aus einem oder mehreren API-Aufrufen besteht.

Verstehen Sie die in den Workflows verwendeten API-Aufrufe

Sie können die Online-Dokumentationsseite Ihrer Unified Manager-Instanz anzeigen, die die Details jedes REST-API-Aufrufs enthält. Dieses Dokument wiederholt nicht die Details der Online-Dokumentation. Jeder in den Workflow-Beispielen in diesem Dokument verwendete 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 des Aufrufs überprüfen, einschließlich der Eingabeparameter, Ausgabeformate, HTTP-Statuscodes und des Anfrageverarbeitungstyps.

Die folgenden Informationen sind für jeden API-Aufruf innerhalb eines Workflows enthalten, um das Auffinden des Aufrufs auf der Dokumentationsseite zu erleichtern:

- Kategorie: Die API-Aufrufe sind auf der Dokumentationsseite in funktional verwandte Bereiche oder Kategorien unterteilt. Um einen bestimmten API-Aufruf zu finden, scrollen Sie zum Ende der Seite und klicken Sie auf die entsprechende API-Kategorie.
- HTTP-Verb (Aufruf): Das HTTP-Verb identifiziert die an einer Ressource ausgeführte Aktion. Jeder API-Aufruf wird über ein einzelnes HTTP-Verb ausgeführt.
- Pfad: Der Pfad bestimmt die spezifische Ressource, auf die die Aktion im Rahmen der Ausführung eines Aufrufs angewendet wird. Die Pfadzeichenfolge wird an die Kern-URL angehängt, um die vollständige URL zur Identifizierung der Ressource zu bilden.

Ermitteln von Platzproblemen in Aggregaten mithilfe von APIs

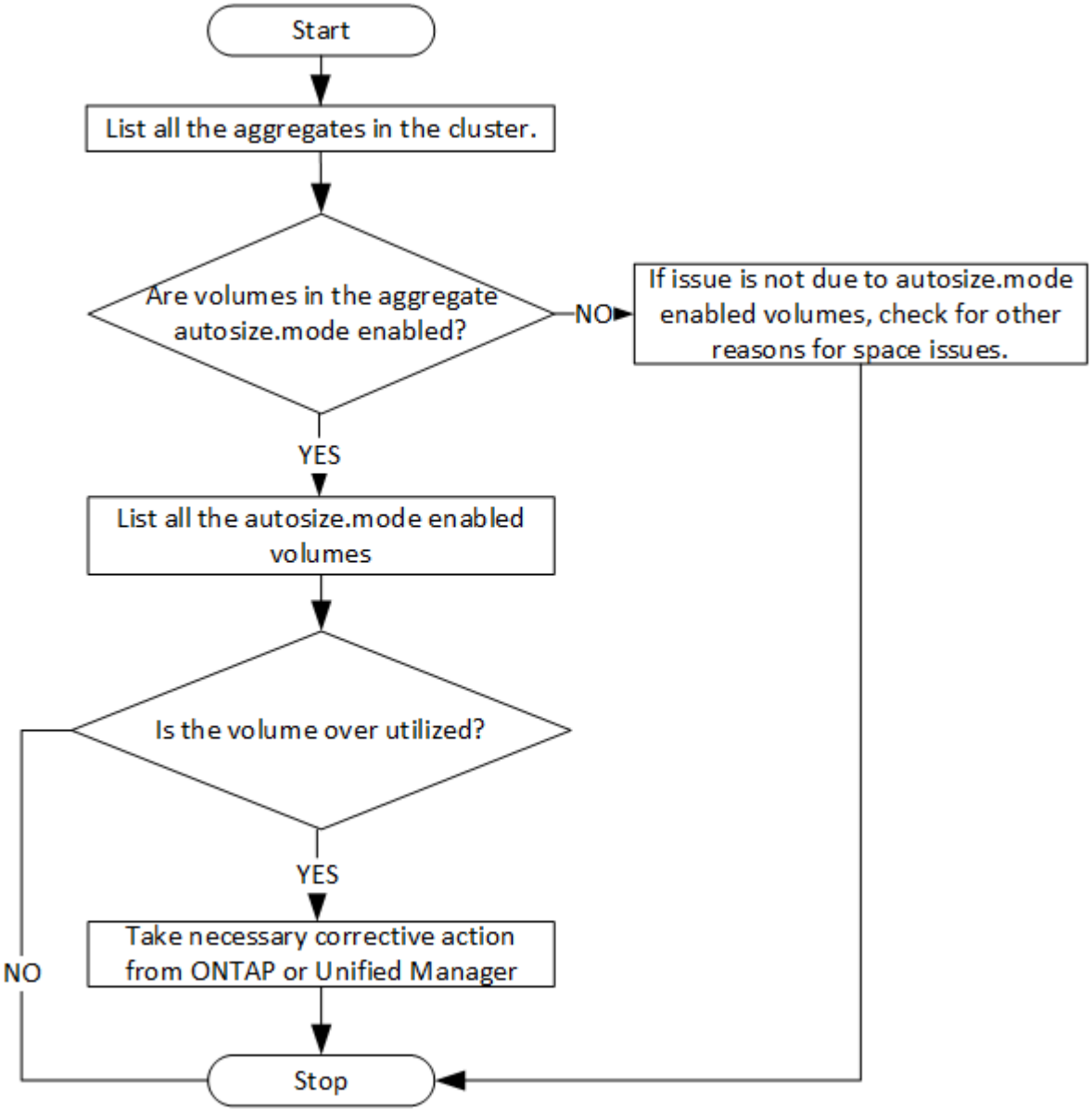
Sie können die Rechenzentrums-APIs in Active IQ Unified Manager verwenden, um die Verfügbarkeit und Nutzung des Speicherplatzes in Ihren Volumes zu überwachen. Sie können Speicherplatzprobleme in Ihrem Volume ermitteln und Speicherressourcen identifizieren, die über- oder unterausgelastet sind.

Die Rechenzentrums-APIs für Aggregate rufen die relevanten Informationen zu verfügbarem und genutztem Speicherplatz sowie zu Einstellungen zur platzsparenden Effizienz ab. Sie können die abgerufenen Informationen auch anhand bestimmter Attribute filtern.

Eine Methode, um einen Platzmangel in Ihren Aggregaten festzustellen, besteht darin, zu überprüfen, ob in Ihrer Umgebung Volumes mit aktiviertem Autosize-Modus vorhanden sind. Anschließend sollten Sie ermitteln,

welche Datenträger übermäßig genutzt werden, und entsprechende Korrekturmaßnahmen ergreifen.

Das folgende Flussdiagramm veranschaulicht den Prozess zum Abrufen von Informationen zu Volumes mit aktiviertem Autosize-Modus:



Dieser Ablauf setzt voraus, dass die Cluster bereits in ONTAP erstellt und zu Unified Manager hinzugefügt wurden.

1. Besorgen Sie sich den Clusterschlüssel, sofern Sie den Wert nicht kennen:

Kategorie	HTTP-Verb	Weg
Rechenzentrum	ERHALTEN	`/datacenter/cluster/clusters`

2. Verwenden Sie den Clusterschlüssel als Filterparameter und fragen Sie die Aggregate in diesem Cluster ab.

Kategorie	HTTP-Verb	Weg
Rechenzentrum	ERHALTEN	`/datacenter/storage/aggregates`

3. Analysieren Sie anhand der Antwort die Speicherplatznutzung der Aggregate und ermitteln Sie, bei welchen Aggregaten Speicherplatzprobleme vorliegen. Rufen Sie für jedes Aggregat mit Speicherplatzproblem den Aggregatschlüssel aus derselben JSON-Ausgabe ab.
4. Filtern Sie mit jedem Aggregatschlüssel alle Volumes, die den Wert für den Parameter autosize.mode als `grow`.

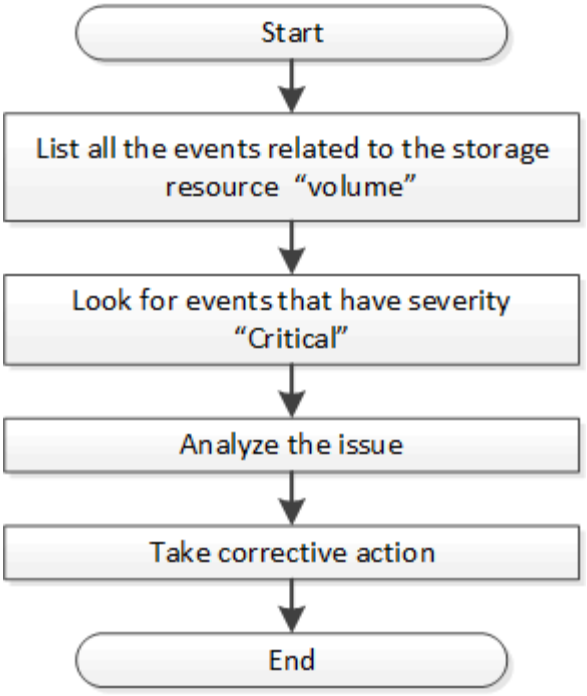
Kategorie	HTTP-Verb	Weg
Rechenzentrum	ERHALTEN	`/datacenter/storage/volumes`

5. Analysieren Sie, welche Volumes übermäßig genutzt werden.
6. Führen Sie alle erforderlichen Korrekturmaßnahmen durch, z. B. das Verschieben des Volumes über Aggregate hinweg, um die Platzprobleme in Ihrem Volume zu beheben. Sie können diese Aktionen über die ONTAP oder Unified Manager-Web-Benutzeroberfläche ausführen.

Ermitteln Sie Probleme in Speicherobjekten mithilfe von Ereignis-APIs

Wenn ein Speicherobjekt in Ihrem Rechenzentrum einen Schwellenwert überschreitet, erhalten Sie eine Benachrichtigung über dieses Ereignis. Mithilfe dieser Benachrichtigung können Sie das Problem analysieren und Korrekturmaßnahmen ergreifen, indem Sie die `events` APIs.

Dieser Workflow verwendet als Beispiel ein Volume als Ressourcenobjekt. Sie können die `events` APIs zum Abrufen der Liste der Ereignisse im Zusammenhang mit einem Volume, Analysieren der kritischen Probleme für dieses Volume und Ergreifen von Korrekturmaßnahmen zur Behebung des Problems.



Befolgen Sie diese Schritte, um die Probleme in Ihrem Volume zu ermitteln, bevor Sie Abhilfemaßnahmen ergreifen.

Schritte

1. Analysieren Sie die kritischen Active IQ Unified Manager Ereignisbenachrichtigungen für die Volumes in Ihrem Rechenzentrum.
2. Fragen Sie alle Ereignisse für die Volumes ab, indem Sie die folgenden Parameter in der API „/management-server/events“ verwenden:
   `"resource_type": "volume"`
   `"severity": "critical"`

Kategorie	HTTP-Verb	Weg
Management-Server	ERHALTEN	/Management-Server/Ereignisse

3. Sehen Sie sich die Ausgabe an und analysieren Sie die Probleme in den jeweiligen Bänden.
4. Führen Sie die erforderlichen Aktionen mithilfe der Unified Manager-REST-APIs oder der Web-Benutzeroberfläche durch, um die Probleme zu beheben.

Fehlerbehebung bei ONTAP -Volumes mithilfe von Gateway-APIs

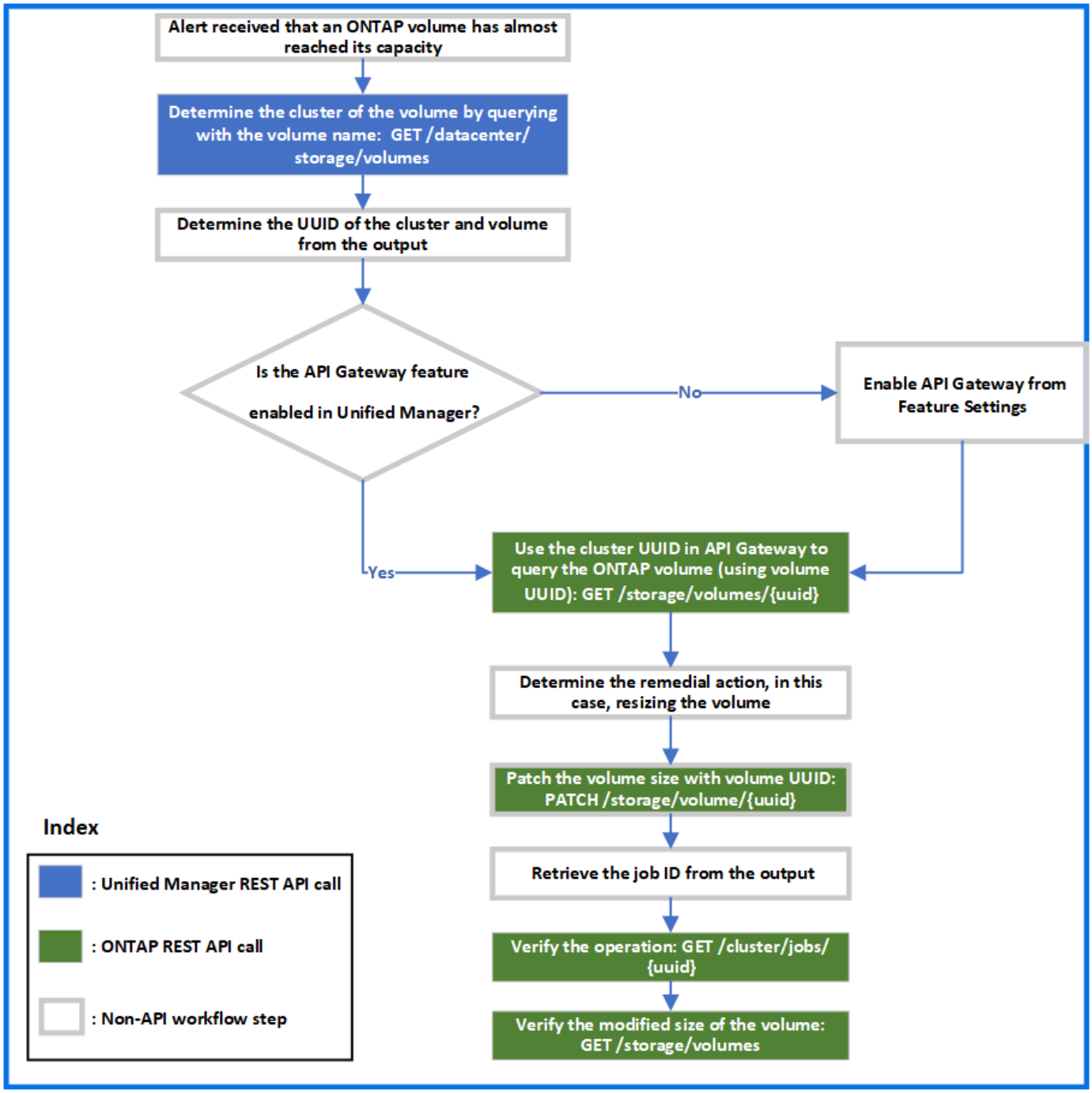
Die Gateway-APIs fungieren als Gateway zum Aufrufen von ONTAP -APIs, um Informationen zu Ihren ONTAP Speicherobjekten abzufragen und Abhilfemaßnahmen zur Behebung der gemeldeten Probleme zu ergreifen.

Dieser Workflow greift einen Beispielanwendungsfall auf, bei dem ein Ereignis ausgelöst wird, wenn ein ONTAP Volume fast seine Kapazität erreicht. Der Workflow zeigt auch, wie dieses Problem durch Aufrufen einer Kombination aus Active IQ Unified Manager und ONTAP REST-APIs behoben werden kann.

Stellen Sie vor dem Ausführen der Workflow-Schritte Folgendes sicher:

- Sie kennen die Gateway-APIs und wissen, wie sie verwendet werden. Weitere Informationen 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 finden Sie unterhttps://docs.netapp.com/us-en/ontap-automation/index.html["ONTAP Automation-Dokumentation"] .
- Sie sind Anwendungsadministrator.
- Der Cluster, auf dem Sie die REST-API-Operationen ausführen möchten, wird von ONTAP 9.5 oder höher unterstützt und der Cluster wird über HTTPS zu Unified Manager hinzugefügt.

Das folgende Diagramm veranschaulicht jeden Schritt im Workflow zur Fehlerbehebung bei der Kapazitätsnutzung des ONTAP Volumes.



Der Workflow deckt die Aufrufpunkte der Unified Manager- und ONTAP REST-APIs ab.

1. Notieren Sie den Datenträgernamen aus dem Ereignis, das die Datenträgerkapazitätsauslastung meldet.
2. Verwenden Sie den Volumenamen als Wert im Namensparameter und fragen Sie das Volume ab, indem Sie die folgende Unified Manager-API ausführen.

Kategorie	HTTP-Verb	Weg
Rechenzentrum	ERHALTEN	`/datacenter/storage/volumes`

3. Rufen Sie die Cluster-UUID und die Volume-UUID aus der Ausgabe ab.

4. Navigieren Sie in der Unified Manager-Web-Benutzeroberfläche zu **Allgemein** > **Funktionseinstellungen** > **API-Gateway**, um zu überprüfen, ob die API-Gateway-Funktion aktiviert ist. Sofern es nicht aktiviert ist, können Sie die APIs in der Gateway-Kategorie nicht aufrufen. Aktivieren Sie die Funktion, wenn sie deaktiviert ist.
5. Verwenden Sie die Cluster-UUID, um die ONTAP -API auszuführen/`storage/volumes/{uuid}` über das API-Gateway. Die Abfrage gibt die Volumedetails zurück, wenn die Volume-UUID als API-Parameter übergeben wird.

   Zum Ausführen der ONTAP -APIs über das API-Gateway werden die Unified Manager-Anmeldeinformationen intern zur Authentifizierung übergeben, und Sie müssen keinen zusätzlichen Authentifizierungsschritt für den Zugriff auf einzelne Cluster ausführen.

Kategorie	HTTP-Verb	Weg
Einheitlicher Manager: Gateway ONTAP: Speicher	ERHALTEN	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 des GET-Vorgangs lautet die generierte URL: `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. Bestimmen Sie anhand der Ausgabe die Größe, Verwendung und zu ergreifenden Abhilfemaßnahmen. In diesem Arbeitsablauf besteht die Abhilfemaßnahme darin, die Größe des Volumes zu ändern.
7. Verwenden Sie die Cluster-UUID und führen Sie die folgende ONTAP -API über das API-Gateway aus, um die Größe des Volumes zu ändern. Informationen zu den Eingabeparametern für die Gateway- und ONTAP -APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Weg

Einheitlicher Manager: Gateway
 	
ONTAP: Speicher
	PATCH	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP -API:
		`/storage/volumes/{uuid}`

Zusammen mit der Cluster-UUID und der Volume-UUID müssen Sie einen Wert für den Größenparameter eingeben, um die Größe des Volumes zu ändern. Stellen Sie sicher, dass Sie den Wert *in Bytes* eingeben. Wenn Sie beispielsweise die Größe eines Volumes von 100 GB auf 120 GB erhöhen möchten, geben Sie am Ende der Abfrage den Wert für den Parameter size ein: `-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. Überprüfen Sie mithilfe der Job-UUID, ob der Job erfolgreich ausgeführt wurde. Verwenden Sie die Cluster-UUID und die Job-UUID, um die folgende ONTAP -API über das API-Gateway auszuführen. Informationen zu den Eingabeparametern für die Gateway- und ONTAP -APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Weg

Einheitlicher Manager: Gateway
 	
ONTAP: Cluster
	ERHALTEN	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP -API:
		`/cluster/jobs/{uuid}`

Die zurückgegebenen HTTP-Codes sind dieselben wie die HTTP-Statuscodes der ONTAP REST API.

9. Führen Sie die folgende ONTAP API aus, um die Details des Volumes mit geänderter Größe abzufragen. Informationen zu den Eingabeparametern für die Gateway- und ONTAP -APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Weg

Einheitlicher Manager: Gateway
 	
ONTAP: Speicher
	ERHALTEN	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP -API:
		`/storage/volumes/{uuid}`

Die Ausgabe zeigt eine erhöhte Volumegröße von 120 GB.

API-Workflows für das Workload-Management

Mit Active IQ Unified Manager können Sie Speicher-Workloads (LUNs, NFS-Dateifreigaben und CIFS-Freigaben) bereitstellen und ändern. Die Bereitstellung umfasst mehrere Schritte, von der Erstellung der Storage Virtual Machine (SVM) bis zur Anwendung von Performance Service Level- und Storage Efficiency Policies auf die Speicher-Workloads. Das Ändern von Workloads umfasst die Schritte zum Ändern bestimmter Parameter und zum Aktivieren zusätzlicher Funktionen.

Folgende Arbeitsabläufe werden beschrieben:

- Workflow für die Bereitstellung von Storage Virtual Machines (SVMs) auf Unified Manager.

  Dieser Workflow muss vor der Bereitstellung von LUNs oder Dateifreigaben auf Unified Manager durchgeführt werden.

- Bereitstellung von Dateifreigaben.
- Bereitstellung von LUNs.
- Ändern von LUNs und Dateifreigaben (anhand des Beispiels zum Aktualisieren des Performance Service Level-Parameters für die Speicher-Workloads).
- Ändern einer NFS-Dateifreigabe zur Unterstützung des CIFS-Protokolls
- Ändern von Workloads zum Upgrade von QoS auf AQoS

Stellen Sie für jeden Bereitstellungsworkflow (LUN und Dateifreigaben) sicher, dass Sie den Workflow zum Überprüfen der SVMs auf den Clustern abgeschlossen haben.

Sie müssen auch die Empfehlungen und Einschränkungen lesen, bevor Sie die einzelnen APIs in den Workflows verwenden. Die relevanten Details der APIs finden Sie in den einzelnen Abschnitten, die in den zugehörigen Konzepten und Referenzen aufgeführt sind.

Überprüfen von SVMs auf Clustern mithilfe von APIs

Bevor Sie Dateifreigaben oder LUNs bereitstellen, müssen Sie überprüfen, ob auf den Clustern Storage Virtual Machines (SVMs) erstellt wurden.

Der Workflow geht davon aus, dass ONTAP Cluster zu Unified Manager hinzugefügt wurden und der Clusterschlüssel abgerufen wurde. Cluster sollten über die erforderlichen Lizenzen für die Bereitstellung von LUNs und Dateifreigaben verfügen.

1. Überprüfen Sie, ob für den Cluster eine SVM erstellt wurde.

Kategorie	HTTP-Verb	Weg
Rechenzentrum	ERHALTEN	`/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, erstellen Sie die SVM. Zum Erstellen der SVMs benötigen Sie den Clusterschlüssel, auf dem Sie die SVM provisionieren. Sie müssen auch den SVM-Namen angeben. Befolgen Sie diese Schritte.

Kategorie	HTTP-Verb	Weg
Rechenzentrum	ERHALTEN	`/datacenter/cluster/clusters` `/datacenter/cluster/clusters/{key}`

Holen Sie sich den Clusterschlüssel.

Beispiel-cURL

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

3. Rufen Sie aus der Ausgabe den Clusterschlüssel ab und verwenden Sie ihn dann als Eingabe zum Erstellen der SVM.

> Achten Sie beim Erstellen der SVM darauf, dass sie alle Protokolle unterstützt, die für die Bereitstellung von LUNs und Dateifreigaben darauf erforderlich sind, beispielsweise CIFS, NFS, FCP und iSCSI. Die Bereitstellungs-Workflows können fehlschlagen, wenn die SVM die erforderlichen Dienste nicht unterstützt. Es wird empfohlen, die Dienste für die jeweiligen Arten von Workloads auch auf der SVM zu aktivieren.

Kategorie	HTTP-Verb	Weg
Rechenzentrum	POST	`/datacenter/svm/svms`

Beispiel-cURL

Geben Sie die SVM-Objektdetails als Eingabeparameter ein.

```
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. Überprüfen Sie die SVM-Erstellung, indem Sie den Jobobjektschlüssel für die Abfrage verwenden. Wenn die SVM erfolgreich erstellt wurde, wird der SVM-Schlüssel in der Antwort zurückgegeben.

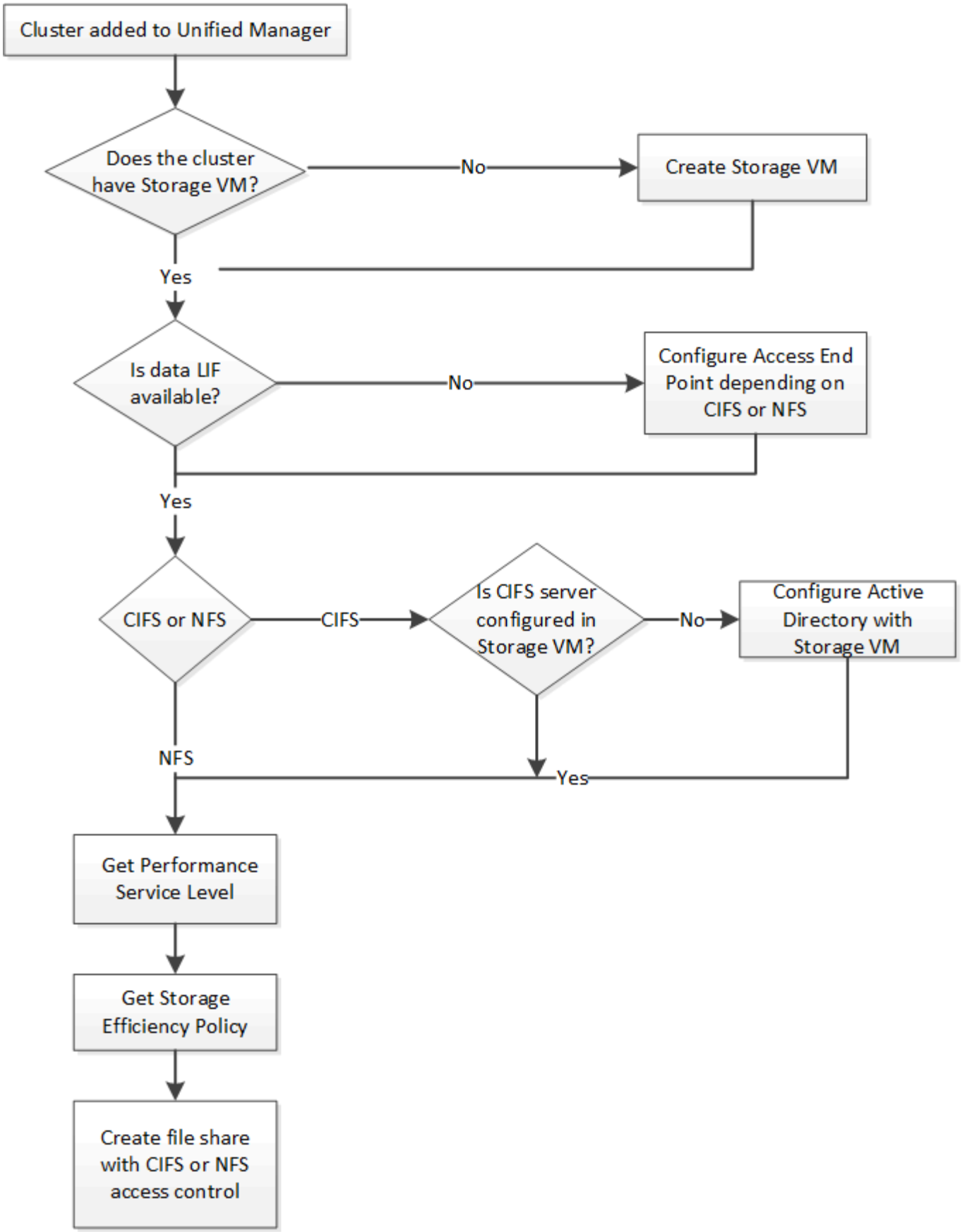
Kategorie	HTTP-Verb	Weg
Management-Server	ERHALTEN	`/management-server/jobs/{key}`

Bereitstellen von CIFS- und NFS-Dateifreigaben mithilfe von APIs

Sie können CIFS-Freigaben und NFS-Dateifreigaben auf Ihren Storage Virtual Machines

(SVMs) bereitstellen, indem Sie die Bereitstellungs-APIs verwenden, die als Teil von Active IQ Unified Manager bereitgestellt werden. Dieser Bereitstellungs-Workflow beschreibt detailliert die Schritte zum Abrufen der Schlüssel der SVMs, Leistungsservicelevel und Speichereffizienzrichtlinien vor dem Erstellen der Dateifreigaben.

Das folgende Diagramm veranschaulicht jeden Schritt in einem Workflow zur Bereitstellung einer Dateifreigabe. Es umfasst die Bereitstellung sowohl von CIFS-Freigaben als auch von NFS-Dateifreigaben.


Cluster added to Unified Manager
Does the cluster have Storage VM?
No
Create Storage VM
Yes
Is data LIF available?
No
Configure Access End Point depending on CIFS or NFS
Yes
CIFS or NFS
CIFS
Is CIFS server configured in Storage VM?
No
Configure Active Directory with Storage VM
NFS
Yes
Get Performance Service Level
Get Storage Efficiency Policy
Create file share with CIFS or NFS access control

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-Dienste. Die Bereitstellung von Dateifreigaben kann fehlschlagen, wenn die SVMs die erforderlichen Dienste nicht unterstützen.
- Der FCP-Port ist für die Portbereitstellung online.

1. Stellen Sie fest, ob Daten-LIFs oder Zugriffsendpunkte auf der SVM verfügbar sind, auf der Sie die CIFS-Freigabe erstellen möchten. Rufen Sie die Liste der verfügbaren Zugriffsendpunkte auf der SVM ab:

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/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. Wenn Ihr Zugriffsendpunkt in der Liste verfügbar ist, rufen Sie den Zugriffsendpunktschlüssel ab, andernfalls erstellen Sie den Zugriffsendpunkt.

Stellen Sie sicher, dass Sie Zugriffsendpunkte erstellen, auf denen das CIFS-Protokoll aktiviert ist. Die Bereitstellung von CIFS-Freigaben schlägt fehl, es sei denn, Sie haben einen Zugriffsendpunkt mit aktiviertem CIFS-Protokoll erstellt.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	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 Zugriffsendpunkt überprüfen können.

3. Überprüfen Sie den Zugriffsendpunkt:

Kategorie	HTTP-Verb	Weg
Management-Server	ERHALTEN	`/management-server/jobs/{key}`

4. Bestimmen Sie, ob Sie eine CIFS-Freigabe oder eine NFS-Dateifreigabe erstellen müssen. Führen Sie zum Erstellen von CIFS-Freigaben die folgenden Teilschritte aus:

   a. Stellen Sie fest, ob der CIFS-Server auf Ihrer SVM konfiguriert ist, d. h., ob auf der SVM eine Active Directory-Zuordnung erstellt wurde.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/active-directories-mappings`

   b. Wenn die Active Directory-Zuordnung erstellt ist, nehmen Sie den Schlüssel, andernfalls erstellen Sie die Active Directory-Zuordnung auf der SVM.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	POST	`/storage-provider/active-directories-mappings`

Beispiel-cURL

Sie müssen die Details zum Erstellen der Active Directory-Zuordnung als Eingabeparameter eingeben.

```
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 Sie können die Erstellung der Active Directory-Zuordnung in der Ausgabe überprüfen. Im Falle eines Fehlers wird die Fehlermeldung angezeigt, damit Sie das Problem beheben und die Anfrage erneut ausführen können.

5. Besorgen Sie sich den SVM-Schlüssel für die SVM, auf der Sie die CIFS-Freigabe oder die NFS-Dateifreigabe erstellen möchten, wie im Workflow-Thema „SVMs auf Clustern überprüfen“ beschrieben.
6. Rufen Sie den Schlüssel für das Performance-Service-Level ab, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie die `system_defined` Eingabeparameter zu `true` . Rufen Sie aus der Ausgabe den Schlüssel des Performance Service Level ab, den Sie auf die Dateifreigabe anwenden möchten.

7. Optional können Sie den Schlüssel der Speichereffizienzrichtlinie für die Speichereffizienzrichtlinie abrufen, die Sie auf die Dateifreigabe anwenden möchten, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/storage-efficiency-policies`

8. Erstellen Sie die Dateifreigabe. Sie können eine Dateifreigabe erstellen, die sowohl CIFS als auch NFS unterstützt, indem Sie die Zugriffskontrollliste und die Exportrichtlinie angeben. Die folgenden Unterschritte

liefern Informationen, wenn Sie eine Dateifreigabe erstellen möchten, die nur eines der Protokolle auf dem Volume unterstützt. Sie können eine NFS-Dateifreigabe auch aktualisieren, um die Zugriffskontrollliste einzuschließen, nachdem Sie die NFS-Freigabe erstellt haben. Weitere Informationen finden Sie im Thema „Ändern von Speicher-Workloads“.

a. Um nur eine CIFS-Freigabe zu erstellen, sammeln Sie die Informationen zur Zugriffskontrollliste (ACL). Geben Sie zum Erstellen der CIFS-Freigabe gültige Werte für die folgenden Eingabeparameter an. Für jede Benutzergruppe, die Sie zuweisen, wird eine ACL erstellt, wenn eine CIFS/SMB-Freigabe bereitgestellt wird. Basierend auf den Werten, die Sie für ACL und Active Directory-Zuordnung eingeben, werden die Zugriffskontrolle und die Zuordnung für die CIFS-Freigabe beim Erstellen 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. Um nur eine NFS-Dateifreigabe zu erstellen, sammeln Sie die Informationen zur Exportrichtlinie. Geben Sie zum Erstellen der NFS-Dateifreigabe gültige Werte für die folgenden Eingabeparameter an. Basierend auf Ihren Werten wird die Exportrichtlinie beim Erstellen mit der NFS-Dateifreigabe verknüpft.

   Beim Bereitstellen der NFS-Freigabe können Sie entweder eine Exportrichtlinie erstellen, indem Sie alle erforderlichen Werte angeben, oder den Exportrichtlinienschlüssel angeben und eine vorhandene Exportrichtlinie wiederverwenden. Wenn Sie eine Exportrichtlinie für die Speicher-VM wiederverwenden möchten, müssen Sie den Exportrichtlinienschlüssel hinzufügen. Sofern Sie den Schlüssel nicht kennen, können Sie den Exportrichtlinienschlüssel mithilfe des `/datacenter/protocols/nfs/export-policies` API. Zum Erstellen einer neuen Richtlinie müssen Sie die Regeln wie im folgenden Beispiel angezeigt eingeben. Für die eingegebenen Regeln versucht die API, durch Abgleichen von Host, Speicher-VM und Regeln nach einer vorhandenen Exportrichtlinie zu suchen. Wenn eine Exportrichtlinie vorhanden ist, wird diese 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"
            }
```

Geben Sie nach der Konfiguration der Zugriffskontrollliste und der Exportrichtlinie die gültigen Werte für die obligatorischen Eingabeparameter für CIFS- und NFS-Dateifreigaben an:

Die Speichereffizienzrichtlinie ist ein optionaler Parameter zum Erstellen von Dateifreigaben.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	POST	`/storage-provider/file-shares`

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie die von Ihnen erstellte Dateifreigabe überprüfen können. . Überprüfen Sie die Erstellung der Dateifreigabe mithilfe des Job-Objektschlüssels, der bei der Abfrage des Jobs zurückgegeben wurde:

Kategorie	HTTP-Verb	Weg
Management-Server	ERHALTEN	`/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. Überprüfen Sie die Erstellung der Dateifreigabe, indem Sie die folgende API mit dem zurückgegebenen Schlüssel ausführen:

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/file-shares/{key}`

Beispiel für JSON-Ausgabe

Sie können sehen, dass die POST-Methode von `/storage-provider/file-shares` ruft intern alle für die einzelnen Funktionen erforderlichen APIs auf und erstellt das Objekt. Beispielsweise ruft es die `/storage-provider/performance-service-levels/` API zum Zuweisen des Performance-Servicelevels auf der Dateifreigabe.

```
{
    "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",
```

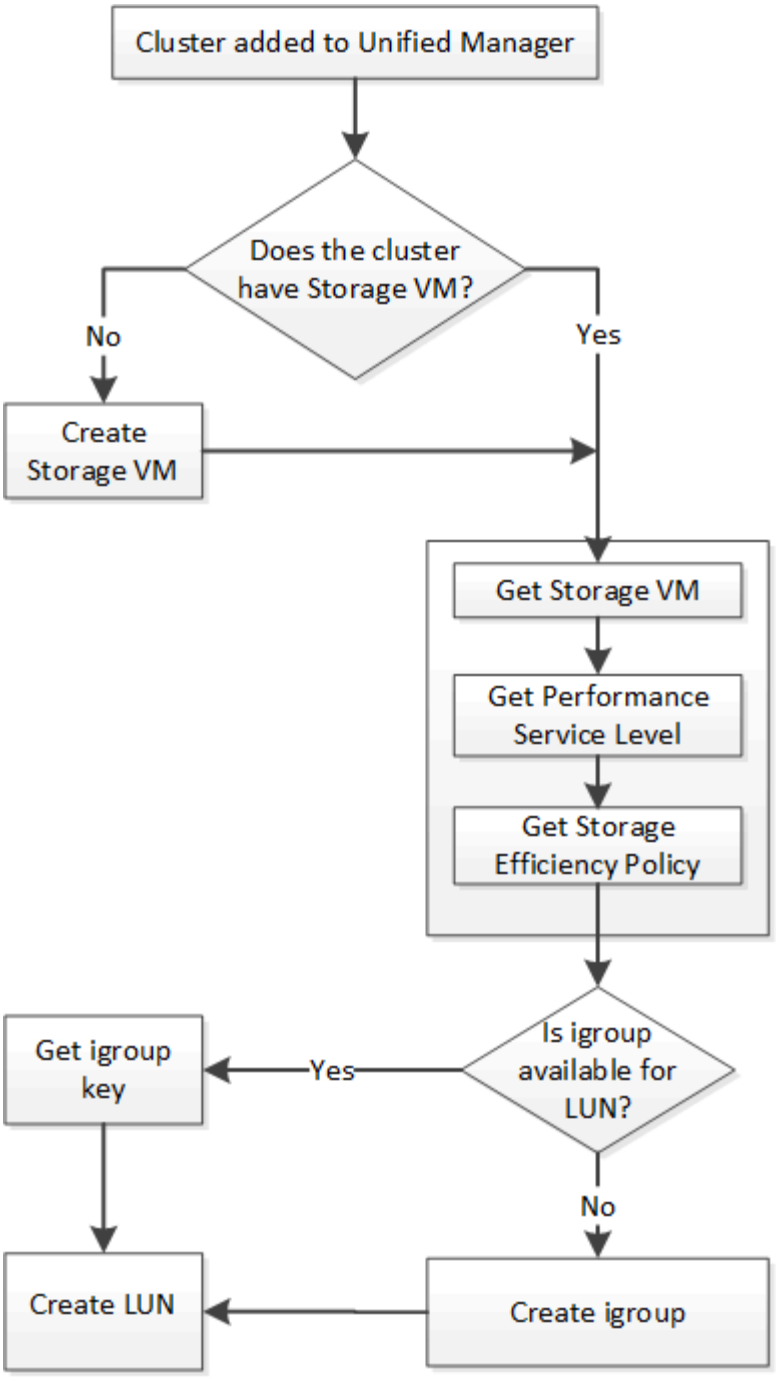
```
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "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"
        }
    }
}
```


Bereitstellen von LUNs mithilfe von APIs

Sie können LUNs auf Ihren Storage Virtual Machines (SVMs) bereitstellen, indem Sie die Bereitstellungs-APIs verwenden, die als Teil von Active IQ Unified Manager bereitgestellt werden. Dieser Bereitstellungs-Workflow beschreibt detailliert die Schritte zum Abrufen der Schlüssel der SVMs, Leistungsservicelevel und Speichereffizienzrichtlinien vor dem Erstellen der LUN.

Das folgende Diagramm veranschaulicht die Schritte in einem LUN-Bereitstellungsworkflow.



Dieser Workflow setzt voraus, dass die ONTAP Cluster zu Unified Manager hinzugefügt wurden und der Clusterschlüssel abgerufen wurde. Der Workflow geht außerdem davon aus, dass die SVMs bereits auf den Clustern erstellt wurden.

1. Besorgen Sie sich den SVM-Schlüssel für die SVM, auf der Sie die LUN erstellen möchten, wie im Workflow-Thema „SVMs auf Clustern überprüfen“ beschrieben.
2. Rufen Sie den Schlüssel für das Performance-Service-Level ab, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie die `system_defined` Eingabeparameter zu `true` . Ermitteln Sie aus der Ausgabe den Schlüssel des Performance Service Levels, den Sie auf die LUN anwenden möchten.

3. Optional können Sie den Schlüssel der Speichereffizienzrichtlinie für die Speichereffizienzrichtlinie abrufen, die Sie auf die LUN anwenden möchten, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/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	Weg
Rechenzentrum	ERHALTEN	`/datacenter/protocols/san/igroups` `/datacenter/protocols/san/igroups/{key}`

Sie müssen den Parameterwert eingeben, um die SVM anzugeben, für die die igroup autorisierten Zugriff hat. Wenn Sie außerdem eine bestimmte Igroup abfragen möchten, geben Sie den Igroup-Namen (Schlüssel) als Eingabeparameter ein.

5. Wenn Sie in der Ausgabe die Igroup finden, der Sie Zugriff gewähren möchten, rufen Sie den Schlüssel ab. Andernfalls erstellen Sie die Igroup.

Kategorie	HTTP-Verb	Weg
Rechenzentrum	POST	`/datacenter/protocols/san/igroups`

Sie müssen die Details der Igroup, die Sie erstellen möchten, als Eingabeparameter eingeben. Dies ist ein synchroner Aufruf und Sie können die Igroup-Erstellung in der Ausgabe überprüfen. Im Falle eines Fehlers wird eine Meldung angezeigt, in der Sie zur Fehlerbehebung und erneuten Ausführung der API aufgefordert werden.

6. Erstellen Sie die LUN.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	POST	`/storage-provider/luns`

Stellen Sie zum Erstellen der LUN sicher, dass Sie die abgerufenen Werte als obligatorische Eingabeparameter hinzugefügt haben.

Die Speichereffizienzrichtlinie ist ein optionaler Parameter zum Erstellen von LUNs.

Beispiel-cURL

Sie müssen alle Details der LUN, die Sie erstellen möchten, als Eingabeparameter eingeben.

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie die von Ihnen erstellte LUN überprüfen können.

7. Überprüfen Sie die LUN-Erstellung mithilfe des Job-Objektschlüssels, der bei der Job-Abfrage zurückgegeben wurde:

Kategorie	HTTP-Verb	Weg
Management-Server	ERHALTEN	`/management-server/jobs/{key}`

Am Ende der Antwort sehen Sie den Schlüssel der erstellten LUN.

8. Überprüfen Sie die Erstellung der LUN, indem Sie die folgende API mit dem zurückgegebenen Schlüssel ausführen:

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/luns/{key}`

Beispiel für JSON-Ausgabe

Sie können sehen, dass die POST-Methode von `/storage-provider/luns` ruft intern alle für die einzelnen Funktionen erforderlichen APIs auf und erstellt das Objekt. Beispielsweise ruft es die `/storage-provider/performance-service-levels/` API zum Zuweisen des Performance Service Levels auf der LUN.

== Schritte zur Fehlerbehebung bei Fehlern bei der LUN-Erstellung oder -Zuordnung

Nach Abschluss dieses Arbeitsablaufs kann es immer noch zu einem Fehler bei der LUN-Erstellung kommen. Auch wenn die LUN erfolgreich erstellt wurde, kann die LUN-Zuordnung mit der igroup fehlschlagen, weil auf dem Knoten, auf dem Sie die LUN erstellen, kein SAN-LIF oder Zugriffsendpunkt verfügbar ist. Im Falle eines Fehlers 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.
```

Befolgen Sie diese Schritte zur Fehlerbehebung, um diesen Fehler zu umgehen.

1. Erstellen Sie einen Zugriffsendpunkt, der das ISCSI/FCP-Protokoll unterstützt, auf der SVM, auf der Sie versucht haben, die LUN zu erstellen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	POST	`/storage-provider/access-endpoints`

Beispiel-cURL

Sie müssen die Details des Zugriffsendpunkts, den Sie erstellen möchten, als Eingabeparameter eingeben.

> Stellen Sie sicher, dass Sie im Eingabeparameter die Adresse hinzugefügt haben, um den Home-Knoten der LUN anzugeben, und die ha_address, um den Partnerknoten des Home-Knotens anzugeben. Wenn Sie diesen Vorgang ausführen, werden Zugriffsendpunkte sowohl auf dem Home-Knoten als auch auf dem Partnerknoten erstellt.

2. Fragen Sie den Job mit dem in der JSON-Ausgabe zurückgegebenen Job-Objektschlüssel ab, um zu überprüfen, ob er erfolgreich ausgeführt wurde, um die Zugriffsendpunkte auf der SVM hinzuzufügen, und ob die iSCSI/FCP-Dienste auf der SVM aktiviert wurden.

Kategorie	HTTP-Verb	Weg
Management-Server	ERHALTEN	`/management-server/jobs/{key}`

Beispiel für JSON-Ausgabe

Am Ende der Ausgabe sehen Sie den Schlüssel der erstellten Zugriffsendpunkte. In der folgenden Ausgabe gibt der Wert „name“: „accessEndpointKey“ den auf dem Home-Knoten der LUN erstellten Zugriffsendpunkt an, für den der Schlüssel 9c964258-14ef-11ea-95e2-00a098e32c28 lautet. Der Wert „name“: „accessEndpointHAKey“ gibt den Zugriffsendpunkt an, der auf dem Partnerknoten des Home-Knotens erstellt wurde, für den der Schlüssel 9d347006-14ef-11ea-8760-00a098e3215f lautet.

3. Ändern Sie die LUN, um die Igroup-Zuordnung zu aktualisieren. Weitere Informationen zur Änderung des Arbeitsablaufs finden Sie unter „Ändern von Speicher-Workloads“.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	PATCH	`/storage-provider/lun/{key}`

Geben Sie in der Eingabe den Igroup-Schlüssel an, mit dem Sie die LUN-Zuordnung aktualisieren

möchten, zusammen mit dem LUN-Schlüssel.

Beispiel-cURL

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie überprüfen können, ob die Zuordnung erfolgreich war.

4. Überprüfen Sie die LUN-Zuordnung, indem Sie eine Abfrage mit dem LUN-Schlüssel durchführen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/luns/{key}`

Beispiel für JSON-Ausgabe

In der Ausgabe können Sie sehen, dass die LUN erfolgreich der Igroup (Schlüssel d19ec2fa-fec7-11e8-b23d-00a098e32c28) zugeordnet wurde, mit der sie ursprünglich bereitgestellt wurde.

Ändern von Speicherworkloads mithilfe von APIs

Das Ändern von Speicher-Workloads besteht aus der Aktualisierung von LUNs oder Dateifreigaben mit fehlenden Parametern oder der Änderung der vorhandenen Parameter.

Dieser Workflow verwendet das Beispiel der Aktualisierung von Performance Service Levels für LUNs und Dateifreigaben.

Der Workflow geht davon aus, dass die LUN oder Dateifreigabe mit Performance Service Levels bereitgestellt wurde.

Ändern von Dateifreigaben

Beim Ändern einer Dateifreigabe können Sie die folgenden Parameter aktualisieren:

- Kapazität oder Größe.
- Online- oder Offline-Einstellung.
- Richtlinie zur Speichereffizienz.
- Leistungsservicelevel.
- Einstellungen der Zugriffskontrollliste (ACL).
- Richtlinieneinstellungen exportieren. Sie können auch Exportrichtlinienparameter löschen und die standardmäßigen (leeren) Exportrichtlinienregeln für die Dateifreigabe wiederherstellen.

Während eines einzelnen API-Laufs können Sie nur einen Parameter aktualisieren.

Dieses Verfahren beschreibt das Hinzufügen eines Performance-Servicelevels zu einer Dateifreigabe. Sie können dasselbe Verfahren zum Aktualisieren aller anderen Dateifreigabeeigenschaften verwenden.

1. Besorgen Sie sich den CIFS-Freigabe- oder NFS-Dateifreigabeschlüssel der Dateifreigabe, die Sie aktualisieren möchten. Diese API fragt alle Dateifreigaben in Ihrem Rechenzentrum ab. Überspringen Sie

diesen Schritt, wenn Sie den Dateifreigabeschlüssel bereits kennen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/file-shares`

2. Zeigen Sie die Details der Dateifreigabe an, indem Sie die folgende API mit dem erhaltenen Dateifreigabeschlüssel ausführen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/file-shares/{key}`

Sehen Sie sich die Details der Dateifreigabe in der Ausgabe an.

```
"assigned_performance_service_level": {
        "key": null,
        "name": "Unassigned",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
      },
```

3. Rufen Sie den Schlüssel für das Performance Service Level ab, das Sie dieser Dateifreigabe zuweisen möchten. Derzeit ist ihm keine Richtlinie zugewiesen.

Kategorie	HTTP-Verb	Weg
Leistungsservice-Levels	ERHALTEN	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie die `system_defined` Eingabeparameter zu `true` . Rufen Sie aus der Ausgabe den Schlüssel des Performance Service Level ab, den Sie auf die Dateifreigabe anwenden möchten.

4. Wenden Sie den Performance Service Level auf die Dateifreigabe an.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	PATCH	`/storage-provider/file-shares/{key}`

In der Eingabe müssen Sie nur den Parameter angeben, den Sie aktualisieren möchten, sowie den

Dateifreigabeschlüssel. In diesem Fall ist es der Schlüssel des Performance Service Levels.

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 Sie überprüfen können, ob die Zugriffsendpunkte auf den Home- und Partnerknoten erfolgreich erstellt wurden.

5. Überprüfen Sie mithilfe des in Ihrer Ausgabe angezeigten Jobobjektschlüssels, ob der Performance Service Level zur Dateifreigabe hinzugefügt wurde.

Kategorie	HTTP-Verb	Weg
Verwaltungsserver	ERHALTEN	`/management-server/jobs/{key}`

Wenn Sie die ID des Job-Objekts abfragen, sehen Sie, ob die Dateifreigabe erfolgreich aktualisiert wurde. Beheben Sie im Falle eines Fehlers den Fehler und führen Sie die API erneut aus. Fragen Sie nach erfolgreicher Erstellung die Dateifreigabe ab, um das geänderte Objekt anzuzeigen:

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/file-shares/{key}`

Sehen Sie sich die Details der Dateifreigabe in der Ausgabe an.

```
"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"
            }
        }
```

LUNs aktualisieren

Beim Aktualisieren einer LUN können Sie die folgenden Parameter ändern:

- Kapazität oder Größe
- Online- oder Offline-Einstellung
- Richtlinie zur Speichereffizienz
- Leistungsservicelevel
- LUN-Karte

Während eines einzelnen API-Laufs können Sie nur einen Parameter aktualisieren.

Dieses Verfahren beschreibt das Hinzufügen eines Performance Service Levels zu einer LUN. Sie können dasselbe Verfahren zum Aktualisieren jeder anderen LUN-Eigenschaft verwenden.

1. Besorgen Sie sich den LUN-Schlüssel der LUN, die Sie aktualisieren möchten. Diese API gibt Details zu allen LUNs in Ihrem Rechenzentrum zurück. Überspringen Sie diesen Schritt, wenn Sie den LUN-Schlüssel bereits kennen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/luns`

2. Zeigen Sie die Details der LUN an, indem Sie die folgende API mit dem LUN-Schlüssel ausführen, den Sie erhalten haben.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/luns/{key}`

   Sehen Sie sich die Details der LUN in der Ausgabe an. Sie können sehen, dass dieser LUN kein Performance-Service-Level zugewiesen ist.

   Beispiel für JSON-Ausgabe

```
"assigned_performance_service_level": {
      "key": null,
      "name": "Unassigned",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
```

3. Besorgen Sie sich den Schlüssel für das Performance Service Level, das Sie der LUN zuweisen möchten.

Kategorie	HTTP-Verb	Weg
Leistungsservice-Levels	ERHALTEN	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie die `system_defined` Eingabeparameter zu `true` . Ermitteln Sie aus der Ausgabe den Schlüssel des Performance Service Levels, den Sie auf die LUN anwenden möchten.

4. Wenden Sie den Performance Service Level auf die LUN an.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	PATCH	`/storage-provider/lun/{key}`

In der Eingabe müssen Sie nur den Parameter angeben, den Sie aktualisieren möchten, zusammen mit dem LUN-Schlüssel. In diesem Fall ist es der Schlüssel des Performance Service Levels.

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 von Ihnen aktualisierte LUN überprüfen können.

5. Zeigen Sie die Details der LUN an, indem Sie die folgende API mit dem LUN-Schlüssel ausführen, den Sie erhalten haben.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/luns/{key}`

Sehen Sie sich die Details der LUN in der Ausgabe an. Sie können sehen, dass dieser LUN das Performance Service Level zugewiesen ist.

Beispiel für 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 Sie eine NFS-Dateifreigabe mithilfe von APIs zur Unterstützung von CIFS

Sie können eine NFS-Dateifreigabe ändern, um das CIFS-Protokoll zu unterstützen. Während der Erstellung der Dateifreigabe können sowohl Parameter der Zugriffskontrollliste (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 auf dieser Dateifreigabe aktualisieren, um CIFS zu unterstützen.

Bevor Sie beginnen

1. Eine NFS-Dateifreigabe muss nur mit den Exportrichtliniendetails erstellt worden sein. Weitere Informationen finden Sie unter *Dateifreigaben verwalten* und *Speicher-Workloads ändern*.
2. Sie müssen über den Dateifreigabeschlüssel verfügen, um diesen Vorgang auszuführen. Informationen zum Anzeigen von Dateifreigabedetails und zum Abrufen des Dateifreigabeschlüssels mithilfe der Job-ID finden Sie unter *Bereitstellung 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, um die ACL-Parameter einzuschließen.

Schritte

1. Führen Sie auf der NFS-Dateifreigabe einen `PATCH` Vorgang mit den ACL-Details zum Erlauben des CIFS-Zugriffs.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	PATCH	`/storage-provider/file-shares`

Beispiel-cURL

Basierend auf den Zugriffsrechten, die Sie der Benutzergruppe zuweisen, wie im folgenden Beispiel dargestellt, wird 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"
    }
```

Beispiel für JSON-Ausgabe

Der Vorgang gibt die Job-ID des Jobs zurück, der das Update ausführt.

2. Überprüfen Sie, ob die Parameter korrekt hinzugefügt wurden, indem Sie die Dateifreigabedetails für dieselbe Dateifreigabe abfragen.

Kategorie	HTTP-Verb	Weg
Speicheranbieter	ERHALTEN	`/storage-provider/file-shares/{key}`

Beispiel für 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 sehen, die zusammen mit der Exportrichtlinie derselben Dateifreigabe zugewiesen wurde.

Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite 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 Patente im Besitz von NetApp 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 zu Active IQ Unified Manager 9.16"

Copyright-Informationen

Copyright © 2025 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.