Documentazione Active IQ Unified Manager

Active IQ Unified Manager 9.12

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/it-it/active-iq-unified-manager-912/index.html on October 16, 2025. Always check docs.netapp.com for the latest.

Sommario

Documentazione Active IQ Unified Manager . . . 1
Note di rilascio . . . 2
Inizia subito . . . 3
Istruzioni di avvio rapido per le installazioni VMware . . . 3
Requisiti di sistema . . . 3
Installazione di Active IQ Unified Manager . . . 3
Istruzioni di avvio rapido per le installazioni Linux . . . 4
Requisiti di sistema . . . 4
Installazione di Active IQ Unified Manager . . . 4
Istruzioni di avvio rapido per le installazioni di Windows . . . 5
Requisiti di sistema . . . 5
Installazione di Active IQ Unified Manager . . . 6
Installare Unified Manager sui sistemi VMware vSphere . . . 7
Introduzione a Active IQ Unified Manager . . . 7
Funzioni del server Unified Manager . . . 7
Panoramica della sequenza di installazione . . . 7
Requisiti per l'installazione di Unified Manager . . . 8
Infrastruttura virtuale e requisiti di sistema hardware . . . 8
Software VMware e requisiti di installazione . . . 9
Browser supportati . . . 10
Requisiti di protocollo e porta . . . 11
Completamento del foglio di lavoro . . . 14
Installazione, aggiornamento e rimozione del software Unified Manager . . . 16
Panoramica del processo di implementazione . . . 16
Implementazione di Unified Manager . . . 17
Aggiornamento di Unified Manager . . . 20
Riavvio della macchina virtuale di Unified Manager . . . 23
Rimozione di Unified Manager . . . 23
Installare Unified Manager su sistemi Linux . . . 25
Introduzione a Active IQ Unified Manager . . . 25
Funzioni del server Unified Manager . . . 25
Panoramica della sequenza di installazione . . . 25
Requisiti per l'installazione di Unified Manager . . . 26
Infrastruttura virtuale e requisiti di sistema hardware . . . 26
Software Linux e requisiti di installazione . . . 28
Browser supportati . . . 30
Requisiti di protocollo e porta . . . 30
Completamento del foglio di lavoro . . . 33
Installazione, aggiornamento e rimozione del software Unified Manager . . . 35
Panoramica del processo di installazione . . . 35
Configurazione dei repository software richiesti . . . 35
Requisiti SELinux sulle condivisioni NFS e CIFS . . . 37
Installazione di Unified Manager su sistemi Linux . . . 40

Aggiornamento di Unified Manager su Red Hat Enterprise Linux o CentOS . . . 47
Aggiornamento di prodotti di terze parti dopo l'installazione di Unified Manager . . . 52
Riavvio di Unified Manager . . . 52
Rimozione di Unified Manager . . . 53
Rimozione dell'utente umadmin personalizzato e del gruppo di manutenzione . . . 54
Installare Unified Manager su sistemi Windows . . . 55
Introduzione a Active IQ Unified Manager . . . 55
Funzioni del server Unified Manager . . . 55
Panoramica della sequenza di installazione . . . 55
Requisiti per l'installazione di Unified Manager . . . 56
Infrastruttura virtuale e requisiti di sistema hardware . . . 56
Software Windows e requisiti di installazione . . . 58
Browser supportati . . . 59
Requisiti di protocollo e porta . . . 60
Completamento del foglio di lavoro . . . 62
Installazione, aggiornamento e rimozione del software Unified Manager . . . 64
Panoramica del processo di installazione . . . 64
Installazione di Unified Manager su Windows . . . 65
Modifica della password JBoss . . . 68
Percorso di aggiornamento supportato per le versioni di Unified Manager . . . 69
Aggiornamento di Unified Manager . . . 69
Aggiornamento di prodotti di terze parti . . . 71
Riavvio di Unified Manager . . . 72
Disinstallazione di Unified Manager . . . 72
Eseguire attività amministrative e di configurazione . . . 74
Configurazione di Active IQ Unified Manager . . . 74
Panoramica della sequenza di configurazione . . . 74
Accesso all'interfaccia utente Web di Unified Manager . . . 74
Esecuzione della configurazione iniziale dell'interfaccia utente Web di Unified Manager . . . 75
Aggiunta di cluster . . . 77
Configurazione di Unified Manager per l'invio di notifiche di avviso . . . 79
Modifica della password utente locale . . . 88
Impostazione del timeout di inattività della sessione . . . 88
Modifica del nome host di Unified Manager . . . 89
Attivazione e disattivazione della gestione dello storage basata su policy . . . 93
Configurazione del backup di Unified Manager . . . 94
Gestione delle impostazioni delle funzioni . . . 94
Gestione dello storage basata su policy . . . 95
Abilitazione di API Gateway . . . 95
Specifica del timeout di inattività . . . 96
Attivazione degli eventi del portale Active IQ . . . 96
Attivazione e disattivazione delle impostazioni di sicurezza per la conformità . . . 97
Attivazione e disattivazione del caricamento degli script . . . 98
Aggiunta banner di accesso . . . 98
Utilizzando la console di manutenzione . . . 98

Quali funzionalità offre la console di manutenzione . . . 98
Cosa fa l'utente che effettua la manutenzione . . . 99
Funzionalità diagnostiche per l'utente . . . 99
Accesso alla console di manutenzione . . . 99
Accesso alla console di manutenzione mediante la console vSphere VM . . . 100
Menu della console di manutenzione . . . 101
Modifica della password utente per la manutenzione in Windows . . . 106
Modifica della password di umadmin sui sistemi Linux . . . 106
Modifica delle porte utilizzate da Unified Manager per i protocolli HTTP e HTTPS . . . 107
Aggiunta di interfacce di rete . . . 107
Aggiunta di spazio su disco alla directory del database di Unified Manager . . . 108
Gestione dell'accesso degli utenti . . . 112
Aggiunta di utenti . . . 112
Modifica delle impostazioni utente . . . 113
Visualizzazione degli utenti . . . 114
Eliminazione di utenti o gruppi . . . 114
Cos'è RBAC . . . 114
Che cosa fa il controllo degli accessi basato sui ruoli . . . 115
Definizioni dei tipi di utente . . . 115
Definizioni dei ruoli utente . . . 116
Ruoli e funzionalità degli utenti di Unified Manager . . . 117
Gestione delle impostazioni di autenticazione SAML . . . 118
Requisiti del provider di identità . . . 119
Attivazione dell'autenticazione SAML . . . 120
Modifica del provider di identità utilizzato per l'autenticazione SAML . . . 121
Aggiornamento delle impostazioni di autenticazione SAML dopo la modifica del certificato di protezione di Unified Manager . . . 122
Disattivazione dell'autenticazione SAML . . . 123
Disattivazione dell'autenticazione SAML dalla console di manutenzione . . . 124
Pagina SAML Authentication . . . 124
Gestione dell'autenticazione . . . 125
Modifica dei server di autenticazione . . . 125
Eliminazione dei server di autenticazione . . . 126
Autenticazione con Active Directory o OpenLDAP . . . 126
Registrazione dell'audit . . . 127
Pagina Remote Authentication (autenticazione remota . . . 129
Gestione dei certificati di sicurezza . . . 133
Visualizzazione del certificato di protezione HTTPS . . . 133
Download di una richiesta di firma del certificato HTTPS . . . 133
Installazione di un certificato HTTPS firmato e restituito dalla CA . . . 134
Installazione di un certificato HTTPS generato utilizzando strumenti esterni . . . 135
Descrizioni delle pagine per la gestione dei certificati . . . 137
Monitorare e gestire lo storage . . . 140
Introduzione a Active IQ Unified Manager . . . 140
Introduzione al monitoraggio dello stato di salute di Active IQ Unified Manager . . . 140

Introduzione al monitoraggio delle performance di Active IQ Unified Manager . . . 141
Utilizzo delle API REST di Unified Manager . . . 142
Funzioni del server Unified Manager . . . 142
Comprensione dell'interfaccia utente . . . 143
Layout tipici delle finestre . . . 143
Personalizzazione del layout delle finestre . . . 144
Utilizzo della Guida di Unified Manager . . . 145
Aggiunta di segnalibri agli argomenti della guida preferiti . . . 146
Ricerca di oggetti storage . . . 146
Esportazione dei dati di storage come report . . . 148
Filtraggio del contenuto della pagina di inventario . . . 149
Visualizzazione degli eventi attivi dal campanello di notifica . . . 150
Monitoraggio e gestione dei cluster dalla dashboard . . . 150
Pagina del dashboard . . . 151
Gestione dei problemi o delle funzionalità di ONTAP direttamente da Unified Manager . . . 154
Gestione dei cluster . . . 161
Come funziona il processo di rilevamento del cluster . . . 161
Visualizzazione dell'elenco dei cluster monitorati . . . 162
Aggiunta di cluster . . . 163
Modifica dei cluster . . . 165
Rimozione dei cluster . . . 166
Riscoprendo i cluster . . . 166
Monitoraggio dell'infrastruttura virtuale VMware . . . 167
Cosa non è supportato . . . 169
Visualizzazione e aggiunta di vCenter Server . . . 170
Monitoraggio delle macchine virtuali . . . 172
Visualizzazione dell'infrastruttura virtuale in una configurazione di disaster recovery . . . 174
Provisioning e gestione dei carichi di lavoro . . . 176
Panoramica sui carichi di lavoro . . . 176
Performance livelli di servizio . . . 184
Gestione delle policy di efficienza dello storage . . . 191
Gestione e monitoraggio delle configurazioni MetroCluster . . . 193
Comportamento del volume durante lo switchover e lo switchback . . . 193
Definizioni dello stato di connettività del cluster per la configurazione MetroCluster su FC . . . 195
Definizioni dello stato del mirroring dei dati per MetroCluster su FC . . . 196
Monitoraggio delle configurazioni MetroCluster . . . 197
Monitoraggio della replica MetroCluster . . . 200
Gestione delle quote . . . 201
Quali sono i limiti di quota . . . 201
Visualizzazione delle quote di utenti e gruppi di utenti . . . 201
Creazione di regole per la generazione di indirizzi e-mail . . . 201
Creazione di un formato di notifica e-mail per le quote di utenti e gruppi di utenti . . . 202
Modifica degli indirizzi e-mail delle quote di utenti e gruppi . . . 203
Ulteriori informazioni sulle quote . . . 203
Descrizione delle finestre di dialogo quote . . . 204

Risoluzione dei problemi . . . 208
Aggiunta di spazio su disco alla directory del database di Unified Manager . . . 208
Modifica dell'intervallo di raccolta delle statistiche delle performance . . . 211
Modifica del periodo di tempo in cui Unified Manager conserva i dati relativi a eventi e performance . . . 212
Errore di autenticazione sconosciuto . . . 213
Utente non trovato . . . 213
Problema con l'aggiunta di LDAP utilizzando altri servizi di autenticazione . . . 214
Gestire eventi e avvisi . . . 215
Gestione degli eventi . . . 215
Quali sono gli eventi della piattaforma Active IQ . . . 215
Quali sono gli eventi del sistema di gestione degli eventi . . . 215
Cosa succede quando si riceve un evento . . . 221
Visualizzazione di eventi e dettagli dell'evento . . . 222
Visualizzazione di eventi non assegnati . . . 223
Riconoscimento e risoluzione degli eventi . . . 223
Assegnazione di eventi a utenti specifici . . . 224
Disattivazione degli eventi indesiderati . . . 225
Risoluzione dei problemi con la risoluzione automatica di Unified Manager . . . 226
Attivazione e disattivazione del reporting degli eventi Active IQ . . . 227
Caricamento di un nuovo file di regole Active IQ . . . 228
Come vengono generati gli eventi della piattaforma Active IQ . . . 229
Risoluzione degli eventi della piattaforma Active IQ . . . 229
Configurazione delle impostazioni di conservazione degli eventi . . . 230
Cos'è una finestra di manutenzione di Unified Manager . . . 230
Gestione degli eventi delle risorse del sistema host . . . 233
Ulteriori informazioni sugli eventi . . . 233
Elenco degli eventi e dei tipi di severità . . . 239
Descrizione delle finestre di dialogo e degli eventi . . . 299
Gestione degli avvisi . . . 311
Quali sono gli avvisi . . . 311
Quali informazioni sono contenute in un messaggio di posta elettronica di avviso . . . 312
Aggiunta di avvisi . . . 312
Aggiunta di avvisi per eventi relativi alle performance . . . 315
Test degli avvisi . . . 316
Attivazione e disattivazione degli avvisi per gli eventi risolti e obsoleti . . . 317
Esclusione dei volumi di destinazione per il disaster recovery dalla generazione di avvisi . . . 317
Visualizzazione degli avvisi . . . 318
Modifica degli avvisi . . . 318
Eliminazione degli avvisi . . . 319
Descrizione delle finestre di avviso e delle finestre di dialogo . . . 319
Gestione degli script . . . 325
Come funzionano gli script con gli avvisi . . . 325
Aggiunta di script . . . 326
Eliminazione degli script . . . 327
Esecuzione di test dello script . . . 328

Comandi CLI di Unified Manager supportati . . . 328
Descrizione delle finestre di script e delle finestre di dialogo . . . 334
Monitorare e gestire le performance del cluster . . . 336
Introduzione al monitoraggio delle performance di Active IQ Unified Manager . . . 336
Funzionalità di monitoraggio delle performance di Unified Manager . . . 336
Interfacce di Unified Manager utilizzate per gestire le performance del sistema storage . . . 337
Attività di raccolta dei dati relativi alla configurazione e alle performance del cluster . . . 337
Che cos'è un ciclo di raccolta di continuità dei dati . . . 339
Cosa significa il timestamp nei dati e negli eventi raccolti . . . 340
Navigazione nei flussi di lavoro delle performance nella GUI di Unified Manager . . . 340
Accesso all'interfaccia utente . . . 340
Interfaccia grafica e percorsi di navigazione . . . 341
Ricerca di oggetti storage . . . 346
Filtraggio del contenuto della pagina di inventario . . . 347
Monitoraggio delle performance del cluster dalla dashboard . . . 349
Informazioni sui pannelli delle performance della dashboard . . . 349
Messaggi e descrizioni dei banner delle performance . . . 350
Modifica dell'intervallo di raccolta delle statistiche delle performance . . . 350
Risoluzione dei problemi dei carichi di lavoro utilizzando l'analizzatore dei carichi di lavoro . . . 351
Quali dati vengono visualizzati dall'analizzatore del carico di lavoro . . . 352
Quando dovrei utilizzare l'analizzatore del carico di lavoro . . . 353
Utilizzo dell'analizzatore del carico di lavoro . . . 354
Monitoraggio delle performance del cluster dalla pagina di destinazione del cluster di performance . . . 354
Informazioni sulla pagina di destinazione del cluster di performance . . . 354
Pagina di destinazione del cluster di performance . . . 355
Monitoraggio delle performance tramite le pagine Performance Inventory . . . 360
Visualizzazione delle pagine di inventario delle performance per tutti gli oggetti di storage . . . 361
Perfezionare il contenuto della pagina dell'inventario delle performance . . . 367
Comprendere le raccomandazioni di Unified Manager per il Tier dei dati nel cloud . . . 369
Monitoraggio delle performance tramite le pagine Performance Explorer . . . 371
Comprensione dell'oggetto root . . . 371
Applicare il filtraggio per ridurre l'elenco degli oggetti correlati nella griglia . . . 371
Specifica di un intervallo di tempo per gli oggetti correlati . . . 371
Definizione dell'elenco degli oggetti correlati per il grafico di confronto . . . 373
Comprensione dei diagrammi di contatore . . . 374
Tipi di tabelle dei contatori delle performance . . . 375
Selezione dei grafici delle prestazioni da visualizzare . . . 378
Espansione del riquadro Counter Chart . . . 379
Modifica della messa a fuoco dei Counter Chart in un periodo di tempo più breve . . . 379
Visualizzazione dei dettagli dell'evento nella cronologia degli eventi . . . 380
Counter Chart Zoom View . . . 380
Visualizzazione della latenza del volume in base al componente del cluster . . . 383
Visualizzazione del traffico IOPS SVM in base al protocollo . . . 384
Visualizzazione dei diagrammi di latenza del volume e del LUN per verificare la garanzia delle performance . . . 384

Visualizzazione delle performance per tutti i cluster di array SAN . . . 385
Visualizzazione degli IOPS dei nodi in base ai carichi di lavoro che risiedono solo sul nodo locale . . . 385
Componenti delle pagine di destinazione degli oggetti . . . 386
Gestione delle performance utilizzando le informazioni del gruppo di policy QoS . . . 392
In che modo la QoS dello storage può controllare il throughput dei carichi di lavoro . . . 392
Visualizzazione di tutti i gruppi di policy QoS disponibili su tutti i cluster . . . 393
Visualizzazione di volumi o LUN che si trovano nello stesso gruppo di criteri QoS . . . 394
Visualizzazione delle impostazioni del gruppo di criteri QoS applicate a volumi o LUN specifici . . . 395
Visualizzazione dei grafici delle performance per confrontare volumi o LUN che si trovano nello stesso gruppo di criteri QoS . . . 395
Come vengono visualizzati i diversi tipi di policy QoS nei grafici di throughput . . . 396
Visualizzazione delle impostazioni minime e massime QoS del carico di lavoro in Performance Explorer . . . 397
Gestire le performance utilizzando la capacità delle performance e le informazioni IOPS disponibili . . . 398
Qual è la capacità di performance utilizzata . . . 399
Cosa significa il valore utilizzato dalla capacità delle performance . . . 400
Quali IOPS sono disponibili . . . 401
Visualizzazione dei valori utilizzati per la capacità di nodo e le performance aggregate . . . 402
Visualizzazione dei valori IOPS disponibili di nodo e aggregazione . . . 403
Visualizzazione dei grafici dei contatori di capacità delle performance per identificare i problemi . . . 404
La capacità di performance ha utilizzato le condizioni di soglia delle performance . . . 406
Utilizzo della capacità di performance utilizzata per gestire le performance . . . 407
Informazioni e utilizzo della pagina Node failover Planning (Pianificazione del failover del nodo) . . . 408
Utilizzo della pagina Node failover Planning (Pianificazione del failover del nodo) per determinare le azioni correttive . . . 408
Componenti della pagina Node failover Planning (Pianificazione del failover del nodo) . . . 408
Utilizzo di un criterio di soglia con la pagina Node failover Planning (Pianificazione del failover del nodo) . . . 410
Utilizzo del grafico di dettaglio Performance Capacity Used per la pianificazione del failover . . . 410
Raccolta di dati e monitoraggio delle performance dei carichi di lavoro . . . 412
Tipi di workload monitorati da Unified Manager . . . 412
Valori di misurazione delle performance del carico di lavoro . . . 413
Qual è la gamma di performance prevista . . . 415
Come viene utilizzata la previsione di latenza nell'analisi delle performance . . . 416
Come Unified Manager utilizza la latenza dei workload per identificare i problemi di performance . . . 417
In che modo le operazioni del cluster possono influire sulla latenza del carico di lavoro . . . 418
Monitoraggio delle performance delle configurazioni MetroCluster . . . 419
Informazioni su eventi e avvisi relativi alle performance . . . 420
Fonti di eventi relativi alle performance . . . 420
Tipi di severità degli eventi relativi alle performance . . . 421
Modifiche alla configurazione rilevate da Unified Manager . . . 422
Tipi di criteri di soglia delle performance definiti dal sistema . . . 422
Analisi e notifica degli eventi relativi alle performance . . . 425
In che modo Unified Manager determina l'impatto delle performance di un evento . . . 427
Componenti del cluster e perché possono essere in conflitto . . . 427

Ruoli dei carichi di lavoro coinvolti in un evento di performance . . . 429
Gestione delle soglie di performance . . . 431
Come funzionano le policy di soglia delle performance definite dall'utente . . . 431
Cosa accade quando una policy di soglia delle performance viene violata . . . 433
Quali contatori delle performance possono essere monitorati utilizzando le soglie . . . 433
Quali oggetti e contatori possono essere utilizzati in policy di soglia combinate . . . 435
Creazione di criteri di soglia delle performance definiti dall'utente . . . 436
Assegnazione di criteri di soglia delle performance agli oggetti di storage . . . 438
Visualizzazione dei criteri di soglia delle performance . . . 439
Modifica dei criteri di soglia delle performance definiti dall'utente . . . 439
Rimozione dei criteri di soglia delle performance dagli oggetti storage . . . 440
Cosa accade quando viene modificata una policy di soglia delle performance . . . 440
Cosa accade ai criteri di soglia delle performance quando un oggetto viene spostato . . . 441
Analisi degli eventi relativi alle performance . . . 442
Visualizzazione di informazioni sugli eventi relativi alle performance . . . 442
Analisi degli eventi dalle soglie di performance definite dall'utente . . . 443
Analisi degli eventi dalle soglie di performance definite dal sistema . . . 444
Analisi degli eventi dalle soglie di performance dinamiche . . . 450
Risoluzione degli eventi relativi alle performance . . . 458
Conferma che la latenza rientra nell'intervallo previsto . . . 458
Esaminare l'impatto delle modifiche alla configurazione sulle performance del carico di lavoro . . . 458
Opzioni per migliorare le performance dei carichi di lavoro dal lato client . . . 458
Verificare la presenza di problemi relativi al client o alla rete . . . 459
Verificare se altri volumi nel gruppo di policy QoS hanno un'attività insolitamente elevata . . . 459
Spostare le interfacce logiche (LIF) . . . 460
Eseguire operazioni di efficienza dello storage in tempi meno impegnati . . . 460
Aggiungere dischi e riallocare i dati . . . 461
In che modo l'attivazione di Flash cache su un nodo può migliorare le performance dei carichi di lavoro . . . 462
In che modo l'abilitazione di Flash Pool su un aggregato di storage può migliorare le performance dei carichi di lavoro . . . 462
Verifica dello stato di salute della configurazione MetroCluster . . . 463
Verifica della configurazione MetroCluster . . . 463
Spostamento dei carichi di lavoro in un aggregato diverso . . . 464
Spostamento dei carichi di lavoro in un nodo diverso . . . 465
Spostamento dei carichi di lavoro in un aggregato su un nodo diverso . . . 466
Spostamento dei carichi di lavoro in un nodo di una coppia ha diversa . . . 468
Spostamento dei carichi di lavoro in un altro nodo di una coppia ha diversa . . . 470
Utilizzare le impostazioni dei criteri QoS per assegnare priorità al lavoro su questo nodo . . . 472
Rimuovere volumi e LUN inattivi . . . 472
Aggiungere dischi ed eseguire la ricostruzione del layout aggregato . . . 473
Impostazione di una connessione tra un server Unified Manager e un provider di dati esterno . . . 473
Dati sulle performance che possono essere inviati a un server esterno . . . 473
Impostazione di Graphite per ricevere i dati sulle performance da Unified Manager . . . 474
Configurazione di una connessione da un server Unified Manager a un provider di dati esterno . . . 475

Monitorare e gestire lo stato dei cluster . . . 478
Introduzione al monitoraggio dello stato di salute di Active IQ Unified Manager . . . 478
Capacità fisica e logica . . . 478
Unità di misura della capacità . . . 478
Funzionalità di monitoraggio dello stato di Unified Manager . . . 479
Interfacce di Unified Manager utilizzate per gestire lo stato di salute del sistema storage . . . 480
Gestione e monitoraggio dei cluster e dello stato degli oggetti del cluster . . . 481
Comprendere il monitoraggio dei cluster . . . 481
Visualizzazione dell'elenco e dei dettagli del cluster . . . 482
Verifica dello stato dei cluster in una configurazione MetroCluster . . . 483
Visualizzazione dello stato di salute e capacità di tutti i cluster di array SAN . . . 485
Visualizzazione dell'elenco dei nodi e dei dettagli . . . 486
Generazione di un report sull'inventario hardware per il rinnovo del contratto . . . 487
Visualizzazione dell'elenco e dei dettagli di Storage VM . . . 487
Visualizzazione dell'elenco aggregato e dei dettagli . . . 488
Visualizzazione delle informazioni sulla capacità FabricPool . . . 488
Visualizzazione dei dettagli del pool di storage . . . 490
Visualizzazione dell'elenco e dei dettagli dei volumi . . . 490
Visualizzazione dei dettagli sulle condivisioni NFS . . . 491
Visualizzazione dei dettagli sulle condivisioni SMB/CIFS . . . 492
Visualizzazione dell'elenco delle copie Snapshot . . . 493
Eliminazione delle copie Snapshot . . . 493
Calcolo dello spazio recuperabile per le copie Snapshot . . . 494
Descrizione delle finestre di dialogo e degli oggetti del cluster . . . 495
Flussi di lavoro e attività comuni per lo stato di salute di Unified Manager . . . 495
Monitoraggio e troubleshooting della disponibilità dei dati . . . 497
Risoluzione dei problemi di capacità . . . 503
Gestione delle soglie di integrità . . . 505
Gestione degli obiettivi di sicurezza del cluster . . . 510
Gestione delle operazioni di backup e ripristino . . . 522
Gestione degli script . . . 539
Gestione e monitoraggio dei gruppi . . . 542
Assegnazione di priorità agli eventi degli oggetti di storage utilizzando le annotazioni . . . 551
Invio di un pacchetto di supporto tramite l'interfaccia utente Web e la console di manutenzione . . . 560
Attività e informazioni relative a diversi flussi di lavoro . . . 567
Proteggere e ripristinare i dati . . . 625
Creazione, monitoraggio e risoluzione dei problemi delle relazioni di protezione . . . 625
Tipi di protezione SnapMirror . . . 625
Impostazione delle relazioni di protezione in Unified Manager . . . 627
Esecuzione di failover e failback delle relazioni di protezione . . . 629
Risoluzione di un errore di un lavoro di protezione . . . 633
Risoluzione dei problemi di ritardo . . . 637
Gestione e monitoraggio delle relazioni di protezione . . . 638
Visualizzazione dello stato di protezione del volume . . . 638
Visualizzazione delle relazioni di protezione dei volumi . . . 641

Monitoraggio delle LUN in una relazione Consistency Group . . . 641
Creazione di una relazione di protezione SnapVault dalla vista Salute: Tutti i volumi . . . 642
Creazione di una relazione di protezione SnapVault dalla pagina dei dettagli relativi a volume/salute . . . 643
Creazione di una relazione di protezione SnapMirror dalla vista Health: All Volumes (Salute: Tutti i volumi) . . . 644
Creazione di una relazione di protezione SnapMirror dalla pagina dei dettagli relativi a volume/stato . . . 645
Creazione di una relazione SnapMirror con replica flessibile della versione . . . 647
Creazione di relazioni SnapMirror con replica flessibile della versione con opzione di backup . . . 648
Configurazione delle impostazioni di efficienza della destinazione . . . 649
Creazione di pianificazioni SnapMirror e SnapVault . . . 650
Creazione di relazioni a cascata o fan-out per estendere la protezione da una relazione di protezione esistente . . . 650
Modifica delle relazioni di protezione dalla pagina Relazioni volume . . . 651
Modifica delle relazioni di protezione dalla pagina Dettagli volume/salute . . . 652
Creazione di una policy SnapMirror per massimizzare l'efficienza del trasferimento . . . 652
Creazione di una policy SnapVault per massimizzare l'efficienza del trasferimento . . . 653
Interruzione di un trasferimento di protezione dei dati attivo dalla pagina Relazioni volume . . . 653
Interruzione di un trasferimento di protezione dei dati attivo dalla pagina dei dettagli relativi a volume/salute . . . 654
Interrompere una relazione di protezione dalla pagina delle relazioni dei volumi . . . 655
Interrompere una relazione di protezione dalla pagina dei dettagli relativi a volume/salute . . . 656
Interruzione di una relazione SnapMirror dalla pagina Relazioni volume . . . 657
Rimozione di una relazione di protezione dalla pagina Relazioni volume . . . 657
Ripresa dei trasferimenti pianificati su una relazione quiescente dalla pagina Volume Relationship (Relazioni volume) . . . 658
Ripresa dei trasferimenti pianificati su una relazione quiescente dalla pagina dei dettagli relativi a volume/salute . . . 658
Inizializzazione o aggiornamento delle relazioni di protezione dalla pagina Relazioni volume . . . 659
Inizializzazione o aggiornamento delle relazioni di protezione dalla pagina Dettagli volume/salute . . . 660
Risincronizzazione delle relazioni di protezione dalla pagina Relazioni volume . . . 661
Invertire le relazioni di protezione dalla pagina Relazioni volume . . . 662
Ripristino dei dati mediante le pagine dei dettagli volume e volume/salute . . . 663
Quali sono i pool di risorse . . . 664
Creazione di pool di risorse . . . 665
Modifica dei pool di risorse . . . 665
Visualizzazione dell'inventario dei pool di risorse . . . 666
Aggiunta di membri del pool di risorse . . . 666
Rimozione di aggregati dai pool di risorse . . . 666
Eliminazione dei pool di risorse . . . 667
Monitoraggio delle relazioni di protezione di Storage VM Disaster Recovery . . . 667
Informazioni sulle associazioni di Storage VM . . . 669
Requisiti di SVM e pool di risorse per supportare i servizi di storage . . . 672
Quali sono i posti di lavoro . . . 672
Monitoraggio dei lavori . . . 673
Visualizzazione dei dettagli del lavoro . . . 673

Interruzione dei lavori . . . 673
Tentativo di nuovo di un processo di protezione non riuscito . . . 674
Descrizione delle finestre di dialogo e delle relazioni di protezione . . . 674
Generare report personalizzati . . . 717
Reporting di Unified Manager . . . 717
Access point per la generazione di report . . . 717
Informazioni sui report . . . 719
Comprensione della relazione tra visualizzazione e report . . . 719
Tipi di report . . . 720
Limiti di reporting . . . 722
Utilizzo dei report . . . 722
Workflow dei report . . . 722
Avvio rapido dei report . . . 723
Ricerca di un report pianificato . . . 726
Personalizzazione dei report . . . 726
Download di report . . . 730
Pianificazione dei report . . . 730
Pianificazione di un report . . . 730
Gestione delle pianificazioni dei report . . . 733
Report personalizzati di esempio . . . 735
Personalizzazione dei report dello storage in cluster . . . 736
Personalizzazione dei report sulla capacità aggregata . . . 739
Personalizzazione dei report sulla capacità dei volumi . . . 741
Personalizzazione dei report di capacità di Qtree . . . 744
Personalizzazione dei report di condivisione NFS . . . 745
Personalizzazione dei report delle macchine virtuali di storage . . . 747
Personalizzazione dei report delle relazioni dei volumi . . . 748
Personalizzazione dei report sulle performance dei volumi . . . 752
Report Microsoft Excel di esempio . . . 753
Creazione di un report per visualizzare una tabella e un grafico della capacità aggregata . . . 753
Creazione di un report per visualizzare i grafici di capacità totale aggregato rispetto a quelli disponibili 756
Creazione di un report per visualizzare i grafici della capacità dei volumi disponibili . . . 759
Creazione di un report per visualizzare gli aggregati con IOPS più disponibili . . . 762
Gestire lo storage utilizzando API REST . . . 764
Introduzione alle API REST di Active IQ Unified Manager . . . 764
Destinatari di questo contenuto . . . 764
Accesso e categorie API Active IQ Unified Manager . . . 764
Servizi REST offerti in Active IQ Unified Manager . . . 766
Versione API in Active IQ Unified Manager . . . 766
Risorse di storage in ONTAP . . . 767
Autenticazione e accesso API REST in Active IQ Unified Manager . . . 768
Autenticazione . . . 770
Codici di stato HTTP utilizzati in Active IQ Unified Manager . . . 771
Raccomandazioni per l'utilizzo delle API per Active IQ Unified Manager . . . 772
Registri per la risoluzione dei problemi . . . 772

Processi asincroni degli oggetti di lavoro . . . 773
Ciao API server . . . 774
API REST di Unified Manager . . . 778
Gestione degli oggetti storage in un data center mediante API . . . 779
Accesso alle API ONTAP tramite accesso proxy . . . 786
Esecuzione di attività amministrative utilizzando le API . . . 788
Gestione degli utenti mediante API . . . 790
Visualizzazione delle metriche delle performance tramite le API . . . 791
Visualizzazione dei processi e dei dettagli di sistema . . . 801
Gestione di eventi e avvisi tramite API . . . 802
Gestione dei carichi di lavoro tramite API . . . 805
Flussi di lavoro API comuni per la gestione dello storage . . . 814
Informazioni sulle chiamate API utilizzate nei flussi di lavoro . . . 814
Determinare i problemi di spazio negli aggregati utilizzando le API . . . 814
Determinazione dei problemi negli oggetti di storage utilizzando le API degli eventi . . . 816
Risoluzione dei problemi relativi ai volumi ONTAP utilizzando le API del gateway . . . 817
Flussi di lavoro API per la gestione dei carichi di lavoro . . . 822
Note legali . . . 849
Copyright . . . 849
Marchi . . . 849
Brevetti . . . 849
Direttiva sulla privacy . . . 849
Open source . . . 849

Documentazione Active IQ Unified Manager

Note di rilascio

Viene fornito un riepilogo delle nuove funzionalità, delle limitazioni e dei problemi noti di Active IQ Unified Manager 9.12.

Per ulteriori informazioni, consultare "Note di rilascio di Active IQ Unified Manager".

Inizia subito

Istruzioni di avvio rapido per le installazioni VMware

È possibile scaricare `.tar` che contiene un certificato root, un `README` e un `OVA` File e implementazione di Unified Manager come appliance virtuale.

Requisiti di sistema

- Sistema operativo: VMware ESXi 6.5, 6.7 e 7.0.x.
- RAM: 12 GB
- CPU: 9572 MHz in totale
- Spazio libero su disco: 5 GB (thin provisioning), 152 GB (thick provisioning)

Per informazioni dettagliate sui requisiti di sistema, consultare "Requisiti per l'installazione di Unified Manager" e. "Matrice di interoperabilità".

Installazione di Active IQ Unified Manager

Scaricare il programma di installazione

1. Scaricare il `.tar` che contiene un certificato root, un `README` e un `OVA` file.
2. Salvare il file in una directory locale o di rete accessibile al client vSphere.
3. Nella directory in cui è stato scaricato `.tar` immettere il `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz` comando. + il necessario `OVA` file, un certificato root e un `README` i file vengono decompressi nella directory di destinazione.

Verificare l'integrità

È possibile verificare l'integrità di `OVA` eseguire la procedura descritta in `README` file.

Installare Unified Manager

1. In vSphere Client, fare clic su **file > Deploy OVF Template** (file > implementa modello OVF).
2. Individuare il file OVA e utilizzare la procedura guidata per implementare l'appliance virtuale sul server ESXi.
3. Nella pagina Review Details (Dettagli revisione), nella sezione Publisher, il messaggio `Entrust Code Signing - OVCS2 (Trusted certificate)` conferma l'integrità del scaricato `OVA` file. Per il messaggio `Entrust Code Signing - OVCS2 (Invalid certificate)`, Aggiornare VMware vCenter Server alla versione 7.0U3E o superiore.
4. Nella scheda Proprietà della pagina Personalizza modello, compilare i campi come richiesto per il tipo di installazione che si sta eseguendo:
   - Per la configurazione statica, inserire le informazioni richieste in tutti i campi. L'aggiunta di informazioni per il campo **DNS secondario** non è obbligatoria.
   - Per DHCP che utilizza IPv4, non aggiungere alcuna informazione in alcun campo.
   - Per DHCP che utilizza IPv6, selezionare la casella "Enable Auto IPv6 Addressing" (attiva

indirizzamento IPv6 automatico). Non aggiungere informazioni in altri campi.

5. Accendere la macchina virtuale.
6. Fare clic sulla scheda Console per visualizzare il processo di avvio iniziale.
7. Configurare il fuso orario.
8. Immettere un nome utente e una password per la manutenzione di Unified Manager.

Al termine dell'installazione, vengono visualizzate le informazioni per la connessione all'interfaccia utente Web di Unified Manager.

Istruzioni di avvio rapido per le installazioni Linux

È possibile scaricare il pacchetto di installazione e installare Unified Manager su una piattaforma fisica o virtuale Red Hat Enterprise Linux o CentOS.

Requisiti di sistema

- Sistema operativo: Red Hat Enterprise Linux versioni 7.x e da 8.0 a 8.6, o CentOS versione 7.x basato sull'architettura x86_64, installato utilizzando l'ambiente di base "Server with GUI" dall'opzione **Software Selection** del programma di installazione del sistema operativo
- RAM: 12 GB, CPU: 9572 MHz in totale
- Spazio libero su disco: 100 GB di spazio su disco in `/opt/netapp/data` 50 GB nella partizione root. Per montaggio separato `/opt` e. `/var/log` directory, assicurarsi che `/opt` Ha 15 GB, `/var/log` Ha 16 GB, e. `/tmp` Dispone di 10 GB di spazio libero.

Per informazioni dettagliate sui requisiti di sistema e sull'installazione del prodotto in un sito protetto, consultare la "Requisiti per l'installazione di Unified Manager" e a. "Matrice di interoperabilità".

Installazione di Active IQ Unified Manager

Scaricare il programma di installazione

1. Scaricare il `ActiveIQUnifiedManager-<version>.zip` pacchetto di installazione con certificato di firma del codice (`.pem`) e firma digitale (`.sig`) .
2. Nella directory in cui è stato scaricato il file di installazione, eseguire:

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

Verificare l'integrità

Eseguire i seguenti comandi per verificare l'integrità del pacchetto di installazione:

- Eseguire `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>` per creare un file con la chiave pubblica dal certificato di firma del codice.
- Eseguire `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip` per verificare la firma sul pacchetto di installazione.

Verificare la configurazione del repository

Le procedure per la configurazione dei repository Red Hat Enterprise Linux o CentOS sono specifiche del sito. È possibile utilizzare `pre_install_check.sh` script incluso nel pacchetto di installazione per verificare la configurazione del sistema operativo. Se il sistema è connesso a Internet, riceverai automaticamente le istruzioni per la configurazione dei repository Red Hat Enterprise Linux o CentOS.

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

Installare Unified Manager

Unified Manager utilizza `yum` utility per installare il software e qualsiasi software dipendente. Poiché esistono immagini diverse di Red Hat Enterprise Linux o CentOS, i pacchetti installati dipendono dal software presente nelle immagini. Il `yum` l'utility determina i pacchetti software dipendenti per l'installazione. Per ulteriori informazioni sui pacchetti software dipendenti, consultare la "Software Linux e requisiti di installazione".

Per installare Unified Manager, eseguire il seguente comando, come utente root o utilizzando `sudo`, dalla directory in cui è stato decompresso il file di installazione:

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

oppure

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

Al termine dell'installazione, vengono visualizzate le informazioni per la connessione all'interfaccia utente Web di Unified Manager. Se non si riesce a connettersi all'interfaccia utente Web, fare riferimento a. `README` file fornito con il software per ulteriori informazioni sulle restrizioni della porta 443.

Istruzioni di avvio rapido per le installazioni di Windows

È possibile scaricare il pacchetto di installazione e installare Unified Manager per monitorare e risolvere i problemi di capacità, disponibilità, performance e protezione dello storage dei dati.

Requisiti di sistema

- Sistemi operativi
  - Microsoft Windows Server 2019 Standard e Datacenter Edition
  - Microsoft Windows Server 2022 Standard e Datacenter Edition

    Unified Manager è supportato dal sistema operativo Windows a 64 bit per le seguenti lingue:

  - Inglese
  - Giapponese
  - Cinese semplificato
- RAM: 12 GB
- CPU: 9572 MHz in totale
- Spazio libero su disco: 100 GB di spazio su disco per la directory di installazione, 50 GB di spazio su disco per la directory dei dati MySQL

Per informazioni dettagliate sui requisiti di sistema, consultare "Requisiti per l'installazione di Unified Manager" e. "Matrice di interoperabilità".

Installazione di Active IQ Unified Manager

Scaricare il programma di installazione

1. Scaricare il `ActiveIQUnifiedManager-<version>.exe` pacchetto di installazione.
2. Copiare il file di installazione in una directory del sistema di destinazione.

Installare Unified Manager

Per installare Unified Manager, assicurarsi di avere installato Microsoft .NET 4.5 o una versione successiva. Come parte del processo di installazione, Unified Manager installa altri pacchetti di terze parti secondo necessità. Per ulteriori informazioni sui pacchetti software dipendenti, fare riferimento a. "Software Windows e requisiti di installazione".

1. Accedere a Windows utilizzando l'account di amministratore locale predefinito.
2. Nella directory in cui è stato scaricato il file di installazione, fare clic con il pulsante destro del mouse ed eseguire il file eseguibile di Unified Manager (.exe) come amministratore.
3. Quando richiesto, inserire il nome utente e la password per creare l'utente di manutenzione di Unified Manager.
4. Nella procedura guidata connessione database, inserire la password root MySQL.
5. Seguire le istruzioni rimanenti per completare l'installazione.
6. Fare clic su **fine** al termine dell'installazione per visualizzare l'interfaccia utente Web di Unified Manager.

Installare Unified Manager sui sistemi VMware vSphere

Introduzione a Active IQ Unified Manager

Active IQ Unified Manager (in precedenza Unified Manager di OnCommand) consente di monitorare e gestire lo stato di salute e le performance dei sistemi storage ONTAP da una singola interfaccia. È possibile implementare Unified Manager su un server Linux, su un server Windows o come appliance virtuale su un host VMware.

Una volta completata l'installazione e aggiunti i cluster che si desidera gestire, Unified Manager fornisce un'interfaccia grafica che visualizza lo stato di capacità, disponibilità, protezione e performance dei sistemi storage monitorati.

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Funzioni del server Unified Manager

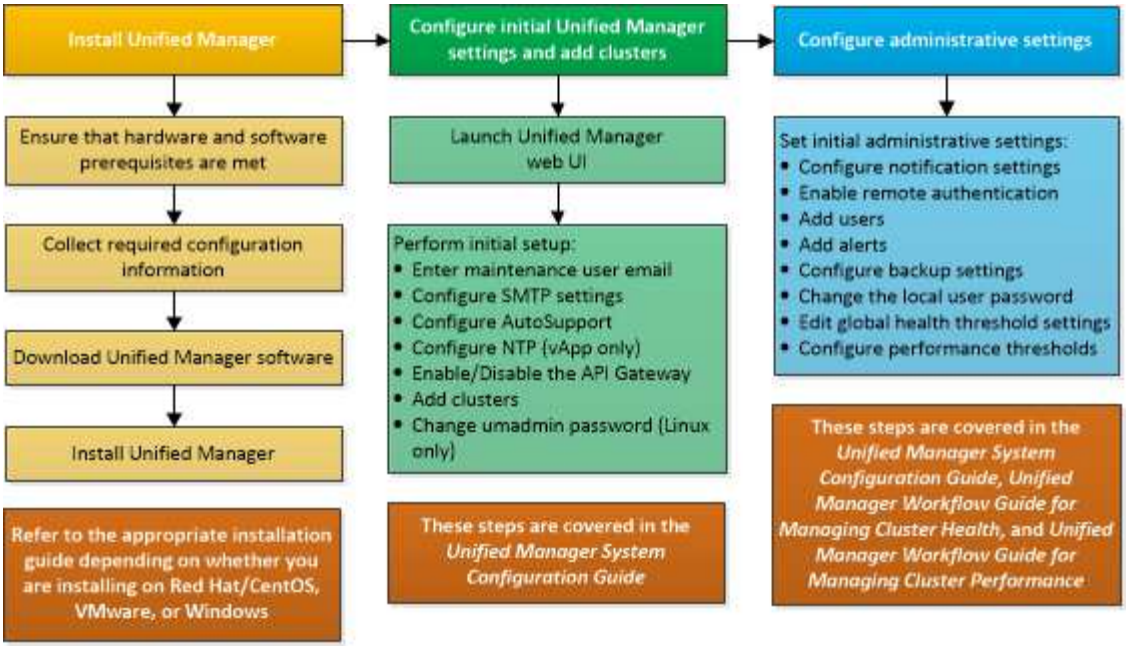
L'infrastruttura server di Unified Manager è costituita da un'unità di raccolta dati, un database e un server applicazioni. Fornisce servizi di infrastruttura come rilevamento, monitoraggio, RBAC (role-based access control), audit e logging.

Unified Manager raccoglie le informazioni sul cluster, memorizza i dati nel database e li analizza per verificare l'eventuale presenza di problemi nel cluster.

Panoramica della sequenza di installazione

Il flusso di lavoro di installazione descrive le attività da eseguire prima di poter utilizzare Unified Manager.

Queste sezioni descrivono ciascuno degli elementi mostrati nel flusso di lavoro seguente.



Requisiti per l'installazione di Unified Manager

Prima di iniziare il processo di installazione, assicurarsi che il server su cui si desidera installare Unified Manager soddisfi i requisiti specifici di software, hardware, CPU e memoria.

NetApp non supporta alcuna modifica del codice applicativo di Unified Manager. Se è necessario applicare misure di sicurezza al server Unified Manager, è necessario apportare tali modifiche al sistema operativo su cui è installato Unified Manager.

Per ulteriori informazioni sull'applicazione delle misure di sicurezza al server Unified Manager, consultare l'articolo della Knowledge base.

"Supporto per le misure di sicurezza applicate a Active IQ Unified Manager per Clustered Data ONTAP"

Informazioni correlate

Per ulteriori informazioni, vedere "Tool di matrice di interoperabilità NetApp"

Infrastruttura virtuale e requisiti di sistema hardware

L'installazione di Unified Manager su un'infrastruttura virtuale o su un sistema fisico deve soddisfare i requisiti minimi di memoria, CPU e spazio su disco.

La seguente tabella mostra i valori consigliati per le risorse di memoria, CPU e spazio su disco. Questi valori sono stati qualificati in modo che Unified Manager soddisfi livelli di performance accettabili.

Configurazione dell'hardware	Impostazioni consigliate
RAM	12 GB (requisito minimo 8 GB)
Processori	4 CPU

Configurazione dell'hardware	Impostazioni consigliate
Capacità del ciclo della CPU	9572 MHz totali (requisito minimo 9572 MHz)
Spazio libero su disco	• 5 GB (thin provisioning) • 152 GB (con thick provisioning)

Unified Manager può essere installato su sistemi con una piccola quantità di memoria, ma i 12 GB di RAM consigliati garantiscono che sia disponibile una quantità di memoria sufficiente per ottenere performance ottimali e che il sistema possa ospitare cluster e oggetti di storage aggiuntivi con la crescita della configurazione. Non è necessario impostare limiti di memoria sulla macchina virtuale in cui è implementato Unified Manager e non attivare alcuna funzione (ad esempio, la bollatura) che impedisca al software di utilizzare la memoria allocata nel sistema.

Inoltre, esiste un limite al numero di nodi che una singola istanza di Unified Manager può monitorare prima di installare una seconda istanza di Unified Manager. Per ulteriori informazioni, vedere "Guida alle Best practice di Unified Manager".

Lo swapping della pagina di memoria influisce negativamente sulle prestazioni del sistema e dell'applicazione di gestione. La concorrenza per le risorse CPU non disponibili a causa dell'utilizzo complessivo dell'host può compromettere le prestazioni.

Requisito per l'utilizzo dedicato

Il sistema fisico o virtuale su cui si installa Unified Manager deve essere utilizzato esclusivamente per Unified Manager e non deve essere condiviso con altre applicazioni. Altre applicazioni potrebbero consumare risorse di sistema e ridurre drasticamente le performance di Unified Manager.

Requisiti di spazio per i backup

Se si intende utilizzare la funzione di backup e ripristino di Unified Manager, allocare ulteriore capacità in modo che la directory o il disco "data" disponga di 150 GB di spazio. Un backup può essere scritto in una destinazione locale o remota. La procedura consigliata consiste nell'identificare una postazione remota esterna al sistema host di Unified Manager che abbia almeno 150 GB di spazio.

Requisiti per la connettività host

Il sistema fisico o virtuale su cui si installa Unified Manager deve essere configurato in modo da poter essere correttamente configurato `ping` il nome host dell'host stesso. In caso di configurazione IPv6, è necessario verificarlo `ping6` Al nome host per garantire che l'installazione di Unified Manager abbia esito positivo.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web del prodotto. Se è stato configurato un indirizzo IP statico per la rete durante l'implementazione, è stato designato un nome per l'host di rete. Se la rete è stata configurata utilizzando DHCP, è necessario ottenere il nome host dal DNS.

Se si prevede di consentire agli utenti di accedere a Unified Manager utilizzando il nome breve invece di utilizzare il nome di dominio completo (FQDN) o l'indirizzo IP, la configurazione di rete deve risolvere questo nome breve in un FQDN valido.

Software VMware e requisiti di installazione

Il sistema VMware vSphere su cui si installa Unified Manager richiede versioni specifiche

del sistema operativo e del software di supporto.

Software del sistema operativo

Sono supportate le seguenti versioni di VMware ESXi:

- ESXi 6.5, 6.7 e 7.0.x.

> Unified Manager OVA su sistemi VMware vSphere esegue Debian OS 11 (bullseye) internamente. Per informazioni sulle versioni dell'hardware della macchina virtuale supportate dalle versioni supportate dei server ESXi, fare riferimento alla documentazione VMware.

Sono supportate le seguenti versioni di vSphere:

- VMware vCenter Server 6.5, 6.7 e 7.0.x.

Consulta la matrice di interoperabilità per l'elenco completo e aggiornato delle versioni di ESXi supportate.

"mysupport.netapp.com/matrix"

L'ora del server VMware ESXi deve coincidere con quella del server NTP affinché l'appliance virtuale funzioni correttamente. La sincronizzazione dell'ora del server VMware ESXi con l'ora del server NTP impedisce un errore di tempo.

Requisiti di installazione

VMware High Availability per l'appliance virtuale Unified Manager è supportata.

Se si implementa un datastore NFS su un sistema storage che esegue il software ONTAP, utilizzare il plug-in NFS NetApp per VMware VAAI per utilizzare il thick provisioning.

Se l'implementazione non riesce utilizzando l'ambiente abilitato per l'alta disponibilità a causa di risorse insufficienti, potrebbe essere necessario modificare le opzioni della macchina virtuale del cluster disattivando la priorità di riavvio della macchina virtuale e lasciando attiva la risposta di isolamento dell'host.

> Durante l'installazione o l'aggiornamento di Unified Manager, le patch di sicurezza e il software di terze parti richiesti vengono installati o aggiornati automaticamente su un sistema VMware vSphere. Poiché i processi di installazione e aggiornamento di Unified Manager controllano questi componenti, non tentare di eseguire un'installazione o un aggiornamento standalone di alcun componente di terze parti.

Browser supportati

Per accedere all'interfaccia utente Web di Unified Manager, utilizzare un browser supportato.

La matrice di interoperabilità contiene l'elenco delle versioni del browser supportate.

"mysupport.netapp.com/matrix"

Per tutti i browser, la disattivazione dei blocchi dei pop-up garantisce la corretta visualizzazione delle funzionalità software.

Se si intende configurare Unified Manager per l'autenticazione SAML, in modo che un provider di identità (IdP) possa autenticare gli utenti, è necessario controllare anche l'elenco dei browser supportati da IdP.

Requisiti di protocollo e porta

Le porte e i protocolli richiesti consentono la comunicazione tra il server Unified Manager e i sistemi di storage gestiti, i server e altri componenti.

Connessioni al server Unified Manager

Nelle installazioni tipiche non è necessario specificare i numeri di porta durante la connessione all'interfaccia utente Web di Unified Manager, poiché vengono sempre utilizzate le porte predefinite. Ad esempio, poiché Unified Manager tenta sempre di essere eseguito sulla porta predefinita, è possibile immettere `https://<host>` invece di `https://<host>:443`.

Il server Unified Manager utilizza protocolli specifici per accedere alle seguenti interfacce:

Interfaccia	Protocollo	Porta	Descrizione
UI Web di Unified Manager	HTTP	80	Utilizzato per accedere all'interfaccia utente Web di Unified Manager; reindirizza automaticamente alla porta sicura 443.
L'interfaccia utente Web di Unified Manager e i programmi che utilizzano API	HTTPS	443	Utilizzato per accedere in modo sicuro all'interfaccia utente Web di Unified Manager o per effettuare chiamate API; le chiamate API possono essere effettuate solo utilizzando HTTPS.
Console di manutenzione	SSH/SFTP	22	Utilizzato per accedere alla console di manutenzione e recuperare i pacchetti di supporto.
Riga di comando Linux	SSH/SFTP	22	Utilizzato per accedere alla riga di comando di Red Hat Enterprise Linux o CentOS e recuperare i bundle di supporto.

Interfaccia	Protocollo	Porta	Descrizione
Syslog	UDP	514	Utilizzato per accedere ai messaggi EMS basati su abbonamento dai sistemi ONTAP e per creare eventi in base ai messaggi.
RIPOSO	HTTPS	9443	Utilizzato per accedere agli eventi EMS basati su API REST in tempo reale da sistemi ONTAP autenticati.

La porta predefinita per MySQL, 3306, è limitata solo all'host locale durante l'installazione di Unified Manager su sistemi VMware vSphere. Questo non influisce su nessuno scenario di aggiornamento, in cui viene mantenuta la configurazione precedente. Questa configurazione può essere modificata e la connessione può essere resa disponibile ad altri host utilizzando `Control access to MySQL port 3306` sulla console di manutenzione. Per ulteriori informazioni, vedere "Opzioni di menu aggiuntive". Le porte utilizzate per le comunicazioni HTTP e HTTPS (porte 80 e 443) possono essere modificate utilizzando la console di manutenzione di Unified Manager. Per ulteriori informazioni, vedere "Menu della console di manutenzione".

Connessioni dal server Unified Manager

È necessario configurare il firewall in modo che apra le porte che consentono la comunicazione tra il server Unified Manager e i sistemi di storage gestiti, i server e altri componenti. Se una porta non è aperta, la comunicazione non riesce.

A seconda dell'ambiente in uso, è possibile scegliere di modificare le porte e i protocolli utilizzati dal server Unified Manager per connettersi a destinazioni specifiche.

Il server Unified Manager si connette utilizzando i seguenti protocolli e porte ai sistemi di storage gestiti, ai server e ad altri componenti:

Destinazione	Protocollo	Porta	Descrizione
Sistema storage	HTTPS	443/TCP	Utilizzato per monitorare e gestire i sistemi storage. Se si utilizza questa porta o qualsiasi altra porta per connettersi a VMware vCenter Server o al server ESXi, assicurarsi che la porta sia disponibile e possa essere collegata in un sito protetto.
Sistema storage	NDMP	10000/TCP	Utilizzato per alcune operazioni di ripristino Snapshot.
Server AutoSupport	HTTPS	443	Utilizzato per inviare informazioni AutoSupport. Per eseguire questa funzione, è necessario disporre dell'accesso a Internet.
Server di autenticazione	LDAP	389	Utilizzato per effettuare richieste di autenticazione e richieste di ricerca di utenti e gruppi.
LDAPS	636	Utilizzato per comunicazioni LDAP sicure.	Server di posta
SMTP	25	Utilizzato per inviare e-mail di notifica degli avvisi.	Mittente trap SNMP

Destinazione	Protocollo	Porta	Descrizione
SNMPv1 o SNMPv3	162/UDP	Utilizzato per inviare messaggi trap SNMP di notifica degli avvisi.	Server del provider di dati esterno
TCP	2003	Utilizzato per inviare dati sulle prestazioni a un provider di dati esterno, ad esempio Graphite.	Server NTP

Completamento del foglio di lavoro

Prima di installare e configurare Unified Manager, è necessario disporre di informazioni specifiche sull'ambiente in uso. È possibile registrare le informazioni nel foglio di lavoro.

Informazioni sull'installazione di Unified Manager

I dettagli necessari per installare Unified Manager.

Sistema su cui viene implementato il software	Il tuo valore
Indirizzo IP del server ESXi	
Nome di dominio completo dell'host	
Host IP address (Indirizzo IP host)	
Maschera di rete	
Indirizzo IP del gateway	
Indirizzo DNS primario	
Indirizzo DNS secondario	
Cerca domini	
Nome utente manutenzione	
Password utente per la manutenzione	

Informazioni sulla configurazione di Unified Manager

I dettagli per configurare Unified Manager dopo l'installazione. Alcuni valori sono facoltativi a seconda della configurazione.

Impostazione	Il tuo valore
Indirizzo e-mail utente manutenzione	
Server NTP	
Nome host o indirizzo IP del server SMTP	
Nome utente SMTP	
Password SMTP	
Porta SMTP	25 (valore predefinito)
E-mail da cui vengono inviate le notifiche di avviso	
Nome host o indirizzo IP del server di autenticazione	
Nome dell'amministratore di Active Directory o nome distinto del binding LDAP	
Password di Active Directory o bind LDAP	
Nome distinto della base del server di autenticazione	
URL del provider di identità (IdP)	
Metadati del provider di identità (IdP)	
Indirizzi IP host di destinazione del trap SNMP	
Porta SNMP	

Informazioni sul cluster

I dettagli dei sistemi storage gestiti con Unified Manager.

Cluster 1 di N.	Il tuo valore
Nome host o indirizzo IP di gestione del cluster	
Nome utente amministratore di ONTAP All'amministratore deve essere stato assegnato il ruolo "admin".	

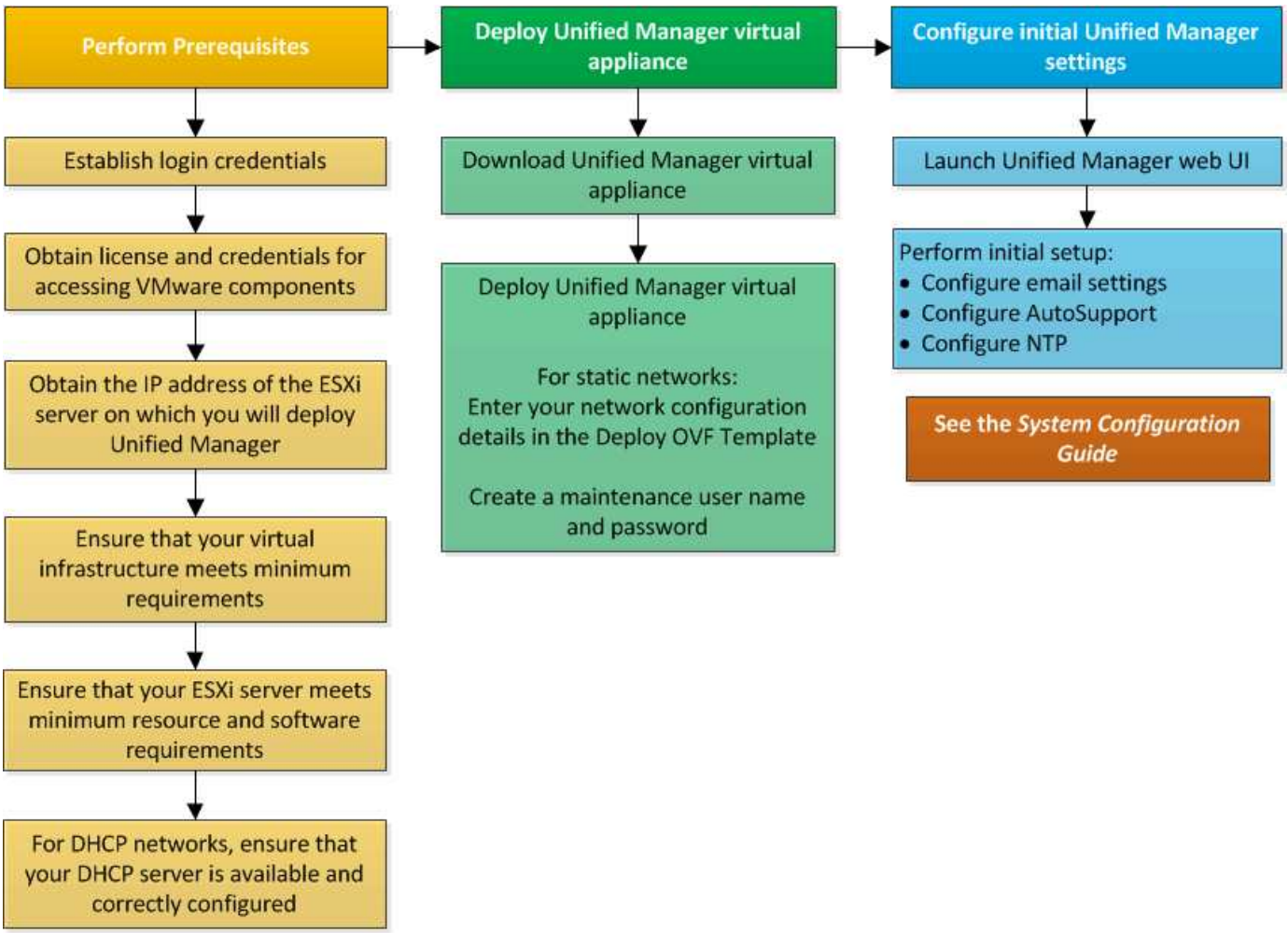
Cluster 1 di N.	Il tuo valore
Password dell'amministratore di ONTAP	
Protocollo	HTTPS

Installazione, aggiornamento e rimozione del software Unified Manager

Sui sistemi VMware vSphere, è possibile installare Unified Manager, eseguire l'aggiornamento a una versione più recente del software o rimuovere l'appliance virtuale Unified Manager (vApp).

Panoramica del processo di implementazione

Il flusso di lavoro di implementazione descrive le attività da eseguire prima di poter utilizzare Unified Manager.



Implementazione di Unified Manager

L'implementazione di Unified Manager include il download del software, l'implementazione dell'appliance virtuale, la creazione di un nome utente e di una password di manutenzione e l'esecuzione della configurazione iniziale nell'interfaccia utente Web.

Cosa ti serve

- Verificare e completare i requisiti di sistema per l'implementazione.

  Vedere "Requisiti di sistema".

- Assicurarsi di disporre delle seguenti informazioni:
  - Credenziali di accesso per il NetApp Support Site
  - Credenziali per l'accesso a VMware vCenter Server e vSphere Web Client
  - Indirizzo IP del server ESXi su cui si sta implementando l'appliance virtuale Unified Manager
  - Dettagli sul data center, ad esempio lo spazio di storage nel datastore e i requisiti di memoria
  - IPv6 deve essere attivato sull'host se si intende utilizzare l'indirizzamento IPv6.

È possibile implementare Unified Manager come appliance virtuale su un server VMware ESXi.

È necessario accedere alla console di manutenzione utilizzando la console VMware e non SSH.

> A partire da Unified Manager 9.8, VMware Tools è stato sostituito con Open VM Tools `open-vm-tools`). Non è più necessario installare VMware Tools come parte dell'installazione perché `open-vm-tools` È incluso nel pacchetto di installazione di Unified Manager.

Al termine dell'implementazione e della configurazione iniziale, è possibile aggiungere cluster o configurare impostazioni di rete aggiuntive nella console di manutenzione e accedere all'interfaccia utente Web.

Fasi

1. Seguire la procedura descritta in "Scarica Unified Manager".
2. Inoltre, seguire la procedura descritta in "Implementare l'appliance virtuale Unified Manager".

Download del file di installazione di Unified Manager

Scarica il file di installazione di Unified Manager dal sito di supporto NetApp per implementare Unified Manager come appliance virtuale.

Cosa ti serve

È necessario disporre delle credenziali di accesso per il NetApp Support Site.

Il file di installazione è un `.tar` che contiene un certificato root, un `README` e un `OVA` File contenente il software Unified Manager configurato per un'appliance virtuale.

Fasi

1. Accedere al NetApp Support Site e accedere alla pagina Download di Unified Manager:

"Sito di supporto NetApp"

2. Selezionare la versione richiesta di Unified Manager e accettare il contratto di licenza con l'utente finale (EULA).
3. Scaricare e salvare `.tar` File per l'installazione di VMware vSphere in una directory locale o di rete accessibile al client vSphere.
4. Verificare il checksum per assicurarsi che il software sia stato scaricato correttamente.
5. Accedere alla directory in cui è stato scaricato `.tar` E immettere il seguente comando nella finestra del terminale per espandere il bundle di Unified Manager:

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

   Il necessario `OVA` file, un certificato root e un `README` I file per Unified Manager vengono decompressi nella directory di destinazione.

6. Verificare l'integrità di `OVA` eseguire la procedura descritta in `README` file.

Implementazione dell'appliance virtuale Unified Manager

Dopo aver scaricato il file di installazione, è possibile implementare Unified Manager come appliance virtuale. Utilizza vSphere Web Client per implementare l'appliance virtuale su un server ESXi. Quando si implementa l'appliance virtuale, viene creata una macchina virtuale.

Cosa ti serve

Esaminare i requisiti di sistema. Apportare le modifiche necessarie prima di implementare l'appliance virtuale Unified Manager.

Vedere "Requisiti dell'infrastruttura virtuale".

Vedere "Software VMware e requisiti di installazione".

Se si utilizza il protocollo DHCP (Dynamic host Configuration Protocol), assicurarsi che il server DHCP sia disponibile e che le configurazioni degli adattatori di rete DHCP e VM (Virtual Machine) siano corrette. DHCP è configurato per impostazione predefinita.

Se si utilizza una configurazione di rete statica, assicurarsi che l'indirizzo IP non sia duplicato nella stessa sottorete e che siano state configurate le voci appropriate del server DNS.

Prima di implementare l'appliance virtuale, ottenere le seguenti informazioni:

- Credenziali per l'accesso a VMware vCenter Server e vSphere Web Client
- Indirizzo IP del server ESXi su cui si sta implementando l'appliance virtuale Unified Manager
- Dettagli sul data center, ad esempio la disponibilità di spazio di storage
- Se non si utilizza DHCP, ottenere gli indirizzi IPv4 o IPv6 per i dispositivi di rete a cui si intende connettersi:
  - FQDN (Fully Qualified Domain Name) dell'host
  - Indirizzo IP dell'host

- Maschera di rete
- Indirizzo IP del gateway predefinito
- Indirizzi DNS primari e secondari
- Cerca domini

A partire da Unified Manager 9.8, VMware Tools è stato sostituito con Open VM Tools (`open-vm-tools`). Non è necessario installare VMware Tools come parte del processo di installazione perché `open-vm-tools` È incluso nel pacchetto di installazione di Unified Manager.

Quando l'appliance virtuale viene implementata, viene generato un certificato autofirmato univoco per l'accesso HTTPS. Quando si accede all'interfaccia utente Web di Unified Manager, potrebbe essere visualizzato un avviso del browser relativo ai certificati non attendibili.

VMware High Availability per l'appliance virtuale Unified Manager è supportata.

Fasi

1. In vSphere Client, fare clic su **file** > **Deploy OVF Template**.
2. Completare la procedura guidata Deploy OVF Template per implementare l'appliance virtuale Unified Manager.

   Nella pagina Review Details (Dettagli revisione):

   - Verificare i dettagli della sezione Publisher. Il messaggio **Entrust Code Signing - OVCS2 (Trusted certificate)** conferma l'integrità del download `OVA` file. + se viene visualizzato il messaggio **Firma codice Entrust - OVCS2 (certificato non valido)**, aggiornare VMware vCenter Server alla versione 7.0U3E o superiore.

     Nella pagina Personalizza modello:

   - Lasciare vuoti tutti i campi quando si utilizza l'indirizzamento DHCP e IPv4.
   - Selezionare la casella "Enable Auto IPv6 Addressing" (attiva indirizzo IPv6 automatico) e lasciare vuoti tutti gli altri campi quando si utilizza l'indirizzamento DHCP e IPv6.
   - Se si desidera utilizzare una configurazione di rete statica, è possibile completare i campi di questa pagina e applicare queste impostazioni durante l'implementazione. Assicurarsi che l'indirizzo IP sia univoco per l'host su cui è distribuito, che non sia già in uso e che disponga di una voce DNS valida.
3. Dopo aver implementato l'appliance virtuale Unified Manager sul server ESXi, accendere la macchina virtuale facendo clic con il pulsante destro del mouse sulla macchina virtuale e selezionando **Power on** (accensione).

   Se l'operazione di accensione non riesce a causa di risorse insufficienti, aggiungere risorse e riprovare l'installazione.

4. Fare clic sulla scheda **Console**.

   Il processo di avvio iniziale richiede alcuni minuti.

5. Per configurare il fuso orario, immettere la propria area geografica e la propria città o regione come richiesto nella finestra di VM Console.

   Tutte le informazioni relative alla data visualizzate utilizzano il fuso orario configurato per Unified Manager, indipendentemente dall'impostazione del fuso orario sui dispositivi gestiti. Se i sistemi storage e il server di

gestione sono configurati con lo stesso server NTP, si riferiscono allo stesso istante in tempo, anche se appaiono in modo diverso. Ad esempio, se si crea una copia Snapshot utilizzando un dispositivo configurato utilizzando un fuso orario diverso da quello del server di gestione, l'indicatore orario corrisponde all'ora del server di gestione.

6. Se non sono disponibili servizi DHCP o se si verifica un errore nei dettagli della configurazione di rete statica, selezionare una delle seguenti opzioni:

Se si utilizza…	**Quindi…**
DHCP	Selezionare **Riprova DHCP**. Se si intende utilizzare DHCP, assicurarsi che sia configurato correttamente. Se si utilizza una rete abilitata per DHCP, le voci FQDN e server DNS vengono fornite automaticamente all'appliance virtuale. Se DHCP non è configurato correttamente con DNS, il nome host "UnifiedManager" viene assegnato automaticamente e associato al certificato di protezione. Se non è stata configurata una rete abilitata DHCP, inserire manualmente le informazioni di configurazione della rete.
Una configurazione di rete statica	a. Selezionare **inserire i dettagli della configurazione di rete statica**. Il completamento del processo di configurazione richiede alcuni minuti. b. Confermare i valori immessi e selezionare **Y**.

7. Quando richiesto, immettere un nome utente per la manutenzione, quindi fare clic su **Invio**.

   Il nome utente per la manutenzione deve iniziare con una lettera da a-z, seguita da una combinazione di -, a-z o 0-9.

8. Quando richiesto, immettere una password, quindi fare clic su **Invio**.

   La console VM visualizza l'URL dell'interfaccia utente Web di Unified Manager.

È possibile accedere all'interfaccia utente Web per eseguire la configurazione iniziale di Unified Manager, come descritto in "Configurazione di Active IQ Unified Manager".

Aggiornamento di Unified Manager

È possibile aggiornare Active IQ Unified Manager alla versione 9.12 solo dalla versione 9.10 o 9.11.

Durante il processo di aggiornamento, Unified Manager non è disponibile. Prima di eseguire l'aggiornamento di Unified Manager, è necessario completare tutte le operazioni in esecuzione.

Se Unified Manager è associato a un'istanza di OnCommand Workflow Automation e sono disponibili nuove

versioni del software per entrambi i prodotti, è necessario scollegare i due prodotti e impostare una nuova connessione per l'automazione del flusso di lavoro dopo aver eseguito gli aggiornamenti. Se si esegue un aggiornamento a uno solo dei prodotti, dopo l'aggiornamento è necessario accedere a Workflow Automation e verificare che stia ancora acquisendo dati da Unified Manager.

Fasi

1. Seguire la procedura descritta in "Scarica l'immagine ISO di Unified Manager".
2. Inoltre, seguire la procedura descritta in "Aggiorna Unified Manager".

Percorso di aggiornamento supportato per le versioni di Unified Manager

Active IQ Unified Manager supporta un percorso di aggiornamento specifico per ciascuna versione.

Non tutte le versioni di Unified Manager possono eseguire un aggiornamento in-place alle versioni successive. Gli aggiornamenti di Unified Manager sono limitati a un modello N-2, il che significa che un aggiornamento può essere eseguito solo nelle 2 release successive su tutte le piattaforme. Ad esempio, è possibile eseguire un aggiornamento a Unified Manager 9.12 solo da Unified Manager 9.10 e 9.11.

Se si utilizza una versione precedente a quella supportata, l'istanza di Unified Manager deve essere prima aggiornata a una delle versioni supportate, quindi aggiornata alla versione corrente.

Ad esempio, se la versione installata è OnCommand 9.5 e si desidera eseguire l'aggiornamento alla versione più recente di Active IQ Unified Manager 9.12, seguire una sequenza di aggiornamenti.

Esempio di percorso di aggiornamento:

1. Upgrade di OnCommand Unified Manager 9.5 → Active IQ Unified Manager 9.7.
2. Aggiornamento 9.7 → 9.9.
3. Aggiornamento 9.9 → 9.11.
4. Aggiornamento 9.11 → 9.12.

Per ulteriori informazioni sulla matrice dei percorsi di aggiornamento, vedere questa sezione "Articolo della Knowledge base (KB)".

Download del file di aggiornamento di Unified Manager

Prima di aggiornare Unified Manager, scaricare il file di aggiornamento di Unified Manager dal NetApp Support Site.

Cosa ti serve

È necessario disporre delle credenziali di accesso per il NetApp Support Site.

Fasi

1. Accedi al sito di supporto NetApp:

   "Sito di supporto NetApp"

2. Accedere alla pagina Download per aggiornare Unified Manager su VMware vSphere.
3. Scaricare il `.iso` Immagine per l'aggiornamento e salvarla in una directory locale o di rete accessibile al client vSphere.

4. Verificare il checksum per assicurarsi che il software sia stato scaricato correttamente.

Aggiornamento dell'appliance virtuale di Unified Manager

È possibile aggiornare l'appliance virtuale Active IQ Unified Manager dalle release 9.10 o 9.11 alla 9.12.

Cosa ti serve

Verificare quanto segue:

- Il file di aggiornamento, l'immagine ISO, è stato scaricato dal NetApp Support Site.
- Il sistema su cui si esegue l'aggiornamento di Unified Manager soddisfa i requisiti di sistema e software.

  Vedere "Requisiti dell'infrastruttura virtuale".

  Vedere "Software VMware e requisiti di installazione".

- Per gli utenti di vSphere 6.5 e versioni successive, è stata installata VMware Remote Console (VMRC).
- Durante l'aggiornamento, potrebbe essere richiesto di confermare se si desidera mantenere le impostazioni predefinite precedenti per la conservazione dei dati sulle prestazioni per 13 mesi o se si desidera modificarli in 6 mesi. Dopo la conferma, i dati storici delle performance vengono eliminati dopo 6 mesi.
- Si dispone delle seguenti informazioni:
  - Credenziali di accesso per il NetApp Support Site
  - Credenziali per l'accesso a VMware vCenter Server e vSphere Web Client
  - Credenziali per l'utente di manutenzione di Unified Manager

Durante il processo di aggiornamento, Unified Manager non è disponibile. Prima di eseguire l'aggiornamento di Unified Manager, è necessario completare tutte le operazioni in esecuzione.

Se si dispone di Workflow Automation e Unified Manager associati, aggiornare manualmente il nome host in Workflow Automation.

Fasi

1. In vSphere Client, fare clic su **Home** > **Inventory** > **VM e modelli**.
2. Selezionare la macchina virtuale (VM) su cui è installata l'appliance virtuale Unified Manager.
3. Se la macchina virtuale di Unified Manager è in esecuzione, accedere a **Riepilogo** > **comandi** > **Chiudi sessione ospite**.
4. Creare una copia di backup, ad esempio uno snapshot o un clone, della macchina virtuale di Unified Manager per creare un backup coerente con l'applicazione.
5. Dal client vSphere, accendere Unified Manager VM.
6. Avviare VMware Remote Console.
7. Fare clic sull'icona **CDROM** e selezionare **Connect to Disk Image file (.iso)**.
8. Selezionare `ActiveIQUnifiedManager-<version>-virtual-update.iso` E fare clic su **Apri**.
9. Fare clic sulla scheda **Console**.
10. Accedere alla console di manutenzione di Unified Manager.

11. Nel menu principale, selezionare **Upgrade**.

    Viene visualizzato un messaggio che indica che Unified Manager non è disponibile durante il processo di aggiornamento e che deve riprendere dopo il completamento.

12. Tipo `y` per continuare.

    Viene visualizzato un avviso che ricorda di eseguire il backup della macchina virtuale su cui risiede l'appliance virtuale.

13. Tipo `y` per continuare.

    Il processo di aggiornamento e il riavvio dei servizi di Unified Manager possono richiedere alcuni minuti.

14. Premere un tasto qualsiasi per continuare.

    L'utente viene disconnesso automaticamente dalla console di manutenzione.

15. **Opzionale:** accedere alla console di manutenzione e verificare la versione di Unified Manager.

È possibile avviare l'interfaccia utente Web in una nuova finestra di un browser Web supportato ed effettuare l'accesso per utilizzare la versione aggiornata di Unified Manager. Tenere presente che è necessario attendere il completamento del processo di rilevamento prima di eseguire qualsiasi attività nell'interfaccia utente.

Riavvio della macchina virtuale di Unified Manager

È possibile riavviare la macchina virtuale (VM) di Unified Manager dalla console di manutenzione. Riavviare la macchina virtuale dopo aver generato un nuovo certificato di protezione o in caso di problemi con la macchina virtuale.

Cosa ti serve

- L'appliance virtuale deve essere accesa.
- L'utente deve essere connesso alla console di manutenzione di Unified Manager come utente di manutenzione.

È inoltre possibile riavviare la macchina virtuale da vSphere utilizzando l'opzione VMware **Restart Guest**.

Fasi

1. Nella console di manutenzione, selezionare **Configurazione del sistema** > **riavvio della macchina virtuale**.
2. Avviare l'interfaccia utente Web di Unified Manager dal browser ed effettuare l'accesso.

Informazioni correlate

"Guida ai cmdlet di VMware vSphere PowerCLI: Restart-VMGuest"

Rimozione di Unified Manager

È possibile disinstallare Unified Manager rimuovendo la macchina virtuale (VM) su cui è installato il software Unified Manager.

Cosa ti serve

- È necessario disporre delle credenziali per l'accesso a VMware vCenter Server e vSphere Web Client.
- Tutte le connessioni attive del server Unified Manager a un server Workflow Automation devono essere chiuse.
- Tutti i cluster (origini dati) devono essere rimossi dal server Unified Manager prima di rimuovere la macchina virtuale (VM).

Fasi

1. Utilizzare la console di manutenzione di Unified Manager per verificare che il server Unified Manager non disponga di una connessione attiva a un provider di dati esterno.
2. In vSphere Client, fare clic su **Home** > **Inventory** > **VM e modelli**.
3. Selezionare la macchina virtuale che si desidera rimuovere e fare clic sulla scheda **Summary** (Riepilogo).
4. Se la macchina virtuale è in esecuzione, fare clic su **alimentazione** > **Arresta il sistema ospite**.
5. Fare clic con il pulsante destro del mouse sulla macchina virtuale che si desidera rimuovere, quindi fare clic su **Delete from Disk** (Elimina dal disco).

Installare Unified Manager su sistemi Linux

Introduzione a Active IQ Unified Manager

Active IQ Unified Manager (in precedenza Unified Manager di OnCommand) consente di monitorare e gestire lo stato di salute e le performance dei sistemi storage ONTAP da una singola interfaccia. È possibile implementare Unified Manager su un server Linux, su un server Windows o come appliance virtuale (vApp) su un host VMware.

Una volta completata l'installazione e aggiunti i cluster che si desidera gestire, Unified Manager fornisce un'interfaccia grafica che visualizza lo stato di capacità, disponibilità, protezione e performance dei sistemi storage monitorati.

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Funzioni del server Unified Manager

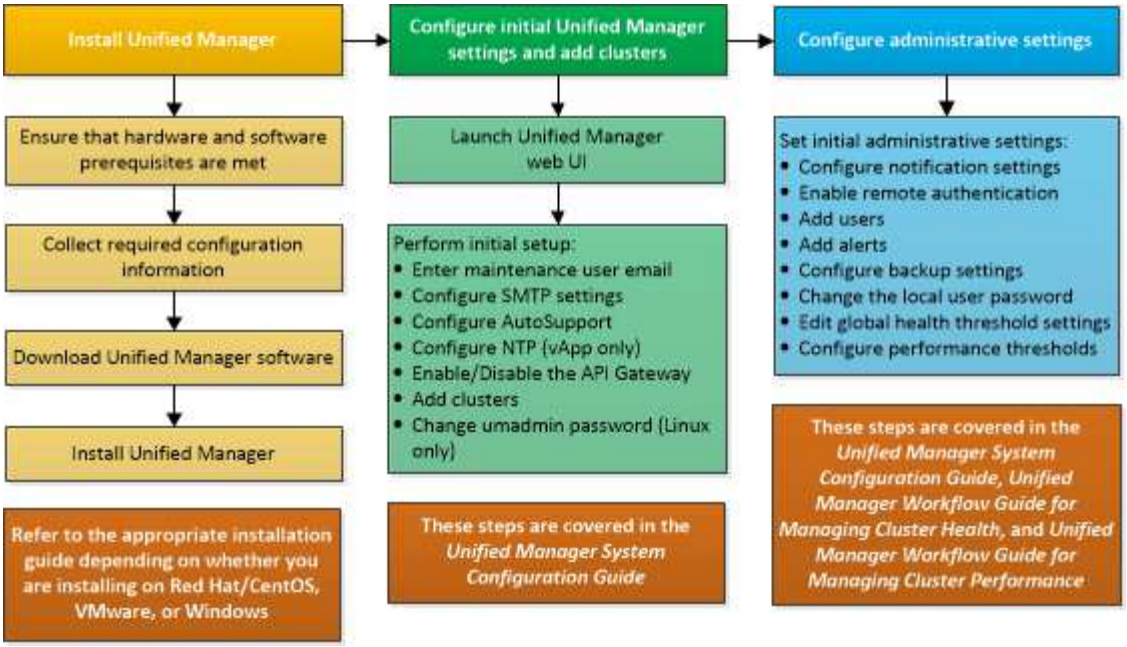
L'infrastruttura server di Unified Manager è costituita da un'unità di raccolta dati, un database e un server applicazioni. Fornisce servizi di infrastruttura come rilevamento, monitoraggio, RBAC (role-based access control), audit e logging.

Unified Manager raccoglie le informazioni sul cluster, memorizza i dati nel database e li analizza per verificare l'eventuale presenza di problemi nel cluster.

Panoramica della sequenza di installazione

Il flusso di lavoro di installazione descrive le attività da eseguire prima di poter utilizzare Unified Manager.

Queste sezioni descrivono ciascuno degli elementi mostrati nel flusso di lavoro seguente.



Requisiti per l'installazione di Unified Manager

Prima di iniziare il processo di installazione, assicurarsi che il server su cui si desidera installare Unified Manager soddisfi i requisiti specifici di software, hardware, CPU e memoria.

NetApp non supporta alcuna modifica del codice applicativo di Unified Manager. Se è necessario applicare misure di sicurezza al server Unified Manager, è necessario apportare tali modifiche al sistema operativo su cui è installato Unified Manager.

Per ulteriori informazioni sull'applicazione delle misure di sicurezza al server Unified Manager, consultare l'articolo della Knowledge base.

"Supporto per le misure di sicurezza applicate a Active IQ Unified Manager per Clustered Data ONTAP"

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Infrastruttura virtuale e requisiti di sistema hardware

L'installazione di Unified Manager su un'infrastruttura virtuale o su un sistema fisico deve soddisfare i requisiti minimi di memoria, CPU e spazio su disco.

La seguente tabella mostra i valori consigliati per le risorse di memoria, CPU e spazio su disco. Questi valori sono stati qualificati in modo che Unified Manager soddisfi livelli di performance accettabili.

Configurazione dell'hardware	Impostazioni consigliate
RAM	12 GB (requisito minimo 8 GB)
Processori	4 CPU

Configurazione dell'hardware	Impostazioni consigliate
Capacità del ciclo della CPU	9572 MHz totali (requisito minimo 9572 MHz)
Spazio libero su disco	150 GB, dove la capacità viene allocata come segue: • 50 GB assegnati alla partizione root • 100 GB di spazio libero su disco assegnato a `/opt/netapp/data` Directory, montata su un disco LVM o su un disco locale separato collegato al sistema di destinazione Per montaggio separato `/opt` e. `/var/log` directory, assicurarsi che `/opt` Ha 15 GB e. `/var/log` Dispone di 16 GB di spazio libero. Il `/tmp` La directory deve disporre di almeno 10 GB di spazio libero.

Unified Manager può essere installato su sistemi con una piccola quantità di memoria, ma i 12 GB di RAM consigliati garantiscono che sia disponibile una quantità di memoria sufficiente per ottenere performance ottimali e che il sistema possa ospitare cluster e oggetti di storage aggiuntivi con la crescita della configurazione. Non è necessario impostare limiti di memoria sulla macchina virtuale in cui è implementato Unified Manager e non attivare alcuna funzione (ad esempio, la bollatura) che impedisca al software di utilizzare la memoria allocata nel sistema.

Inoltre, esiste un limite al numero di nodi che una singola istanza di Unified Manager può monitorare prima di installare una seconda istanza di Unified Manager. Per ulteriori informazioni, consulta la *Guida alle Best Practice*.

"Report tecnico 4621: Guida alle Best practice di Unified Manager"

Lo swapping della pagina di memoria influisce negativamente sulle prestazioni del sistema e dell'applicazione di gestione. La concorrenza per le risorse CPU non disponibili a causa dell'utilizzo complessivo dell'host può compromettere le prestazioni.

Requisito per l'utilizzo dedicato

Il sistema fisico o virtuale su cui si installa Unified Manager deve essere utilizzato esclusivamente per Unified Manager e non deve essere condiviso con altre applicazioni. Altre applicazioni potrebbero consumare risorse di sistema e ridurre drasticamente le performance di Unified Manager.

Requisiti di spazio per i backup

Se si intende utilizzare la funzione di backup e ripristino di Unified Manager, allocare ulteriore capacità in modo che la directory o il disco "data" disponga di 150 GB di spazio. Un backup può essere scritto in una destinazione locale o remota. La procedura consigliata consiste nell'identificare una postazione remota esterna al sistema host di Unified Manager che abbia almeno 150 GB di spazio.

Requisiti per la connettività host

Il sistema fisico o virtuale su cui si installa Unified Manager deve essere configurato in modo da poter essere

correttamente configurato `ping` il nome host dell'host stesso. In caso di configurazione IPv6, è necessario verificarlo `ping6` Al nome host per garantire che l'installazione di Unified Manager abbia esito positivo.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web del prodotto. Se è stato configurato un indirizzo IP statico per la rete durante l'implementazione, è stato designato un nome per l'host di rete. Se la rete è stata configurata utilizzando DHCP, è necessario ottenere il nome host dal DNS.

Se si prevede di consentire agli utenti di accedere a Unified Manager utilizzando il nome breve invece di utilizzare il nome di dominio completo (FQDN) o l'indirizzo IP, la configurazione di rete deve risolvere questo nome breve in un FQDN valido.

Software Linux e requisiti di installazione

Il sistema Linux su cui si installa Unified Manager richiede versioni specifiche del sistema operativo e del software di supporto.

Software del sistema operativo

Il sistema Linux deve disporre delle seguenti versioni del sistema operativo e del software di supporto installati:

- Red Hat Enterprise Linux versioni 7.x e dalla 8.0 alla 8.6, basato sull'architettura x86_64.
- CentOS versione 7.x basato sull'architettura x86_64. CentOS Stream non è supportato.

Consulta la matrice di interoperabilità per l'elenco completo e aggiornato delle versioni supportate di Red Hat Enterprise Linux e CentOS.

"mysupport.netapp.com/matrix"

Software di terze parti

Unified Manager viene implementato su un server Web WildFly. WildFly 19.0.0 viene fornito in bundle e configurato con Unified Manager.

I seguenti pacchetti di terze parti sono richiesti, ma non sono inclusi in Unified Manager. Questi pacchetti vengono installati automaticamente da `yum` programma di installazione durante l'installazione, a condizione che i repository siano stati configurati come indicato nelle seguenti sezioni.

- MySQL Community Edition versione 8.0.30 (dal repository MySQL).
- OpenJDK versione 11.0.17 (dal repository Red Hat Extra Enterprise Linux Server)
- Python 3.6.x
- P7zip versione 16.02 o successiva (dal repository Red Hat Extra Packages per Enterprise Linux)

> Prima di aggiornare qualsiasi software di terze parti, è necessario chiudere un'istanza di Unified Manager in esecuzione. Una volta completata l'installazione del software di terze parti, è possibile riavviare Unified Manager.

Requisiti di autorizzazione dell'utente

L'installazione di Unified Manager su un sistema Linux può essere eseguita dall'utente root o da utenti non root utilizzando `sudo` comando.

Requisiti di installazione

Di seguito sono elencate le Best practice per l'installazione di Red Hat Enterprise Linux o CentOS e dei repository associati al sistema. I sistemi installati o configurati in modo diverso o implementati fuori sede (nel cloud) potrebbero richiedere ulteriori passaggi e Unified Manager potrebbe non funzionare correttamente in tali implementazioni.

- È necessario installare Red Hat Enterprise Linux o CentOS in base alle Best practice di Red Hat e selezionare le seguenti opzioni predefinite, che richiedono la selezione dell'ambiente di base "Sserver with GUI".
- Durante l'installazione di Unified Manager su Red Hat Enterprise Linux o CentOS, il sistema deve avere accesso al repository appropriato in modo che il programma di installazione possa accedere e installare tutte le dipendenze software richieste.
- Per `yum` Installer per trovare il software dipendente nei repository Red Hat Enterprise Linux, devi aver registrato il sistema durante l'installazione di Red Hat Enterprise Linux o in seguito utilizzando un abbonamento Red Hat valido.

  Per informazioni su Red Hat Subscription Manager, consulta la documentazione di Red Hat.

- È necessario abilitare il repository Extra Packages for Enterprise Linux (EPEL) per installare correttamente le utility di terze parti richieste nel sistema.

  Se il repository EPEL non è configurato sul sistema, è necessario scaricare e configurare manualmente il repository.

  Vedere "Configurazione manuale del repository EPEL".

- Se la versione corretta di MySQL non è installata, devi abilitare il repository MySQL per installare correttamente il software MySQL sul tuo sistema.

  Se il repository MySQL non è configurato sul sistema, è necessario scaricare e configurare manualmente il repository.

  Vedere "Configurazione manuale del repository MySQL".

Se il sistema non dispone di accesso a Internet e i repository non vengono mirrorati da un sistema connesso a Internet al sistema non connesso, seguire le istruzioni di installazione per determinare le dipendenze software esterne del sistema. Quindi, è possibile scaricare il software richiesto sul sistema connesso a Internet e copiare `.rpm` Al sistema su cui si intende installare Unified Manager. Per scaricare gli artefatti e i pacchetti, è necessario utilizzare `yum install` comando. È necessario assicurarsi che i due sistemi eseguano la stessa versione del sistema operativo e che la licenza di abbonamento sia per la versione appropriata di Red Hat Enterprise Linux o CentOS.

> Non è necessario installare il software di terze parti richiesto da repository diversi da quelli elencati qui. Il software installato dai repository Red Hat è progettato esplicitamente per Red Hat Enterprise Linux e conforme alle Best practice Red Hat (layout di directory, permessi e così via). Il software di altre sedi potrebbe non seguire queste linee guida, il che potrebbe causare un errore nell'installazione di Unified Manager o problemi con aggiornamenti futuri.

Requisito della porta 443

Le immagini generiche di Red Hat Enterprise Linux e CentOS potrebbero bloccare l'accesso esterno alla porta 443. A causa di questa restrizione, potrebbe non essere possibile connettersi all'interfaccia utente Web

dell'amministratore dopo l'installazione di Unified Manager. L'esecuzione del seguente comando consente l'accesso alla porta 443 per tutti gli utenti esterni e le applicazioni su un sistema generico Red Hat Enterprise Linux o CentOS.

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

È necessario installare Red Hat Enterprise Linux e CentOS con l'ambiente di base "Server with GUI". Fornisce i comandi utilizzati dalle istruzioni di installazione di Unified Manager. Altri ambienti di base potrebbero richiedere l'installazione di comandi aggiuntivi per validare o completare l'installazione. Se il `firewall-cmd` non è disponibile nel sistema, è necessario installarlo eseguendo il seguente comando:

```
# sudo yum install firewalld
```

Prima di eseguire i comandi, contattare il reparto IT per verificare se le policy di sicurezza richiedono una procedura diversa.

> Il THP (transparent enorme Pages) deve essere disattivato sui sistemi CentOS e Red Hat. Se attivata, in alcuni casi può causare l'arresto di Unified Manager quando alcuni processi consumano una quantità eccessiva di memoria e vengono terminati.

Browser supportati

Per accedere all'interfaccia utente Web di Unified Manager, utilizzare un browser supportato.

La matrice di interoperabilità contiene l'elenco delle versioni del browser supportate.

"mysupport.netapp.com/matrix"

Per tutti i browser, la disattivazione dei blocchi dei pop-up garantisce la corretta visualizzazione delle funzionalità software.

Se si intende configurare Unified Manager per l'autenticazione SAML, in modo che un provider di identità (IdP) possa autenticare gli utenti, è necessario controllare anche l'elenco dei browser supportati da IdP.

Requisiti di protocollo e porta

Le porte e i protocolli richiesti consentono la comunicazione tra il server Unified Manager e i sistemi di storage gestiti, i server e altri componenti.

Connessioni al server Unified Manager

Nelle installazioni tipiche non è necessario specificare i numeri di porta durante la connessione all'interfaccia utente Web di Unified Manager, poiché vengono sempre utilizzate le porte predefinite. Ad esempio, poiché Unified Manager tenta sempre di essere eseguito sulla porta predefinita, è possibile immettere `https://<host>` invece di `https://<host>:443`.

Il server Unified Manager utilizza protocolli specifici per accedere alle seguenti interfacce:

Interfaccia	Protocollo	Porta	Descrizione
UI Web di Unified Manager	HTTP	80	Utilizzato per accedere all'interfaccia utente Web di Unified Manager; reindirizza automaticamente alla porta sicura 443.
L'interfaccia utente Web di Unified Manager e i programmi che utilizzano API	HTTPS	443	Utilizzato per accedere in modo sicuro all'interfaccia utente Web di Unified Manager o per effettuare chiamate API; le chiamate API possono essere effettuate solo utilizzando HTTPS.
Console di manutenzione	SSH/SFTP	22	Utilizzato per accedere alla console di manutenzione e recuperare i pacchetti di supporto.
Riga di comando Linux	SSH/SFTP	22	Utilizzato per accedere alla riga di comando di Red Hat Enterprise Linux o CentOS e recuperare i bundle di supporto.
Database MySQL	MySQL	3306	Utilizzato per abilitare l'accesso ai servizi API OnCommand Workflow Automation e OnCommand a Unified Manager.
Syslog	UDP	514	Utilizzato per accedere ai messaggi EMS basati su abbonamento dai sistemi ONTAP e per creare eventi in base ai messaggi.
RIPOSO	HTTPS	9443	Utilizzato per accedere agli eventi EMS basati su API REST in tempo reale da sistemi ONTAP autenticati.

La porta predefinita per MySQL, 3306, è limitata solo all'host locale durante l'installazione di Unified Manager su sistemi Linux. Questo non influisce su nessuno scenario di aggiornamento, in cui viene mantenuta la configurazione precedente. Questa configurazione può essere modificata e la connessione può essere resa disponibile ad altri host utilizzando `Control access to MySQL port 3306` sulla console di manutenzione. Per ulteriori informazioni, vedere "Opzioni di menu aggiuntive". Le porte utilizzate per le comunicazioni HTTP e HTTPS (porte 80 e 443) possono essere modificate utilizzando la console di manutenzione di Unified Manager. Per ulteriori informazioni, vedere "Menu della console di manutenzione".

Connessioni dal server Unified Manager

È necessario configurare il firewall in modo che apra le porte che consentono la comunicazione tra il server Unified Manager e i sistemi di storage gestiti, i server e altri componenti. Se una porta non è aperta, la comunicazione non riesce.

A seconda dell'ambiente in uso, è possibile scegliere di modificare le porte e i protocolli utilizzati dal server Unified Manager per connettersi a destinazioni specifiche.

Il server Unified Manager si connette utilizzando i seguenti protocolli e porte ai sistemi di storage gestiti, ai server e ad altri componenti:

Destinazione	Protocollo	Porta	Descrizione
Sistema storage	HTTPS	443/TCP	Utilizzato per monitorare e gestire i sistemi storage.
Sistema storage	NDMP	10000/TCP	Utilizzato per alcune operazioni di ripristino Snapshot.
Server AutoSupport	HTTPS	443	Utilizzato per inviare informazioni AutoSupport. Per eseguire questa funzione, è necessario disporre dell'accesso a Internet.
Server di autenticazione	LDAP	389	Utilizzato per effettuare richieste di autenticazione e richieste di ricerca di utenti e gruppi.
LDAPS	636	Utilizzato per comunicazioni LDAP sicure.	Server di posta
SMTP	25	Utilizzato per inviare e-mail di notifica degli avvisi.	Mittente trap SNMP

Destinazione	Protocollo	Porta	Descrizione
SNMPv1 o SNMPv3	162/UDP	Utilizzato per inviare messaggi trap SNMP di notifica degli avvisi.	Server del provider di dati esterno
TCP	2003	Utilizzato per inviare dati sulle prestazioni a un provider di dati esterno, ad esempio Graphite.	Server NTP

Completamento del foglio di lavoro

Prima di installare e configurare Unified Manager, è necessario disporre di informazioni specifiche sull'ambiente in uso. È possibile registrare le informazioni nel foglio di lavoro.

Informazioni sull'installazione di Unified Manager

I dettagli necessari per installare Unified Manager.

Sistema su cui viene implementato il software	Il tuo valore
Nome di dominio completo dell'host	
Host IP address (Indirizzo IP host)	
Maschera di rete	
Indirizzo IP del gateway	
Indirizzo DNS primario	
Indirizzo DNS secondario	
Cerca domini	
Nome utente manutenzione	
Password utente per la manutenzione	

Informazioni sulla configurazione di Unified Manager

I dettagli per configurare Unified Manager dopo l'installazione. Alcuni valori sono facoltativi a seconda della configurazione.

Impostazione	Il tuo valore
Indirizzo e-mail utente manutenzione	
Nome host o indirizzo IP del server SMTP	
Nome utente SMTP	
Password SMTP	
Porta SMTP	25 (valore predefinito)
E-mail da cui vengono inviate le notifiche di avviso	
Nome host o indirizzo IP del server di autenticazione	
Nome dell'amministratore di Active Directory o nome distinto del binding LDAP	
Password di Active Directory o bind LDAP	
Nome distinto della base del server di autenticazione	
URL del provider di identità (IdP)	
Metadati del provider di identità (IdP)	
Indirizzi IP host di destinazione del trap SNMP	
Porta SNMP	

Informazioni sul cluster

I dettagli dei sistemi storage gestiti con Unified Manager.

Cluster 1 di N.	Il tuo valore
Nome host o indirizzo IP di gestione del cluster	
Nome utente amministratore di ONTAP All'amministratore deve essere stato assegnato il ruolo "admin".	
Password dell'amministratore di ONTAP	

Cluster 1 di N.	Il tuo valore
Protocollo	HTTPS

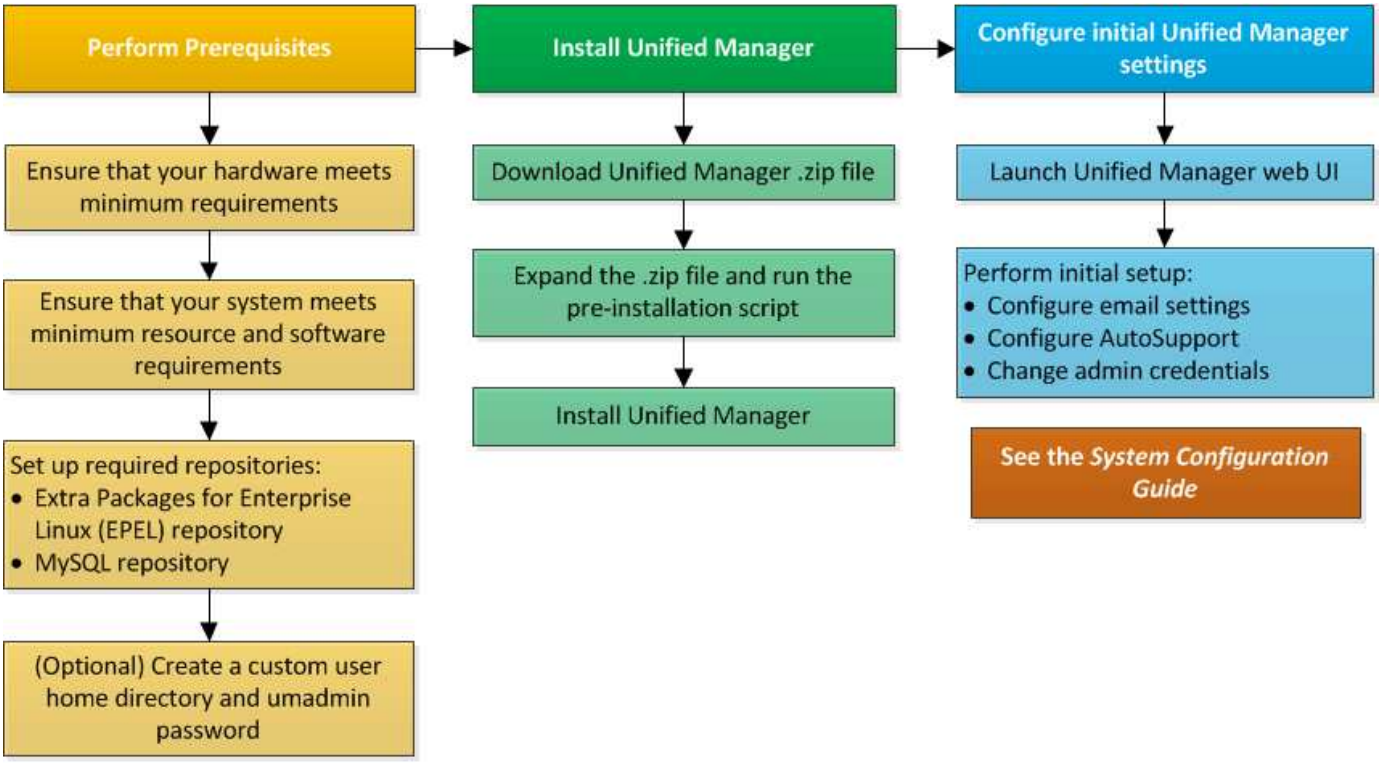
Installazione, aggiornamento e rimozione del software Unified Manager

Sui sistemi Linux, è possibile installare il software Unified Manager, eseguire l'aggiornamento a una versione più recente del software o rimuovere Unified Manager.

Unified Manager può essere installato sui server Red Hat Enterprise Linux o CentOS. Il server Linux su cui si installa Unified Manager può essere eseguito su una macchina fisica o su una macchina virtuale in esecuzione su VMware ESXi, Microsoft Hyper-V o Citrix XenServer.

Panoramica del processo di installazione

Il flusso di lavoro di installazione descrive le attività da eseguire prima di poter utilizzare Unified Manager.



Configurazione dei repository software richiesti

Il sistema deve avere accesso a determinati repository in modo che il programma di installazione possa accedere e installare tutte le dipendenze software richieste.

Configurazione manuale del repository EPEL

Se il sistema su cui si installa Unified Manager non ha accesso al repository Extra

Packages for Enterprise Linux (EPEL), è necessario scaricare e configurare manualmente il repository per una corretta installazione.

Il repository EPEL fornisce l'accesso alle utility di terze parti necessarie che devono essere installate nel sistema. Utilizzate il repository EPEL sia che stiate installando Unified Manager su un sistema Red Hat Enterprise Linux o CentOS.

Fasi

1. Scarica il repository EPEL per la tua installazione. Per Red Hat Enterprise Linux 7, scaricalo da:

   ```
   wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
   ```

   Per la versione 8, scaricarla da:

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

2. Configurare il repository EPEL:

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

Per i sistemi Red Hat Enterprise Linux 8, se si dispone di repository interni con pacchetti RPM modulari, ad esempio *`javapackages-filesystem-<version>.module.rpm`*, assicurarsi che i metadati per i pacchetti modulari siano disponibili anche nello stesso repository.

Configurazione manuale del repository MySQL

Se il sistema su cui si installa Unified Manager non ha accesso al repository MySQL Community Edition, è necessario scaricare e configurare manualmente il repository per una corretta installazione.

Il repository MySQL fornisce l'accesso al software MySQL richiesto che deve essere installato sul sistema.

> Questa attività potrebbe non riuscire se il sistema non dispone della connettività Internet. Se il sistema su cui si installa Unified Manager non dispone dell'accesso a Internet, consultare la documentazione di MySQL.

Fasi

1. Scarica il repository MySQL appropriato per la tua installazione. Per Red Hat Enterprise Linux 7, scaricalo da:

   ```
   wget http://repo.mysql.com/yum/mysql-8.0-community/el/7/x86_64/mysql80-
   community-release-el7-3.noarch.rpm
   ```

   Per la versione 8, scaricarla da:

   ```
   wget http://repo.mysql.com/yum/mysql-8.0-community/el/8/x86_64/mysql80-
   community-release-el8-1.noarch.rpm
   ```

2. Configurare il repository MySQL:

   ```
   yum install mysql80-community-release-<version>.noarch.rpm
   ```

Per il sistema Red Hat Enterprise Linux 8, se si dispone di repository interni con java-11-openjdk, p7zip e altri pacchetti software forniti dal repository AppStream, è necessario disattivare il repository AppStream e installare MySQL Community Server. Eseguire il seguente comando:

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

Se viene visualizzato un errore relativo alla mancata corrispondenza della chiave o della chiave e l'installazione non riesce, attenersi alla seguente procedura:

- Su un sistema connesso, importare la chiave MySQL aggiornata eseguendo il seguente comando:

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

for example:

rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022
```

- Su un sistema che non dispone di connessione a Internet, aggiorna il file MySQL repo e disattiva `gpgcheck` mediante marcatura `gpgcheck=0`.

Requisiti SELinux sulle condivisioni NFS e CIFS

Se si prevede di montare `/opt/netapp` oppure `/opt/netapp/data` Su un dispositivo NAS o SAN e se SELinux è abilitato, è necessario tenere presente alcune considerazioni.

Se si prevede di montare `/opt/netapp` oppure `/opt/netapp/data` Da qualsiasi punto diverso dal file system root e se SELinux è abilitato nel proprio ambiente, si dovrebbe impostare il contesto corretto per le directory montate. Per lo scenario applicabile nell'ambiente in uso, seguire questa procedura per impostare e confermare il contesto SELinux corretto.

Configurazione del contesto SELinux quando `/opt/netapp/data` è montato

Se è stato montato `/opt/netapp/data` Nel sistema e SELinux è impostato su `Enforcing`, Assicurarsi che il tipo di contesto SELinux per `/opt/netapp/data` è impostato su `mysqld_db_t`, che è l'elemento di contesto predefinito per la posizione dei file di database.

1. Eseguire questo comando per verificare il contesto:

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

   Un output di esempio:

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

In questo output, il contesto è `default_t`. Impostare questo contesto su `mysqld_db_t`.

2. Eseguire questa procedura per impostare il contesto in base al modo in cui è stato montato `/opt/netapp/data`.
   a. Eseguire i seguenti comandi per impostare il contesto su `mysqld_db_t`:
   `semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"`
   `` `restorecon -R -v /opt/netapp/data ``
   b. Se è stato configurato `/opt/netapp/data` poll `/etc/fstab`, è necessario modificare `/etc/fstab` file. Per `/opt/netapp/data/` Montare l'opzione, aggiungere l'etichetta MySQL come:

      `context=system_u:object_r:mysqld_db_t:s0`

   c. Smontare e rimontare `/opt/netapp/data/` per abilitare il contesto.
   d. Se si dispone di un mount NFS diretto, eseguire il seguente comando per impostare il contesto su `mysqld_db_t`:

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

3. Verificare che il contesto sia impostato correttamente:

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

Un output di esempio:

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

Configurazione del contesto SELinux quando `/opt/netapp` sia montato, e. `/opt/netapp/data/` è montato anche separatamente

In questo scenario, in un primo momento, è necessario impostare il contesto per `/opt/netapp/data/` come descritto nella sezione precedente. Dopo aver impostato il contesto corretto per `/opt/netapp/data/`, assicurarsi che la directory principale `/opt/netapp` Il contesto SELinux non è impostato su `file_t`.

Fasi

1. Eseguire questo comando per verificare il contesto:

   `ls -dZ /opt/netapp`

   Un output di esempio:

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

   In questo output, il contesto è `file_t` deve essere modificato. I seguenti comandi impostano il contesto su `usr_t`. È possibile impostare il contesto su un valore diverso da `file_t` in base ai tuoi requisiti di sicurezza.

2. Eseguire questa procedura per impostare il contesto, in base al modo in cui è stato montato `/opt/netapp`.
   a. Eseguire i seguenti comandi per impostare il contesto:

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

1. Se è stato configurato `/opt/netapp` poll `/etc/fstab`, è necessario modificare `/etc/fstab` file. Per `/opt/netapp` Montare l'opzione, aggiungere l'etichetta MySQL come:

   `context=system_u:object_r:usr_t:s0`

2. Smontare e montare nuovamente `/opt/netapp` per abilitare il contesto.
3. Se si dispone di un mount NFS diretto, eseguire il seguente comando per impostare il contesto:

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

   a. Verificare che il contesto sia impostato correttamente:

      `ls -dZ /opt/netapp`

   Un output di esempio

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

Configurazione del contesto SELinux quando `/opt/netapp` sia montato, e. `/opt/netapp/data/` non è montato separatamente

Se è stato montato `/opt/netapp` Nel sistema e SELinux è impostato su `Enforcing`, Assicurarsi che il tipo di contesto SELinux per `/opt/netapp` è impostato su `mysqld_db_t`, che è l'elemento di contesto predefinito per la posizione dei file di database.

Fasi

1. Eseguire questo comando per verificare il contesto:

   `ls -dZ /opt/netapp`

   Un output di esempio:

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

   In questo output, il contesto è `default_t`. Impostare questo contesto su `mysqld_db_t`.

2. Attenersi alla seguente procedura per impostare il contesto in base alla modalità di montaggio `/opt/netapp`.

a. Eseguire i seguenti comandi per impostare il contesto su `mysqld_db_t`:
`semanage fcontext -a -t mysqld_db_t "/opt/netapp"`
`` `restorecon -R -v /opt/netapp ``

b. Se è stato configurato `/opt/netapp` poll `/etc/fstab`, modificare il `/etc/fstab` file. Per `/opt/netapp/` Montare l'opzione, aggiungere l'etichetta MySQL come:
`context=system_u:object_r:mysqld_db_t:s0`

c. Smontare e montare nuovamente `/opt/netapp/` per abilitare il contesto.

d. Se si dispone di un mount NFS diretto, eseguire il seguente comando per impostare il contesto su `mysqld_db_t`:
`mount <nfsshare>:/<mountpoint> /opt/netapp -o context=system_u:object_r:mysqld_db_t:s0`

3. Verificare che il contesto sia impostato correttamente:

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

Un output di esempio:

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

Installazione di Unified Manager su sistemi Linux

È importante comprendere che la sequenza dei passaggi per scaricare e installare Unified Manager varia in base allo scenario di installazione.

Creazione di una home directory utente personalizzata e di una password umadmin prima dell'installazione

È possibile creare una home directory personalizzata e definire la propria password utente umadmin prima di installare Unified Manager. Questa attività è facoltativa, ma alcuni siti potrebbero aver bisogno della flessibilità necessaria per ignorare le impostazioni predefinite di installazione di Unified Manager.

Cosa ti serve

- Il sistema deve soddisfare i requisiti descritti in "Requisiti di sistema hardware".
- Devi essere in grado di accedere come utente root al sistema Red Hat Enterprise Linux o CentOS.

L'installazione predefinita di Unified Manager esegue le seguenti operazioni:

- Crea l'utente umadmin con `/home/umadmin` come home directory.
- Assegna la password predefinita "admin" all'utente umadmin.

Perché alcuni ambienti di installazione limitano l'accesso a. `/home`, l'installazione non riesce. È necessario creare la home directory in una posizione diversa. Inoltre, alcuni siti potrebbero avere regole sulla complessità delle password o richiedere che le password siano impostate dagli amministratori locali piuttosto che dal programma di installazione.

Se l'ambiente di installazione richiede l'override di queste impostazioni predefinite, attenersi alla seguente procedura per creare una home directory personalizzata e per definire la password dell'utente umadmin.

Quando queste informazioni vengono definite prima dell'installazione, lo script di installazione rileva queste impostazioni e utilizza i valori definiti invece di utilizzare le impostazioni predefinite dell'installazione.

Inoltre, l'installazione predefinita di Unified Manager include l'utente umadmin nei file sudoers (`ocum_sudoers` e. `ocie_sudoers`) in `/etc/sudoers.d/` directory. Se si rimuove questo contenuto dall'ambiente a causa di policy di sicurezza o a causa di alcuni strumenti di monitoraggio della sicurezza, è necessario aggiungerlo nuovamente. È necessario preservare la configurazione dei sudoers perché alcune operazioni di Unified Manager richiedono questi privilegi sudo.

Le policy di sicurezza nel tuo ambiente non devono limitare i privilegi sudo per l'utente di manutenzione di Unified Manager. Alcune operazioni di Unified Manager potrebbero non riuscire se i privilegi sono limitati. Verificare di essere in grado di eseguire il seguente comando sudo una volta effettuato l'accesso come utente umadmin dopo aver completato l'installazione.

```
sudo systemctl status ocie
```

Questo comando dovrebbe restituire lo stato appropriato del servizio ocie senza errori.

Fasi

1. Accedere come utente root al server.
2. Creare l'account di gruppo umadmin chiamato "maintenance":

   ```
   groupadd maintenance
   ```

3. Creare l'account utente "umadmin" nel gruppo di manutenzione sotto una home directory a scelta:

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

4. Definire la password di umadmin:

   ```
   passwd umadmin
   ```

   Il sistema richiede di inserire una nuova stringa di password per l'utente umadmin.

Dopo aver installato Unified Manager, specificare la shell di login utente umadmin.

Download di Unified Manager

È necessario scaricare Unified Manager `.zip` Dal NetApp Support Site per installare Unified Manager.

Cosa ti serve

È necessario disporre delle credenziali di accesso per il NetApp Support Site.

Scarica lo stesso pacchetto di installazione di Unified Manager per i sistemi Red Hat Enterprise Linux e CentOS.

Fasi

1. Accedere al NetApp Support Site e accedere alla pagina Download di Unified Manager:

   "Sito di supporto NetApp"

2. Selezionare la versione richiesta di Unified Manager e accettare il contratto di licenza con l'utente finale (EULA).
3. Scaricare il file di installazione di Unified Manager per Linux e salvare `.zip` in una directory del sistema di destinazione.

   - Assicurarsi di scaricare la versione corretta del file di installazione per il sistema Red Hat Enterprise Linux. A seconda che sia installato Red Hat Enterprise Linux 7 o 8, assicurarsi di scaricare la versione appropriata di Unified Manager `.zip` file.
   - NetApp consiglia di scaricare il certificato di firma del codice (`.pem`) e firma digitale (`.sig`) insieme a `.zip` file.

4. Verificare l'integrità del software scaricato.
5. Se sono stati scaricati il certificato di firma del codice e la firma digitale, è possibile verificare l'integrità del file di installazione. È possibile utilizzare i seguenti comandi per verificare l'integrità del file di installazione:
   - Questo comando crea un file con la chiave pubblica dal certificato di firma del codice:

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

     - Dove **AIQUM-RHEL-CLIENT-INTER-ROOT.pem** è il file che contiene il certificato di firma del codice.
   - Questo comando verifica la firma sul file di installazione:

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

     Il messaggio è simile a. `Verified Ok` conferma che il file di installazione è sicuro da utilizzare.

Installazione di Unified Manager

È possibile installare Unified Manager su una piattaforma fisica o virtuale Red Hat Enterprise Linux o CentOS.

Cosa ti serve

- Il sistema su cui si desidera installare Unified Manager deve soddisfare i requisiti di sistema e software.

  Vedere "Requisiti di sistema hardware".

  Vedere "Software Linux e requisiti di installazione".

- È necessario aver scaricato Unified Manager `.zip` Dal sito di supporto NetApp al sistema di destinazione.

- Dovresti aver verificato l'integrità del scaricato `.zip` file.
- È necessario disporre di un browser Web supportato.
- Il software di emulazione del terminale deve avere lo scrollback attivato.

Il sistema Red Hat Enterprise Linux o CentOS potrebbe avere tutte le versioni richieste del software di supporto richiesto (Java, MySQL, utility aggiuntive) installato, solo una parte del software richiesto installato o potrebbe essere un sistema appena installato senza alcun software richiesto installato.

Fasi

1. Accedere al server su cui si sta installando Unified Manager.
2. Immettere i comandi appropriati per valutare quale software potrebbe richiedere l'installazione o l'aggiornamento sul sistema di destinazione per supportare l'installazione:

Software richiesto e versione minima	Comando per verificare il software e la versione
OpenJDK versione 11.0.17	`java -version`
MySQL 8.0.30 Community Edition	`rpm -qa
grep -i mysql`	p7zip 16.02
`rpm -qa	grep p7zip`

3. Se la versione installata di MySQL è precedente a MySQL 8.0.30 Community Edition, immettere il seguente comando per disinstallarla:

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

   Se si ricevono errori di dipendenza, è necessario aggiungere `--nodeps` opzione per disinstallare il componente.

4. Accedere alla directory in cui è stata scaricata l'installazione `.zip` Archiviare ed espandere il bundle Unified Manager:

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

   Il necessario `.rpm` I moduli per Unified Manager vengono decompressi nella directory di destinazione.

5. Verificare che il seguente modulo sia disponibile nella directory:

   ```
   ls *.rpm
   ```

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

6. Eseguire lo script di preinstallazione per assicurarsi che non vi siano impostazioni di configurazione del sistema o software installati che potrebbero entrare in conflitto con l'installazione di Unified Manager:

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

   Lo script di preinstallazione verifica che il sistema disponga di un abbonamento Red Hat Enterprise Linux

valido e che abbia accesso ai repository software richiesti. Se lo script identifica eventuali problemi, è necessario risolverli prima di installare Unified Manager.

Per il sistema Red Hat Enterprise Linux 8, se si dispone di repository interni con JDK 11 - OpenJDK, p7zip e altri pacchetti software forniti dal repository AppStream, è necessario disattivare il repository AppStream e installare MySQL Community Server. Eseguire il seguente comando:

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

7. **Opzionale:** eseguire il passaggio 7 solo se il sistema non è connesso a Internet e si devono scaricare manualmente i pacchetti necessari per l'installazione. Se il sistema dispone dell'accesso a Internet e sono disponibili tutti i pacchetti richiesti, passare al punto 8. Per i sistemi che non sono connessi a Internet o che non utilizzano i repository Red Hat Enterprise Linux, attenersi alla seguente procedura per determinare se mancano i pacchetti richiesti, quindi scaricarli:

   a. Sul sistema in cui si installa Unified Manager, visualizzare l'elenco dei pacchetti disponibili e non disponibili:
   `yum install netapp-um<version>.x86_64.rpm --assumeno`

   Gli elementi della sezione "Installing:" sono i pacchetti disponibili nella directory corrente, mentre gli elementi della sezione "Installing for dependenze:" sono i pacchetti mancanti nel sistema.

   b. Su un sistema con accesso a Internet, scaricare i pacchetti mancanti:

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

   > Poiché il plug-in "yum-plugin-downloadonly" non è sempre abilitato sui sistemi Red Hat Enterprise Linux, potrebbe essere necessario abilitare la funzionalità per scaricare un pacchetto senza installarlo:
   > `yum install yum-plugin-downloadonly`

   a. Copiare i pacchetti mancanti dal sistema connesso a Internet al sistema di installazione.

8. Come utente root, o utilizzando `sudo`, eseguire il seguente comando per installare il software:

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

   Questo comando installa i pacchetti .rpm, tutti gli altri software di supporto necessari e il software Unified Manager.

   > Non tentare l'installazione utilizzando comandi alternativi (ad esempio `rpm -ivh`). Una corretta installazione di Unified Manager su un sistema Red Hat Enterprise Linux o CentOS richiede che tutti i file di Unified Manager e i file correlati siano installati in un ordine specifico in una struttura di directory specifica che viene applicata automaticamente da `yum install netapp-um<version>.x86_64.rpm` comando.

9. Ignorare la notifica e-mail visualizzata immediatamente dopo i messaggi di installazione.

   L'e-mail notifica all'utente root un errore iniziale del processo cron, che non ha alcun effetto negativo sull'installazione.

10. Una volta completati i messaggi di installazione, scorrere indietro i messaggi fino a visualizzare il messaggio in cui il sistema visualizza un indirizzo IP o un URL per l'interfaccia utente Web di Unified Manager, il nome utente per la manutenzione (umadmin) e una password predefinita.

    Il messaggio è simile al seguente:

    ```
    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. Registrare l'indirizzo IP o l'URL, il nome utente assegnato (umadmin) e la password corrente.
12. Se è stato creato un account utente umadmin con una home directory personalizzata prima di installare Unified Manager, è necessario specificare la shell di accesso utente umadmin:

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

Accedere all'interfaccia utente Web per modificare la password predefinita dell'utente umadmin ed eseguire la configurazione iniziale di Unified Manager, come descritto in "Configurazione di Active IQ Unified Manager". È obbligatorio modificare la password predefinita dell'utente umadmin.

Utenti creati durante l'installazione di Unified Manager

Quando installate Unified Manager su Red Hat Enterprise Linux o CentOS, Unified Manager e le utility di terze parti creano i seguenti utenti: Umadmin, jboss e mysql.

- **umadmin**

  Utilizzato per accedere a Unified Manager per la prima volta. A questo utente viene assegnato un ruolo utente "Application Administrator" ed è configurato come tipo "Maintenance User". Questo utente viene creato da Unified Manager.

- **jboss**

  Utilizzato per eseguire i servizi di Unified Manager correlati all'utility JBoss. Questo utente viene creato da Unified Manager.

- **mysql**

  Utilizzato per eseguire query di database MySQL di Unified Manager. Questo utente viene creato dall'utility MySQL di terze parti.

Oltre a questi utenti, Unified Manager crea anche gruppi corrispondenti: Maintenance, jboss e mysql. I gruppi Maintenance e jboss vengono creati da Unified Manager, mentre il gruppo mysql viene creato da un'utility di

terze parti.

> Se è stata creata una home directory personalizzata e definita la propria password utente umadmin prima di installare Unified Manager, il programma di installazione non ricreerà il gruppo di manutenzione o l'utente umadmin.

Modifica della password JBoss

È possibile reimpostare la password JBoss specifica dell'istanza impostata durante l'installazione. È possibile reimpostare la password facoltativamente, nel caso in cui il sito richieda questa funzionalità di sicurezza per ignorare l'impostazione di installazione di Unified Manager. Questa operazione modifica anche la password utilizzata da JBoss per accedere a MySQL.

- È necessario disporre dell'accesso utente root al sistema Red Hat Enterprise Linux o CentOS su cui è installato Unified Manager.
- Devi essere in grado di accedere al servizio fornito da NetApp `password.sh` script nella directory `/opt/netapp/essentials/bin`.

Fasi

1. Accedere come utente root sul sistema.
2. Arrestare i servizi di Unified Manager immettendo i seguenti comandi nell'ordine indicato:

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

   Non interrompere il software MySQL associato.

3. Immettere il seguente comando per avviare il processo di modifica della password:

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

4. Quando richiesto, inserire la nuova password JBoss, quindi immetterla una seconda volta per confermarla.

   Tenere presente che la password deve essere compresa tra 8 e 16 caratteri e deve contenere almeno una cifra, caratteri maiuscoli e minuscoli e almeno uno dei seguenti caratteri speciali:

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

5. Al termine dello script, avviare i servizi di Unified Manager immettendo i seguenti comandi nell'ordine indicato:

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

6. Una volta avviati tutti i servizi, è possibile accedere all'interfaccia utente di Unified Manager.

Aggiornamento di Unified Manager su Red Hat Enterprise Linux o CentOS

È possibile aggiornare Unified Manager quando è disponibile una nuova versione.

Le release di patch del software Unified Manager, se fornite da NetApp, vengono installate utilizzando la stessa procedura delle nuove release.

Se Unified Manager è associato a un'istanza di OnCommand Workflow Automation e sono disponibili nuove versioni del software per entrambi i prodotti, è necessario scollegare i due prodotti e impostare una nuova connessione per l'automazione del flusso di lavoro dopo aver eseguito gli aggiornamenti. Se si esegue un aggiornamento a uno solo dei prodotti, dopo l'aggiornamento è necessario accedere a Workflow Automation e verificare che stia ancora acquisendo dati da Unified Manager.

Percorso di aggiornamento supportato per le versioni di Unified Manager

Active IQ Unified Manager supporta un percorso di aggiornamento specifico per ciascuna versione.

Non tutte le versioni di Unified Manager possono eseguire un aggiornamento in-place alle versioni successive. Gli aggiornamenti di Unified Manager sono limitati a un modello N-2, il che significa che un aggiornamento può essere eseguito solo nelle 2 release successive su tutte le piattaforme. Ad esempio, è possibile eseguire un aggiornamento a Unified Manager 9.12 solo da Unified Manager 9.10 e 9.11.

Se si utilizza una versione precedente a quella supportata, l'istanza di Unified Manager deve essere prima aggiornata a una delle versioni supportate, quindi aggiornata alla versione corrente.

Ad esempio, se la versione installata è OnCommand 9.5 e si desidera eseguire l'aggiornamento alla versione più recente di Active IQ Unified Manager 9.12, seguire una sequenza di aggiornamenti.

Esempio di percorso di aggiornamento:

1. Upgrade di OnCommand Unified Manager 9.5 → Active IQ Unified Manager 9.7.
2. Aggiornamento 9.7 → 9.9.
3. Aggiornamento 9.9 → 9.11.
4. Aggiornamento 9.11 → 9.12.

Per ulteriori informazioni sulla matrice dei percorsi di aggiornamento, vedere questa sezione "Articolo della Knowledge base (KB)".

Aggiornamento di Unified Manager

È possibile eseguire l'aggiornamento da Unified Manager 9.10 o 9.11 a 9.12 scaricando ed eseguendo il file di installazione sulla piattaforma Linux.

Cosa ti serve

- Il sistema su cui si esegue l'aggiornamento di Unified Manager deve soddisfare i requisiti di sistema e software.

  Vedere "Requisiti di sistema hardware".

  Vedere "Software Linux e requisiti di installazione".

- È necessario disporre di un abbonamento a Red Hat Enterprise Linux Subscription Manager.
- Prima di aggiornare Unified Manager, è necessario installare o aggiornare alla versione corretta di OpenJDK.

  Vedere "Aggiornamento di JRE su Linux".

- Per evitare la perdita di dati, è necessario aver creato un backup del database di Unified Manager in caso di problemi durante l'aggiornamento. NetApp consiglia di spostare il file di backup da `/opt/netapp/data` directory in una posizione esterna.
- Durante l'aggiornamento, potrebbe essere richiesto di confermare se si desidera mantenere le impostazioni predefinite precedenti per la conservazione dei dati sulle prestazioni per 13 mesi o se si desidera modificarli in 6 mesi. Dopo la conferma, i dati storici delle performance vengono eliminati dopo 6 mesi.
- Le operazioni in esecuzione dovrebbero essere state completate, poiché Unified Manager non è disponibile durante il processo di aggiornamento.
- MySQL Community Edition viene aggiornato automaticamente durante l'aggiornamento di Unified Manager. Se la versione installata di MySQL sul sistema è precedente alla 8.0.30, il processo di aggiornamento di Unified Manager aggiorna automaticamente MySQL alla versione 8.0.30.

Fasi

1. Accedere al server Red Hat Enterprise Linux o CentOS di destinazione.
2. Scaricare il bundle Unified Manager sul server.

   Vedere "Download di Unified Manager per Linux".

3. Accedere alla directory di destinazione ed espandere il bundle Unified Manager:

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

   I moduli RPM richiesti per Unified Manager vengono decompressi nella directory di destinazione.

4. Verificare che il seguente modulo sia disponibile nella directory:

   ```
   ls *.rpm
   ```

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

5. Eseguire lo script di preinstallazione per assicurarsi che non vi siano impostazioni di configurazione del sistema o software installati che potrebbero entrare in conflitto con l'aggiornamento:

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

   Lo script di preinstallazione verifica che il sistema disponga di un abbonamento Red Hat Enterprise Linux valido e che abbia accesso ai repository software richiesti. Se lo script identifica eventuali problemi, è necessario risolvere i problemi e continuare con l'aggiornamento.

   Se sono stati rilevati pacchetti mancanti, eseguire la procedura descritta in "Ulteriori passaggi da eseguire per i pacchetti mancanti". Se non sono presenti pacchetti mancanti, procedere con i passi successivi.

6. Aggiornare Unified Manager utilizzando il seguente script:

   ```
   upgrade.sh
   ```

Questo script esegue automaticamente i moduli RPM, aggiornando il software di supporto necessario e i moduli Unified Manager che li eseguono. Inoltre, lo script di aggiornamento verifica se sono presenti impostazioni di configurazione del sistema o software installati che potrebbero entrare in conflitto con l'aggiornamento. Se lo script identifica eventuali problemi, è necessario risolverli prima di aggiornare Unified Manager. Se in precedenza sono stati installati pacchetti, come *net-snmp* prima di aggiornare Unified Manager, la dipendenza MySQL potrebbe disinstallare il pacchetto durante l'aggiornamento. Per continuare a utilizzarlo, è necessario installare di nuovo il pacchetto manualmente.

7. Una volta completato l'aggiornamento, scorrere i messaggi fino a visualizzare un indirizzo IP o un URL per l'interfaccia utente Web di Unified Manager, il nome utente per la manutenzione (umadmin) e la password predefinita.

   Il messaggio è simile al seguente:

   ```
   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/
   ```

Inserire l'indirizzo IP o l'URL specificato in una nuova finestra di un browser Web supportato per avviare l'interfaccia utente Web di Unified Manager, quindi accedere utilizzando lo stesso nome utente di manutenzione (umadmin) e la stessa password impostati in precedenza.

Ulteriori passaggi da eseguire per i pacchetti mancanti

Se durante l'aggiornamento sono stati rilevati pacchetti mancanti, se il sistema non è connesso a Internet o se non si utilizzano i repository Red Hat Enterprise Linux, attenersi alla seguente procedura per determinare se mancano i pacchetti richiesti e scaricarli.

> Questi passaggi devono essere eseguiti dopo la fase *5* della procedura principale. Questa procedura aggiorna Unified Manager e non è necessario eseguire ulteriori passaggi per l'aggiornamento.

1. Visualizzare l'elenco dei pacchetti disponibili e non disponibili:

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

   Gli elementi della sezione "Installing:" sono i pacchetti disponibili nella directory corrente, mentre gli elementi della sezione "Installing for dependenze:" sono i pacchetti mancanti nel sistema.

2. Su un altro sistema con accesso a Internet, eseguire il seguente comando per scaricare i pacchetti mancanti.

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

   I pacchetti vengono scaricati nella directory specificata come `--downloaddir=`.

   Poiché il plug-in "yum-plugin-downloadonly" non è sempre abilitato sui sistemi Red Hat Enterprise Linux,

potrebbe essere necessario abilitare la funzionalità per scaricare un pacchetto senza installarlo:

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

3. Copiare i pacchetti scaricati nella directory in cui è stato decompresso il bundle Unified Manager sul sistema di installazione.
4. Cambiare le directory in quella directory ed eseguire il seguente comando per installare i pacchetti mancanti, insieme alle relative dipendenze.

```
yum install *.rpm
```

5. Avviare il server Unified Manager. Eseguire questi comandi:

```
systemctl start ocie

systemctl start ocieau
```

Questo processo completa il processo di aggiornamento di Unified Manager. Inserire l'indirizzo IP o l'URL specificato in una nuova finestra di un browser Web supportato per avviare l'interfaccia utente Web di Unified Manager, quindi accedere utilizzando lo stesso nome utente di manutenzione (umadmin) e la stessa password impostati in precedenza.

Aggiornamento del sistema operativo host da Red Hat Enterprise Linux 7.x a 8.x.

Se in precedenza è stato installato Unified Manager su un sistema Red Hat Enterprise Linux 7.x e si desidera eseguire l'aggiornamento a Red Hat Enterprise Linux 8.x, seguire una delle procedure elencate in questo argomento. In entrambi i casi, è necessario creare un backup di Unified Manager sul sistema Red Hat Enterprise Linux 7.x, quindi ripristinare il backup su un sistema Red Hat Enterprise Linux 8.x. Le versioni supportate di Red Hat Enterprise Linux vanno dalla 8.0 alla 8.6.

La differenza tra le due opzioni elencate di seguito è che in un caso si esegue il ripristino di Unified Manager su un nuovo server 8.x e nell'altro si esegue l'operazione di ripristino sullo stesso server.

Poiché questa attività richiede la creazione di un backup di Unified Manager sul sistema Red Hat Enterprise Linux 7.x, è necessario creare il backup solo quando si è pronti a completare l'intero processo di aggiornamento in modo che Unified Manager non sia in linea per il periodo di tempo più breve. Le lacune nei dati raccolti appaiono nell'interfaccia utente di Unified Manager per il periodo di tempo durante il quale il sistema Red Hat Enterprise Linux 7.x viene spento e prima dell'avvio del nuovo Red Hat Enterprise Linux 8.x.

Vedere "Gestione delle operazioni di backup e ripristino" se è necessario rivedere le istruzioni dettagliate per i processi di backup e ripristino.

Aggiornamento del sistema operativo host mediante un nuovo server

Se si dispone di un sistema di riserva su cui è possibile installare il software Red Hat Enterprise Linux 8.x in modo da poter eseguire il ripristino di Unified Manager su quel sistema mentre il sistema Red Hat Enterprise Linux 7.x è ancora disponibile, seguire questa procedura.

1. Installare e configurare un nuovo server con il software Red Hat Enterprise Linux 8.x.

   Vedere "Software Linux e requisiti di installazione".

2. Sul sistema Red Hat Enterprise Linux 8.x, installate la stessa versione del software Unified Manager presente sul sistema Red Hat Enterprise Linux 7.x.

   Vedere "Installazione di Unified Manager su Linux".

   Non avviare l'interfaccia utente né configurare cluster, utenti o impostazioni di autenticazione al termine dell'installazione. Il file di backup inserisce queste informazioni durante il processo di ripristino.

3. Sul sistema Red Hat Enterprise Linux 7.x, dal menu Administration (Amministrazione) dell'interfaccia utente Web, creare un backup di Unified Manager e quindi copiare il file di backup (`.7z` file) e il contenuto della directory del repository del database (`/database-dumps-repo` sottodirectory) in una posizione esterna.
4. Sul sistema Red Hat Enterprise Linux 7.x, arrestare Unified Manager.
5. Sul sistema Red Hat Enterprise Linux 8.x, copiare il file di backup (`.7z` file) dalla posizione esterna a. `/opt/netapp/data/ocum-backup/` e i file di repository del database su `/database-dumps-repo` sotto la sottodirectory `/ocum-backup` directory.
6. Immettere il seguente comando per ripristinare il database di Unified Manager dal file di backup:

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

7. Inserire l'indirizzo IP o l'URL nel browser Web per avviare l'interfaccia utente Web di Unified Manager, quindi accedere al sistema.

Una volta verificato il corretto funzionamento del sistema, è possibile rimuovere Unified Manager dal sistema Red Hat Enterprise Linux 7.x.

Aggiornamento del sistema operativo host sullo stesso server

Se non si dispone di un sistema libero su cui è possibile installare il software Red Hat Enterprise Linux 8.x.

1. Dal menu Administration (Amministrazione) dell'interfaccia utente Web, creare un backup di Unified Manager, quindi copiare il file di backup (`.7z` file) e il contenuto della directory del repository del database (`/database-dumps-repo` sottodirectory) in una posizione esterna.
2. Rimuovere l'immagine di Red Hat Enterprise Linux 7.x dal sistema e pulire completamente il sistema.
3. Installare e configurare il software Red Hat Enterprise Linux 8.x sullo stesso sistema.

   Vedere "Software Linux e requisiti di installazione".

4. Sul sistema Red Hat Enterprise Linux 8.x, installare la stessa versione del software Unified Manager del sistema Red Hat Enterprise Linux 7.x.

   Vedere "Installazione di Unified Manager su Linux".

   Non avviare l'interfaccia utente né configurare cluster, utenti o impostazioni di autenticazione al termine dell'installazione. Il file di backup inserisce queste informazioni durante il processo di ripristino.

5. Copiare il file di backup (`.7z` file) dalla posizione esterna a. `/opt/netapp/data/ocum-backup/` e i file di repository del database su `/database-dumps-repo` sotto la sottodirectory `/ocum-backup` directory.
6. Immettere il seguente comando per ripristinare il database di Unified Manager dal file di backup:

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

7. Inserire l'indirizzo IP o l'URL nel browser Web per avviare l'interfaccia utente Web di Unified Manager, quindi accedere al sistema.

Aggiornamento di prodotti di terze parti dopo l'installazione di Unified Manager

È possibile aggiornare prodotti di terze parti, come JRE, quando Unified Manager è già installato sui sistemi Linux.

Le aziende che sviluppano questi prodotti di terze parti segnalano regolarmente le vulnerabilità della sicurezza. È possibile eseguire l'aggiornamento alle versioni più recenti di questo software in base alla propria pianificazione.

Aggiornamento di OpenJDK su Linux

È possibile eseguire l'aggiornamento a una versione più recente di OpenJDK sul server Linux su cui è installato Unified Manager per ottenere correzioni per le vulnerabilità della sicurezza.

Cosa ti serve

È necessario disporre dei privilegi di root per il sistema Linux su cui è installato Unified Manager.

È possibile aggiornare le release di OpenJDK all'interno delle famiglie di release. Ad esempio, è possibile eseguire l'aggiornamento da OpenJDK 11.0.14 a OpenJDK 11.0.17, ma non è possibile eseguire l'aggiornamento direttamente da OpenJDK 11 a OpenJDK 12.

Fasi

1. Accedere come utente root sul computer host di Unified Manager.
2. Scaricare la versione appropriata di OpenJDK (64 bit) sul sistema di destinazione.
3. Arrestare i servizi di Unified Manager:

```
systemctl stop ocieau

systemctl stop ocie
```

4. Installare l'ultima versione di OpenJDK sul sistema.
5. Avviare i servizi di Unified Manager:

```
systemctl start ocie

systemctl start ocieau
```

Riavvio di Unified Manager

Potrebbe essere necessario riavviare Unified Manager dopo aver apportato modifiche alla configurazione.

Cosa ti serve

È necessario disporre dell'accesso utente root al server Red Hat Enterprise Linux o CentOS su cui è installato

Unified Manager.

Fasi

1. Accedere come utente root al server sul quale si desidera riavviare il servizio Unified Manager.
2. Arrestare il servizio Unified Manager e il software MySQL associato nell'ordine indicato:

```
systemctl stop ocieau

systemctl stop ocie

systemctl stop mysqld
```

3. Avviare Unified Manager nell'ordine indicato:

```
systemctl start mysqld

systemctl start ocie

systemctl start ocieau
```

`mysqld` È un programma daemon necessario per avviare e arrestare il server MySQL.

Rimozione di Unified Manager

È possibile arrestare e disinstallare Unified Manager dall'host Red Hat Enterprise Linux o CentOS con un singolo comando.

Cosa ti serve

- È necessario disporre dell'accesso dell'utente root al server dal quale si desidera rimuovere Unified Manager.
- Security-Enhanced Linux (SELinux) deve essere disattivato sul sistema Linux. Impostare la modalità runtime di SELinux su "permissive" utilizzando `setenforce 0` comando.
- Tutti i cluster (origini dati) devono essere rimossi dal server Unified Manager prima di rimuovere il software.
- È necessario eliminare manualmente le regole del firewall create per consentire o bloccare la porta MySQL 3306. Le regole del firewall non vengono eliminate automaticamente.

Fasi

1. Accedere come utente root al server sul quale si desidera rimuovere Unified Manager.
2. Arrestare e rimuovere Unified Manager dal server:

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

Questo passaggio rimuove tutti i pacchetti RPM NetApp associati. Non rimuove i moduli software prerequisiti, come Java, MySQL e p7zip.

3. **Opzionale:** se necessario, rimuovere i moduli software di supporto, come Java, MySQL e p7zip:

```
rpm -e p7zip mysql-community-client mysql-community-server mysql-community-
```

```
common mysql-community-libs java-x.y
```

Al termine di questa operazione, il software viene rimosso. Tutti i dati di `/opt/netapp/data` la directory viene spostata in `/opt/netapp/data/BACKUP` dopo la disinstallazione. La disinstallazione di Unified Manager rimuove anche i pacchetti Java e MySQL, a meno che i pacchetti non siano richiesti e utilizzati da qualsiasi altra applicazione del sistema. Tuttavia, i dati MySQL non vengono cancellati.

Rimozione dell'utente umadmin personalizzato e del gruppo di manutenzione

Se è stata creata una home directory personalizzata per definire il proprio account di manutenzione e utente umadmin prima di installare Unified Manager, è necessario rimuovere questi elementi dopo aver disinstallato Unified Manager.

La disinstallazione standard di Unified Manager non rimuove un account di manutenzione e un utente umadmin personalizzato. È necessario eliminare questi elementi manualmente.

Fasi

1. Accedere come utente root al server Red Hat Enterprise Linux.
2. Eliminare l'utente umadmin:

   ```
   userdel umadmin
   ```

3. Eliminare il gruppo di manutenzione:

   ```
   groupdel maintenance
   ```

Installare Unified Manager su sistemi Windows

Introduzione a Active IQ Unified Manager

Active IQ Unified Manager (in precedenza Unified Manager di OnCommand) consente di monitorare e gestire lo stato di salute e le performance dei sistemi storage ONTAP da una singola interfaccia. È possibile implementare Unified Manager su un server Linux, su un server Windows o come appliance virtuale su un host VMware.

Una volta completata l'installazione e aggiunti i cluster che si desidera gestire, Unified Manager fornisce un'interfaccia grafica che visualizza lo stato di capacità, disponibilità, protezione e performance dei sistemi storage monitorati.

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Funzioni del server Unified Manager

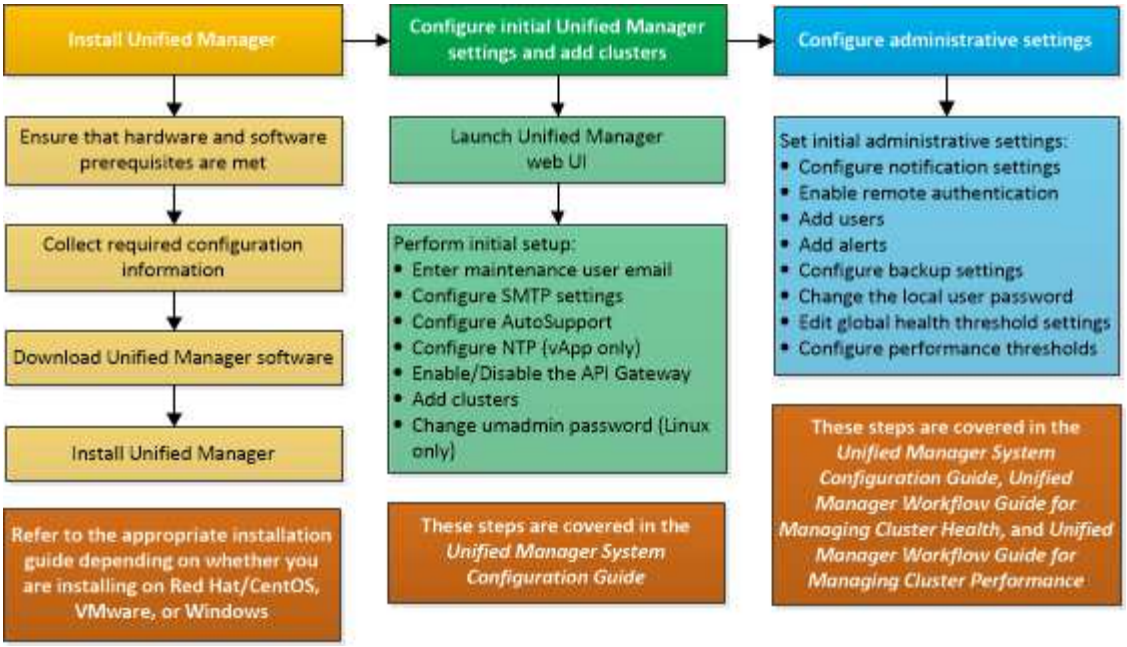
L'infrastruttura server di Unified Manager è costituita da un'unità di raccolta dati, un database e un server applicazioni. Fornisce servizi di infrastruttura come rilevamento, monitoraggio, RBAC (role-based access control), audit e logging.

Unified Manager raccoglie le informazioni sul cluster, memorizza i dati nel database e li analizza per verificare l'eventuale presenza di problemi nel cluster.

Panoramica della sequenza di installazione

Il flusso di lavoro di installazione descrive le attività da eseguire prima di poter utilizzare Unified Manager.

Queste sezioni descrivono ciascuno degli elementi mostrati nel flusso di lavoro seguente.



Requisiti per l'installazione di Unified Manager

Prima di iniziare il processo di installazione, assicurarsi che il server su cui si desidera installare Unified Manager soddisfi i requisiti specifici di software, hardware, CPU e memoria.

NetApp non supporta alcuna modifica del codice applicativo di Unified Manager. Se è necessario applicare misure di sicurezza al server Unified Manager, è necessario apportare tali modifiche al sistema operativo su cui è installato Unified Manager.

Per ulteriori informazioni sull'applicazione delle misure di sicurezza al server Unified Manager, consultare l'articolo della Knowledge base.

"Supporto per le misure di sicurezza applicate a Active IQ Unified Manager per Clustered Data ONTAP"

Informazioni correlate

"Tool di matrice di interoperabilità NetApp"

Infrastruttura virtuale e requisiti di sistema hardware

L'installazione di Unified Manager su un'infrastruttura virtuale o su un sistema fisico deve soddisfare i requisiti minimi di memoria, CPU e spazio su disco.

La seguente tabella mostra i valori consigliati per le risorse di memoria, CPU e spazio su disco. Questi valori sono stati qualificati in modo che Unified Manager soddisfi livelli di performance accettabili.

Configurazione dell'hardware	Impostazioni consigliate
RAM	12 GB (requisito minimo 8 GB)
Processori	4 CPU

Configurazione dell'hardware	Impostazioni consigliate
Capacità del ciclo della CPU	9572 MHz totali (requisito minimo 9572 MHz)
Spazio libero su disco	150 GB, dove la capacità viene allocata come segue: • 100 GB di spazio su disco per la directory di installazione • 50 GB di spazio su disco per la directory dei dati MySQL

Unified Manager può essere installato su sistemi con una piccola quantità di memoria, ma i 12 GB di RAM consigliati garantiscono che sia disponibile una quantità di memoria sufficiente per ottenere performance ottimali e che il sistema possa ospitare cluster e oggetti di storage aggiuntivi con la crescita della configurazione. Non è necessario impostare limiti di memoria sulla macchina virtuale in cui è implementato Unified Manager e non attivare alcuna funzione (ad esempio, la bollatura) che impedisca al software di utilizzare la memoria allocata nel sistema.

Inoltre, esiste un limite al numero di nodi che una singola istanza di Unified Manager può monitorare prima di installare una seconda istanza di Unified Manager. Per ulteriori informazioni, consulta la *Guida alle Best Practice*.

"Report tecnico 4621: Guida alle Best practice di Unified Manager"

Lo swapping della pagina di memoria influisce negativamente sulle prestazioni del sistema e dell'applicazione di gestione. La concorrenza per le risorse CPU non disponibili a causa dell'utilizzo complessivo dell'host può compromettere le prestazioni.

Requisito per l'utilizzo dedicato

Il sistema fisico o virtuale su cui si installa Unified Manager deve essere utilizzato esclusivamente per Unified Manager e non deve essere condiviso con altre applicazioni. Altre applicazioni potrebbero consumare risorse di sistema e ridurre drasticamente le performance di Unified Manager.

Requisiti di spazio per i backup

Se si intende utilizzare la funzione di backup e ripristino di Unified Manager, allocare ulteriore capacità in modo che la directory o il disco "data" disponga di 150 GB di spazio. Un backup può essere scritto in una destinazione locale o remota. La procedura consigliata consiste nell'identificare una postazione remota esterna al sistema host di Unified Manager che abbia almeno 150 GB di spazio.

Requisiti per la connettività host

Il sistema fisico o virtuale su cui si installa Unified Manager deve essere configurato in modo da poter essere correttamente configurato `ping` il nome host dell'host stesso. In caso di configurazione IPv6, è necessario verificarlo `ping6` Al nome host per garantire che l'installazione di Unified Manager abbia esito positivo.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web del prodotto. Se è stato configurato un indirizzo IP statico per la rete durante l'implementazione, è stato designato un nome per l'host di rete. Se la rete è stata configurata utilizzando DHCP, è necessario ottenere il nome host dal DNS.

Se si prevede di consentire agli utenti di accedere a Unified Manager utilizzando il nome breve invece di utilizzare il nome di dominio completo (FQDN) o l'indirizzo IP, la configurazione di rete deve risolvere questo

nome breve in un FQDN valido.

Software Windows e requisiti di installazione

Per una corretta installazione di Unified Manager su Windows, è necessario assicurarsi che il sistema su cui viene installato Unified Manager soddisfi i requisiti software.

Software del sistema operativo

È possibile installare Unified Manager nelle seguenti edizioni di Windows:

- Microsoft Windows Server 2019 Standard e Datacenter Edition
- Microsoft Windows Server 2022 Standard e Datacenter Edition

Unified Manager è supportato dal sistema operativo Windows a 64 bit per le seguenti lingue:

- Inglese
- Giapponese
- Cinese semplificato

Consultare la matrice di interoperabilità per l'elenco completo e aggiornato delle versioni di Windows supportate.

"mysupport.netapp.com/matrix"

NetApp non supporta l'installazione di Unified Manager utilizzando strumenti di terze parti, come Microsoft System Center Configuration Manager (SCCM).

Il server deve essere dedicato all'esecuzione di Unified Manager. Sul server non devono essere installate altre applicazioni. È possibile che nel sistema Windows sia installato un software antivirus attivo a causa delle normative aziendali. Disattivare il software antivirus prima di installare Unified Manager per evitare errori di installazione.

Software di terze parti

I seguenti pacchetti di terze parti sono forniti in bundle con Unified Manager. Se questi pacchetti di terze parti non sono installati nel sistema, Unified Manager li installa come parte dell'installazione.

- Microsoft Visual C& 43; 43; 2015 Redistributable Package versione 14.26.28720.3
- Microsoft Visual C& 43; 43; Redistributable Packages per Visual Studio 2013 versione 12.0.40660.0
- MySQL Community Edition versione 8.0.30
- Python 3.11.1
- OpenJDK versione 11.0.16
- p7zip versione 18.05 o successiva

A partire da Unified Manager 9.5, OpenJDK viene fornito nel pacchetto di installazione di Unified Manager e installato automaticamente. Oracle Java non è supportato a partire da Unified Manager 9.5.

Se MySQL è preinstallato, devi assicurarti che:

- Sta utilizzando la porta predefinita.
- I database di esempio non sono installati.
- Il nome del servizio è “MYSQL8”.

Unified Manager viene implementato su un server Web WildFly. WildFly 19.0.0 viene fornito in bundle e configurato con Unified Manager.

Prima di aggiornare qualsiasi software di terze parti, chiudere un’istanza di Unified Manager in esecuzione. Una volta completata l’installazione del software di terze parti, è possibile riavviare Unified Manager.

Requisiti di installazione

- È necessario installare Microsoft .NET 4.5.2 o versione successiva.
- Il `temp` La directory deve essere configurata con 2 GB di spazio su disco per l’estrazione dei file di installazione. Per verificare se la directory è stata creata, eseguire il seguente comando dall’interfaccia della riga di comando: `echo %temp%`
- È necessario riservare 2 GB di spazio su disco nell’unità Windows per il caching dei file MSI di Unified Manager.
- Il Microsoft Windows Server su cui si desidera installare Unified Manager deve essere configurato con un FQDN (Fully Qualified Domain Name) in modo tale che `ping` Le risposte al nome host e all’FQDN sono riuscite.
- Disattivare il servizio di pubblicazione Web internazionale di Microsoft IIS e assicurarsi che le porte 80 e 443 siano libere.
- Durante l’installazione, assicurarsi che l’impostazione Remote Desktop Session host per “Windows Installer RDS Compatibility” (compatibilità RDS di Windows Installer) sia disattivata.
- La porta UDP 514 deve essere libera e non deve essere utilizzata da altri servizi.
- Prima di installare Unified Manager, disattivare tutti i software antivirus presenti nel sistema. Al termine dell’installazione, assicurarsi di escludere manualmente i seguenti percorsi dalla scansione antivirus:
  - Directory dei dati di Unified Manager, ad esempio `C:\ProgramData\NetApp\OnCommandAppData\`
  - Directory di installazione di Unified Manager, ad esempio `\C:\Program Files\NetApp\`
  - Directory di dati MySQL, ad esempio `C:\ProgramData\MySQL\MySQLServerData`

Browser supportati

Per accedere all’interfaccia utente Web di Unified Manager, utilizzare un browser supportato.

La matrice di interoperabilità contiene l’elenco delle versioni del browser supportate.

"mysupport.netapp.com/matrix"

Per tutti i browser, la disattivazione dei blocchi dei pop-up garantisce la corretta visualizzazione delle funzionalità software.

Se si intende configurare Unified Manager per l’autenticazione SAML, in modo che un provider di identità (IdP) possa autenticare gli utenti, è necessario controllare anche l’elenco dei browser supportati da IdP.

Requisiti di protocollo e porta

Le porte e i protocolli richiesti consentono la comunicazione tra il server Unified Manager e i sistemi di storage gestiti, i server e altri componenti.

Connessioni al server Unified Manager

Nelle installazioni tipiche non è necessario specificare i numeri di porta durante la connessione all'interfaccia utente Web di Unified Manager, poiché vengono sempre utilizzate le porte predefinite. Ad esempio, poiché Unified Manager tenta sempre di essere eseguito sulla porta predefinita, è possibile immettere `https://<host>` invece di `https://<host>:443`.

Il server Unified Manager utilizza protocolli specifici per accedere alle seguenti interfacce:

Interfaccia	Protocollo	Porta	Descrizione
UI Web di Unified Manager	HTTP	80	Utilizzato per accedere all'interfaccia utente Web di Unified Manager; reindirizza automaticamente alla porta sicura 443.
L'interfaccia utente Web di Unified Manager e i programmi che utilizzano API	HTTPS	443	Utilizzato per accedere in modo sicuro all'interfaccia utente Web di Unified Manager o per effettuare chiamate API; le chiamate API possono essere effettuate solo utilizzando HTTPS.
Console di manutenzione	SSH/SFTP	22	Utilizzato per accedere alla console di manutenzione e recuperare i pacchetti di supporto.
Riga di comando Linux	SSH/SFTP	22	Utilizzato per accedere alla riga di comando di Red Hat Enterprise Linux o CentOS e recuperare i bundle di supporto.
Syslog	UDP	514	Utilizzato per accedere ai messaggi EMS basati su abbonamento dai sistemi ONTAP e per creare eventi in base ai messaggi.

Interfaccia	Protocollo	Porta	Descrizione
RIPOSO	HTTPS	9443	Utilizzato per accedere agli eventi EMS basati su API REST in tempo reale da sistemi ONTAP autenticati.
Database MySQL	MySQL	3306	Utilizzato per abilitare l'accesso ai servizi API OnCommand Workflow Automation e OnCommand a Unified Manager.

La porta predefinita per MySQL, 3306, è limitata solo all'host locale durante l'installazione di Unified Manager su sistemi Windows. Questo non influisce su nessuno scenario di aggiornamento, in cui viene mantenuta la configurazione precedente. Questa configurazione può essere modificata e la connessione può essere resa disponibile ad altri host utilizzando `Control access to MySQL port 3306` sulla console di manutenzione. Per ulteriori informazioni, vedere "Opzioni di menu aggiuntive". Le porte utilizzate per le comunicazioni HTTP e HTTPS (porte 80 e 443) possono essere modificate utilizzando la console di manutenzione di Unified Manager. Per ulteriori informazioni, vedere "Configurazione di Active IQ Unified Manager".

Connessioni dal server Unified Manager

È necessario configurare il firewall in modo che apra le porte che consentono la comunicazione tra il server Unified Manager e i sistemi di storage gestiti, i server e altri componenti. Se una porta non è aperta, la comunicazione non riesce.

A seconda dell'ambiente in uso, è possibile scegliere di modificare le porte e i protocolli utilizzati dal server Unified Manager per connettersi a destinazioni specifiche.

Il server Unified Manager si connette utilizzando i seguenti protocolli e porte ai sistemi di storage gestiti, ai server e ad altri componenti:

Destinazione	Protocollo	Porta	Descrizione
Sistema storage	HTTPS	443/TCP	Utilizzato per monitorare e gestire i sistemi storage.
Sistema storage	NDMP	10000/TCP	Utilizzato per alcune operazioni di ripristino Snapshot.

Destinazione	Protocollo	Porta	Descrizione
Server AutoSupport	HTTPS	443	Utilizzato per inviare informazioni AutoSupport. Per eseguire questa funzione, è necessario disporre dell'accesso a Internet.
Server di autenticazione	LDAP	389	Utilizzato per effettuare richieste di autenticazione e richieste di ricerca di utenti e gruppi.
LDAPS	636	Utilizzato per comunicazioni LDAP sicure.	Server di posta
SMTP	25	Utilizzato per inviare e-mail di notifica degli avvisi.	Mittente trap SNMP
SNMPv1 o SNMPv3	162/UDP	Utilizzato per inviare messaggi trap SNMP di notifica degli avvisi.	Server del provider di dati esterno
TCP	2003	Utilizzato per inviare dati sulle prestazioni a un provider di dati esterno, ad esempio Graphite.	Server NTP

Completamento del foglio di lavoro

Prima di installare e configurare Unified Manager, è necessario disporre di informazioni specifiche sull'ambiente in uso. È possibile registrare le informazioni nel foglio di lavoro.

Informazioni sull'installazione di Unified Manager

I dettagli necessari per installare Unified Manager.

Sistema su cui viene implementato il software	Il tuo valore
Nome di dominio completo dell'host	
Host IP address (Indirizzo IP host)	
Maschera di rete	
Indirizzo IP del gateway	

Sistema su cui viene implementato il software	Il tuo valore
Indirizzo DNS primario	
Indirizzo DNS secondario	
Cerca domini	
Nome utente manutenzione	
Password utente per la manutenzione	

Informazioni sulla configurazione di Unified Manager

I dettagli per configurare Unified Manager dopo l'installazione. Alcuni valori sono facoltativi a seconda della configurazione.

Impostazione	Il tuo valore
Indirizzo e-mail utente manutenzione	
Nome host o indirizzo IP del server SMTP	
Nome utente SMTP	
Password SMTP	
Porta SMTP	25 (valore predefinito)
E-mail da cui vengono inviate le notifiche di avviso	
Nome host o indirizzo IP del server di autenticazione	
Nome dell'amministratore di Active Directory o nome distinto del binding LDAP	
Password di Active Directory o bind LDAP	
Nome distinto della base del server di autenticazione	
URL del provider di identità (IdP)	
Metadati del provider di identità (IdP)	
Indirizzi IP host di destinazione del trap SNMP	

Impostazione	Il tuo valore
Porta SNMP	

Informazioni sul cluster

I dettagli dei sistemi storage gestiti con Unified Manager.

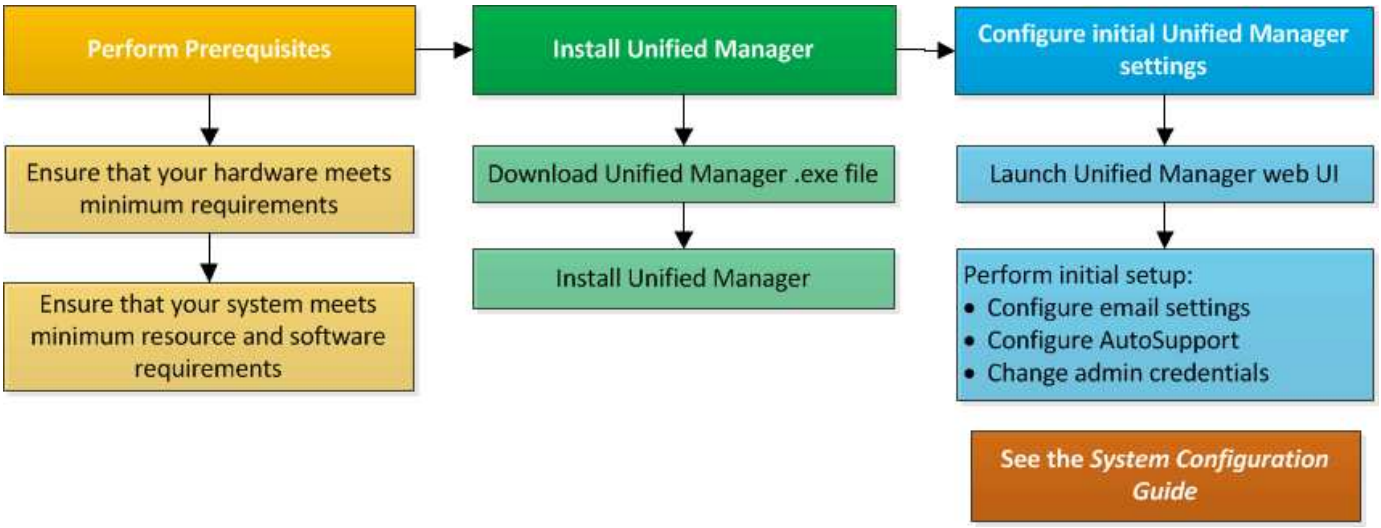
Cluster 1 di N.	Il tuo valore
Nome host o indirizzo IP di gestione del cluster	
Nome utente amministratore di ONTAP All'amministratore deve essere stato assegnato il ruolo "admin".	
Password dell'amministratore di ONTAP	
Protocollo	HTTPS

Installazione, aggiornamento e rimozione del software Unified Manager

È possibile installare Unified Manager, eseguire l'aggiornamento a una versione più recente o rimuovere l'applicazione Unified Manager.

Panoramica del processo di installazione

Il flusso di lavoro di installazione descrive le attività da eseguire prima di poter utilizzare Unified Manager.



Installazione di Unified Manager su Windows

È importante comprendere la sequenza di passaggi per scaricare e installare Unified Manager su Windows.

Installazione di Unified Manager

È possibile installare Unified Manager per monitorare e risolvere i problemi di capacità, disponibilità, performance e protezione dello storage dei dati.

Cosa ti serve

- Il sistema su cui si intende installare Unified Manager deve soddisfare i requisiti di sistema e software.

  Vedere "Requisiti di sistema hardware".

  Vedere "Software Windows e requisiti di installazione".

  > A partire da Unified Manager 9.5, OpenJDK viene fornito nel pacchetto di installazione e installato automaticamente. Oracle Java non è supportato a partire da Unified Manager 9.5.

- È necessario disporre dei privilegi di amministratore di Windows. Assicurarsi che il nome utente non inizi con un punto esclamativo "!". Installation of Unified Manager might fail if the user name of user running the installation begins with "!".
- Si dovrebbe disporre di un browser Web supportato.
- La password utente per la manutenzione di Unified Manager deve essere compresa tra 8 e 20 caratteri, deve contenere lettere maiuscole o minuscole, numeri e caratteri speciali.
- I seguenti caratteri speciali non sono consentiti nella stringa della password per l'utente di manutenzione o per l'utente root MySQL: " ' ` % , = & < > | ^ / ( ) [ ] ;:

  Sono consentiti i seguenti caratteri speciali: ~ ! @ * - ? . + { }

Fasi

1. Accedere a Windows utilizzando l'account di amministratore locale predefinito.
2. Accedere al NetApp Support Site e accedere alla pagina Download di Unified Manager:

   "Sito di supporto NetApp"

3. Selezionare la versione richiesta di Unified Manager e accettare il contratto di licenza con l'utente finale (EULA).
4. Scaricare il file di installazione di Unified Manager Windows in una directory di destinazione sul sistema Windows.
5. Accedere alla directory in cui si trova il file di installazione.
6. Fare clic con il pulsante destro del mouse ed eseguire il file eseguibile del programma di installazione di Unified Manager (.exe) come amministratore.

   Unified Manager rileva i pacchetti di terze parti mancanti o preinstallati e li elenca. Se i pacchetti di terze parti richiesti non sono installati nel sistema, Unified Manager li installa come parte dell'installazione.

7. Fare clic su **Avanti**.
8. Immettere il nome utente e la password per creare l'utente di manutenzione.
9. Nella procedura guidata connessione database, inserire la password root MySQL.
10. Fare clic su **Change** per specificare una nuova posizione per la directory di installazione di Unified Manager e la directory dei dati MySQL.

    Se non si modifica la directory di installazione, Unified Manager viene installato nella directory di installazione predefinita.

11. Fare clic su **Avanti**.
12. Nella procedura guidata Ready to Install Shield, fare clic su **Install** (Installa).
13. Al termine dell'installazione, fare clic su **fine**.
14. Se sul sistema Windows è installato un software antivirus attivo, escludere manualmente i seguenti percorsi dalla scansione antivirus al termine dell'installazione:
    - Directory dei dati di Unified Manager
    - Directory di installazione di Unified Manager
    - Directory dei dati MySQL

L'installazione crea più directory:

- Directory di installazione

  Si tratta della directory principale di Unified Manager, specificata durante l'installazione. Esempio: `C:\Program Files\NetApp\`

- Directory dei dati MySQL

  Questa è la directory in cui sono memorizzati i database MySQL, specificata durante l'installazione. Esempio: `C:\ProgramData\MySQL\MySQLServerData\`

- Directory Java

  Questa è la directory in cui è installato OpenJDK. Esempio: `C:\Program Files\NetApp\JDK\`

- Directory dei dati dell'applicazione di Unified Manager (appDataDir)

  Questa è la directory in cui vengono memorizzati tutti i dati generati dall'applicazione. Sono inclusi log, bundle di supporto, backup e tutti gli altri dati aggiuntivi. Esempio: `C:\ProgramData\NetApp\OnCommandAppData\`

È possibile accedere all'interfaccia utente Web per eseguire la configurazione iniziale di Unified Manager, come descritto in "Configurazione di Active IQ Unified Manager".

Esecuzione di un'installazione automatica di Unified Manager

È possibile installare Unified Manager senza l'intervento dell'utente utilizzando l'interfaccia della riga di comando. È possibile completare l'installazione automatica passando i parametri in coppie chiave-valore.

Fasi

1. Accedere all'interfaccia della riga di comando di Windows utilizzando l'account di amministratore locale predefinito.
2. Individuare la posizione in cui si desidera installare Unified Manager e scegliere una delle seguenti opzioni:

Opzione	Istruzioni

Se i pacchetti di terze parti sono preinstallati	`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"`
	
	Esempio:
	
	`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"`

Se non sono installati pacchetti di terze parti	`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"`
	
	Esempio:
	
	`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"`

Il `/qr` l'opzione attiva la modalità silenziosa con un'interfaccia utente ridotta. Viene visualizzata un'interfaccia utente di base che mostra l'avanzamento dell'installazione. Non vengono richiesti input. Se i pacchetti di terze parti come JRE, MySQL e 7zip non sono preinstallati, utilizzare `/qr` opzione. L'installazione non riesce se `/qn` l'opzione viene utilizzata su un server in cui non sono installati pacchetti

di terze parti.

Il `/qn` l'opzione attiva la modalità silenziosa senza interfaccia utente. Durante l'installazione non viene visualizzata alcuna interfaccia utente o dettagli. Non utilizzare `/qn` opzione quando non sono installati pacchetti di terze parti.

3. Accedere all'interfaccia utente Web di Unified Manager utilizzando il seguente URL:

   `https://IP address`

Modifica della password JBoss

È possibile reimpostare la password JBoss specifica dell'istanza impostata durante l'installazione. È possibile reimpostare la password facoltativamente, nel caso in cui il sito richieda questa funzionalità di sicurezza per ignorare l'impostazione di installazione di Unified Manager. Questa operazione modifica anche la password utilizzata da JBoss per accedere a MySQL.

Cosa ti serve

- È necessario disporre dei privilegi di amministratore di Windows per il sistema su cui è installato Unified Manager.
- Devi avere la password per l'utente root MySQL.
- Dovresti essere in grado di accedere al servizio fornito da NetApp `password.bat` script nella directory

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

Fasi

1. Accedere come utente amministratore sul computer host di Unified Manager.
2. Utilizzare la console dei servizi Windows per arrestare i seguenti servizi di Unified Manager:
   - Servizio di acquisizione NetApp Active IQ (Ocie-au)
   - Servizio server di gestione NetApp Active IQ (Oncommandsvc)
3. Avviare `password.bat` script per avviare il processo di modifica della password:

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

4. Quando richiesto, inserire la password dell'utente root MySQL.
5. Quando richiesto, inserire la nuova password utente JBoss, quindi immetterla di nuovo per confermarla.

   Tenere presente che la password deve essere compresa tra 8 e 16 caratteri e deve contenere almeno una cifra, caratteri maiuscoli e minuscoli e almeno uno dei seguenti caratteri speciali:

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

6. Al termine dello script, avviare i servizi di Unified Manager utilizzando la console dei servizi Windows:
   - Servizio server di gestione NetApp Active IQ (Oncommandsvc)
   - Servizio di acquisizione NetApp Active IQ (Ocie-au)

7. Una volta avviati tutti i servizi, è possibile accedere all'interfaccia utente di Unified Manager.

Percorso di aggiornamento supportato per le versioni di Unified Manager

Active IQ Unified Manager supporta un percorso di aggiornamento specifico per ciascuna versione.

Non tutte le versioni di Unified Manager possono eseguire un aggiornamento in-place alle versioni successive. Gli aggiornamenti di Unified Manager sono limitati a un modello N-2, il che significa che un aggiornamento può essere eseguito solo nelle 2 release successive su tutte le piattaforme. Ad esempio, è possibile eseguire un aggiornamento a Unified Manager 9.12 solo da Unified Manager 9.10 e 9.11.

Se si utilizza una versione precedente a quella supportata, l'istanza di Unified Manager deve essere prima aggiornata a una delle versioni supportate, quindi aggiornata alla versione corrente.

Ad esempio, se la versione installata è OnCommand 9.5 e si desidera eseguire l'aggiornamento alla versione più recente di Active IQ Unified Manager 9.12, seguire una sequenza di aggiornamenti.

Esempio di percorso di aggiornamento:

1. Upgrade di OnCommand Unified Manager 9.5 → Active IQ Unified Manager 9.7.
2. Aggiornamento 9.7 → 9.9.
3. Aggiornamento 9.9 → 9.11.
4. Aggiornamento 9.11 → 9.12.

Per ulteriori informazioni sulla matrice dei percorsi di aggiornamento, vedere questa sezione "Articolo della Knowledge base (KB)".

Aggiornamento di Unified Manager

È possibile aggiornare Unified Manager 9.10 o 9.11 a 9.12 scaricando ed eseguendo il file di installazione sulla piattaforma Windows.

Cosa ti serve

- Il sistema su cui si esegue l'aggiornamento di Unified Manager deve soddisfare i requisiti di sistema e software.

  Vedere "Requisiti di sistema hardware".

  Vedere "Software Windows e requisiti di installazione".

  A partire da Unified Manager 9.5, OpenJDK viene fornito nel pacchetto di installazione e installato automaticamente. Oracle Java non è supportato a partire da Unified Manager 9.5.

  Prima di avviare l'aggiornamento, assicurarsi che sul sistema sia installato Microsoft .NET 4.5.2 o versione successiva.

- MySQL Community Edition viene aggiornato automaticamente durante l'aggiornamento di Unified Manager. Se la versione installata di MySQL sul sistema è precedente alla 8.0.30, il processo di aggiornamento di Unified Manager aggiorna automaticamente MySQL alla versione 8.0.30. Non è necessario eseguire un aggiornamento standalone di una versione precedente di MySQL alla versione

8.0.30.

- È necessario disporre dei privilegi di amministratore di Windows. Assicurarsi che il nome utente non inizi con un punto esclamativo "!". Installation of Unified Manager might fail if the user name of user running the installation begins with "!".
- Per accedere al NetApp Support Site, è necessario disporre di credenziali valide.
- Per evitare la perdita di dati, è necessario aver creato un backup della macchina Unified Manager in caso di problemi durante l'aggiornamento.
- Per eseguire l'aggiornamento, è necessario disporre di spazio su disco sufficiente.

  Lo spazio disponibile sul disco di installazione deve essere di 2.5 GB più grande della dimensione della directory dei dati. L'aggiornamento si interrompe e viene visualizzato un messaggio di errore che indica la quantità di spazio da aggiungere se lo spazio disponibile non è sufficiente.

- Durante l'aggiornamento, potrebbe essere richiesto di confermare se si desidera mantenere le impostazioni predefinite precedenti per la conservazione dei dati sulle prestazioni per 13 mesi o se si desidera modificarli in 6 mesi. Alla conferma, i dati storici delle performance dopo 6 mesi vengono eliminati.
- Prima di eseguire l'aggiornamento, chiudere tutti i file o le cartelle aperti in *<InstallDir>* e *directory dati MySQL*.
- Se sul sistema Windows è installato un software antivirus attivo, l'aggiornamento di Unified Manager potrebbe non riuscire. Prima di eseguire l'aggiornamento di Unified Manager, disattivare tutti i software di scansione antivirus presenti nel sistema.

Durante il processo di aggiornamento, Unified Manager non è disponibile. Prima di eseguire l'aggiornamento di Unified Manager, è necessario completare tutte le operazioni in esecuzione.

Se Unified Manager è associato a un'istanza di OnCommand Workflow Automation e sono disponibili nuove versioni del software per entrambi i prodotti, è necessario scollegare i due prodotti e impostare una nuova connessione per l'automazione del flusso di lavoro dopo aver eseguito gli aggiornamenti. Se si esegue un aggiornamento a uno solo dei prodotti, dopo l'aggiornamento è necessario accedere a Workflow Automation e verificare che stia ancora acquisendo dati da Unified Manager.

Fasi

1. Accedere al NetApp Support Site e accedere alla pagina Download di Unified Manager:

   "Sito di supporto NetApp".

2. Selezionare la versione richiesta di Unified Manager e accettare il contratto di licenza con l'utente finale (EULA).
3. Scaricare il file di installazione di Unified Manager Windows in una directory di destinazione sul sistema Windows.
4. Fare clic con il pulsante destro del mouse ed eseguire il file eseguibile del programma di installazione di Unified Manager (.exe) come amministratore.

   Unified Manager visualizza il seguente messaggio:

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

5. Fare clic su **Sì**, quindi su **Avanti**.
6. Immettere la password root di MySQL8 impostata durante l'installazione, quindi fare clic su **Avanti**.
7. Avviare l'interfaccia utente Web in una nuova finestra di un browser Web supportato e accedere per utilizzare la versione aggiornata di Unified Manager.
8. Se sul sistema Windows è installato un software antivirus attivo, assicurarsi di escludere manualmente i seguenti percorsi dalla scansione antivirus una volta completato l'aggiornamento:
   - Directory dei dati di Unified Manager
   - Directory di installazione di Unified Manager
   - Directory dei dati MySQL

Per eseguire un aggiornamento silent di Unified Manager, eseguire il seguente comando: `ActiveIQUnifiedManager-<version\>.exe /s /v"MYSQL_PASSWORD=<password> /qn /l*v <system_drive>:\install.log"`

Aggiornamento di prodotti di terze parti

È possibile aggiornare prodotti di terze parti, come JRE, su Unified Manager se installati su sistemi Windows.

Le aziende che sviluppano questi prodotti di terze parti segnalano regolarmente le vulnerabilità della sicurezza. È possibile eseguire l'aggiornamento alle versioni più recenti di questo software in base alla propria pianificazione.

Aggiornamento di OpenJDK

È possibile eseguire l'aggiornamento a una versione più recente di OpenJDK sul server Windows su cui è installato Unified Manager per ottenere correzioni per le vulnerabilità della sicurezza.

Cosa ti serve

È necessario disporre dei privilegi di amministratore di Windows per il sistema su cui è installato Unified Manager.

È possibile aggiornare le release di OpenJDK all'interno delle famiglie di release. Ad esempio, è possibile eseguire l'aggiornamento da OpenJDK 11.0.14 a OpenJDK 11.0.16, ma non è possibile eseguire l'aggiornamento direttamente da OpenJDK 11 a OpenJDK 12.

Fasi

1. Accedere come utente amministratore sul computer host di Unified Manager.
2. Scaricare la versione appropriata di OpenJDK (64 bit) dal sito OpenJDK sul sistema di destinazione.

   Ad esempio, scarica `openjdk-11_windows-x64_bin.zip from http://jdk.java.net/11/`.

3. Utilizzare la console dei servizi Windows per arrestare i seguenti servizi di Unified Manager:
   - Servizio di acquisizione NetApp Active IQ (Ocie-au)
   - Servizio server di gestione NetApp Active IQ (Oncommandsvc)

4. Espandere `zip` file.
5. Copiare le directory e i file dal risultato `jdk` directory (ad esempio, `jdk-11.0.16` Nella posizione in cui è installato Java. Esempio: `C:\Program Files\NetApp\JDK\`
6. Avviare i servizi di Unified Manager utilizzando la console dei servizi Windows:
   - Servizio server di gestione NetApp Active IQ (Oncommandsvc)
   - Servizio di acquisizione NetApp Active IQ (Ocie-au)

Riavvio di Unified Manager

Potrebbe essere necessario riavviare Unified Manager dopo aver apportato modifiche alla configurazione.

Cosa ti serve

È necessario disporre dei privilegi di amministratore di Windows.

Fasi

1. Accedere a Windows utilizzando l'account di amministratore locale predefinito.
2. Arrestare i servizi di Unified Manager:

Dal…	Interrompere i servizi nell'ordine seguente…
Riga di comando	a. `sc stop ocie-au` b. `sc stop Oncommandsvc`
Microsoft Service Manager	a. Servizio di acquisizione NetApp Active IQ (Ocie-au) b. Servizio server di gestione NetApp Active IQ (Oncommandsvc)

3. Avviare i servizi di Unified Manager:

Dal…	Avviare i servizi nel seguente ordine…
Riga di comando	a. `sc start Oncommandsvc` b. `sc start ocie-au`
Microsoft Service Manager	a. Servizio server di gestione NetApp Active IQ (Oncommandsvc) b. Servizio di acquisizione NetApp Active IQ (Ocie-au)

Disinstallazione di Unified Manager

È possibile disinstallare Unified Manager utilizzando la procedura guidata programmi e

funzionalità o eseguendo una disinstallazione automatica dall'interfaccia della riga di comando.

Cosa ti serve

- È necessario disporre dei privilegi di amministratore di Windows.
- Tutti i cluster (origini dati) devono essere rimossi dal server Unified Manager prima di disinstallare il software.
- È necessario eliminare manualmente le regole del firewall create per consentire o bloccare la porta MySQL 3306. Le regole del firewall non vengono eliminate automaticamente.

Fasi

1. Disinstallare Unified Manager scegliendo una delle seguenti opzioni:
   - Se si disinstalla Unified Manager dalla procedura guidata **programmi e funzionalità**, attenersi alla seguente procedura:
     i. Accedere a **pannello di controllo** > **programmi e funzionalità**.
     ii. Selezionare Active IQ Unified Manager e fare clic su **Disinstalla**.
   - Se si disinstalla Unified Manager dalla riga di comando, attenersi alla seguente procedura:
     i. Accedere alla riga di comando di Windows utilizzando i privilegi di amministratore.
     ii. Accedere alla directory Active IQ Unified Manager ed eseguire il seguente comando:

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

     Se il controllo dell'account utente (UAC) è attivato sul server e si è connessi come utente di dominio, è necessario utilizzare il metodo di disinstallazione dalla riga di comando.

   Unified Manager viene disinstallato dal sistema.
2. Disinstallare i seguenti pacchetti e dati di terze parti che non vengono rimossi durante la disinstallazione di Unified Manager:
   - Pacchetti di terze parti: JRE, MySQL, Microsoft Visual C& 43; 43; 2015 Redistributable, Python, e 7zip
   - Dati dell'applicazione MySQL generati da Unified Manager
   - Log delle applicazioni e contenuto della directory dei dati delle applicazioni

Eseguire attività amministrative e di configurazione

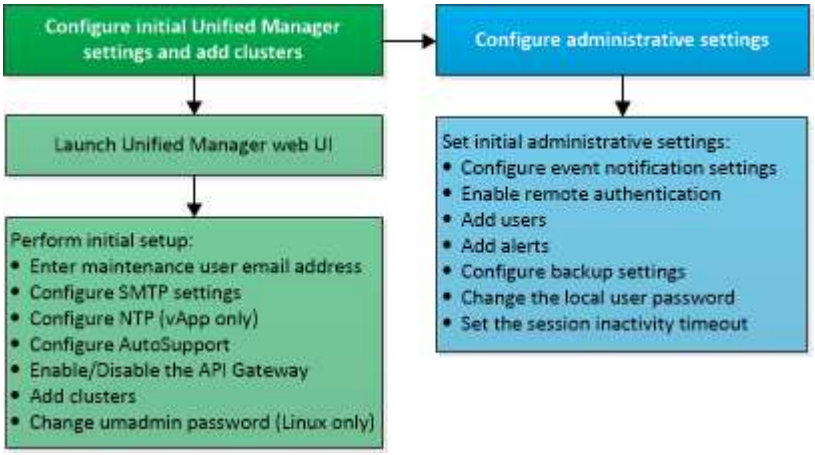
Configurazione di Active IQ Unified Manager

Dopo aver installato Active IQ Unified Manager (precedentemente noto come Gestore unificato di OnCommand), è necessario completare la configurazione iniziale (chiamata anche procedura guidata per la prima esperienza) per accedere all'interfaccia utente Web. È quindi possibile eseguire ulteriori attività di configurazione, ad esempio l'aggiunta di cluster, la configurazione dell'autenticazione remota, l'aggiunta di utenti e l'aggiunta di avvisi.

Alcune delle procedure descritte in questo manuale sono necessarie per completare la configurazione iniziale dell'istanza di Unified Manager. Altre procedure sono le impostazioni di configurazione consigliate che sono utili per la configurazione sulla nuova istanza o che sono utili prima di iniziare il monitoraggio regolare dei sistemi ONTAP.

Panoramica della sequenza di configurazione

Il flusso di lavoro di configurazione descrive le attività da eseguire prima di poter utilizzare Unified Manager.



Accesso all'interfaccia utente Web di Unified Manager

Dopo aver installato Unified Manager, è possibile accedere all'interfaccia utente Web per configurare Unified Manager in modo da poter iniziare il monitoraggio dei sistemi ONTAP.

Cosa ti serve

- Se si accede per la prima volta all'interfaccia utente Web, è necessario effettuare l'accesso come utente di manutenzione (o come utente umadmin per le installazioni Linux).
- Se si prevede di consentire agli utenti di accedere a Unified Manager utilizzando il nome breve invece di utilizzare il nome di dominio completo (FQDN) o l'indirizzo IP, la configurazione di rete deve risolvere questo nome breve in un FQDN valido.

- Se il server utilizza un certificato digitale autofirmato, il browser potrebbe visualizzare un avviso che indica che il certificato non è attendibile. È possibile riconoscere il rischio di continuare l'accesso o installare un certificato digitale firmato dall'autorità di certificazione (CA) per l'autenticazione del server.

Fasi

1. Avviare l'interfaccia utente Web di Unified Manager dal browser utilizzando l'URL visualizzato al termine dell'installazione. L'URL è l'indirizzo IP o FQDN (Fully Qualified Domain Name) del server Unified Manager.

   Il link è nel seguente formato: `https://URL`.

2. Accedere all'interfaccia utente Web di Unified Manager utilizzando le credenziali utente di manutenzione.

> Se si effettuano tre tentativi consecutivi di accesso all'interfaccia utente Web senza esito positivo entro un'ora, l'utente viene bloccato dal sistema e deve contattare l'amministratore di sistema. Questo è valido solo per gli utenti locali.

Esecuzione della configurazione iniziale dell'interfaccia utente Web di Unified Manager

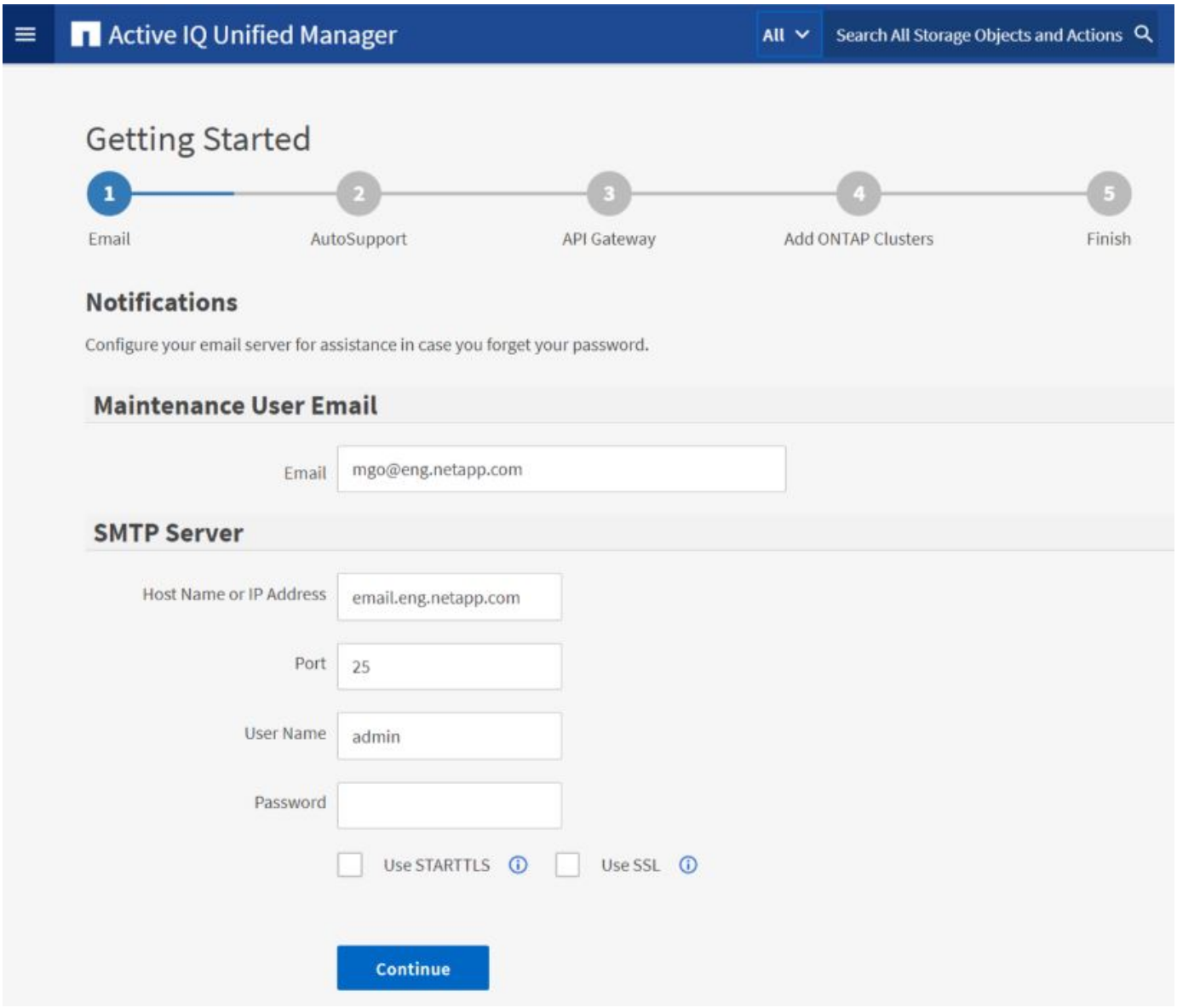
Per utilizzare Unified Manager, è necessario prima configurare le opzioni di configurazione iniziale, tra cui il server NTP, l'indirizzo e-mail dell'utente di manutenzione, l'host del server SMTP e l'aggiunta di cluster ONTAP.

Cosa ti serve

È necessario aver eseguito le seguenti operazioni:

- Ha avviato l'interfaccia utente Web di Unified Manager utilizzando l'URL fornito dopo l'installazione
- Accesso effettuato utilizzando il nome utente e la password di manutenzione (utente umadmin per installazioni Linux) creati durante l'installazione

La pagina Guida introduttiva di Active IQ Unified Managerviene visualizzata solo quando si accede per la prima volta all'interfaccia utente Web. La pagina riportata di seguito è tratta da un'installazione su VMware.



Se si desidera modificare una di queste opzioni in un secondo momento, è possibile selezionare una delle opzioni generali nel riquadro di navigazione sinistro di Unified Manager. Tenere presente che l'impostazione NTP è valida solo per le installazioni VMware e può essere modificata in un secondo momento utilizzando la console di manutenzione di Unified Manager.

Fasi

1. Nella pagina Configurazione iniziale di Active IQ Unified Manager, immettere l'indirizzo e-mail dell'utente di manutenzione, il nome host del server SMTP e le eventuali opzioni SMTP aggiuntive e il server NTP (solo installazioni VMware). Quindi fare clic su **continua**.

   Se è stata selezionata l'opzione **Use STARTTLS** or **Use SSL** (Usa STARTTLS* o **Use SSL**), dopo aver fatto clic sul pulsante **Continue** viene visualizzata una pagina di certificato. Verificare i dettagli del certificato e accettare il certificato per continuare con le impostazioni di configurazione iniziali dell'interfaccia utente Web.

2. Nella pagina AutoSupport, fare clic su **Accetto e continua** per abilitare l'invio di messaggi AutoSupport da Unified Manager a NetAppActive IQ.

   Se è necessario designare un proxy per fornire l'accesso a Internet per inviare contenuti AutoSupport o se

si desidera disattivare AutoSupport, utilizzare l'opzione **Generale** > **AutoSupport** dall'interfaccia utente Web.

3. Nei sistemi Red Hat e CentOS, modificare la password utente di umadmin dalla stringa predefinita "admin" a una stringa personalizzata.
4. Nella pagina Set up API Gateway (Configura gateway API), selezionare se si desidera utilizzare la funzione API Gateway che consente a Unified Manager di gestire i cluster ONTAP che si intende monitorare utilizzando le API REST di ONTAP. Quindi fare clic su **continua**.

   È possibile attivare o disattivare questa impostazione in un secondo momento nell'interfaccia utente Web da **Generale** > **Impostazioni delle funzioni** > **Gateway API**. Per ulteriori informazioni sulle API, vedere "Introduzione alle API REST di Active IQ Unified Manager".

5. Aggiungere i cluster che si desidera gestire con Unified Manager, quindi fare clic su **Avanti**. Per ogni cluster che si intende gestire, è necessario disporre del nome host o dell'indirizzo IP di gestione del cluster (IPv4 o IPv6) insieme alle credenziali del nome utente e della password. L'utente deve avere il ruolo "admin".

   Questo passaggio è facoltativo. È possibile aggiungere cluster in un secondo momento nell'interfaccia utente Web da **Storage Management** > **Cluster Setup**.

6. Nella pagina Summary (Riepilogo), verificare che tutte le impostazioni siano corrette e fare clic su **Finish** (fine).

La pagina Getting Started (Guida introduttiva) si chiude e viene visualizzata la pagina Unified Manager Dashboard.

Aggiunta di cluster

È possibile aggiungere un cluster a Active IQ Unified Manager in modo da poter monitorare il cluster. Ciò include la possibilità di ottenere informazioni sul cluster, come lo stato di salute, la capacità, le performance e la configurazione del cluster, in modo da individuare e risolvere eventuali problemi che potrebbero verificarsi.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario disporre delle seguenti informazioni:
  - Nome host o indirizzo IP di gestione del cluster

    Il nome host è l'FQDN o il nome breve utilizzato da Unified Manager per connettersi al cluster. Il nome host deve essere risolto nell'indirizzo IP di gestione del cluster.

    L'indirizzo IP di gestione del cluster deve essere la LIF di gestione del cluster della SVM (Administrative Storage Virtual Machine). Se si utilizza una LIF di gestione dei nodi, l'operazione non riesce.

  - Il cluster deve eseguire il software ONTAP versione 9.1 o superiore.
  - Nome utente e password dell'amministratore di ONTAP

    Questo account deve avere il ruolo *admin* con accesso applicazione impostato su *ontapi*, *console* e *http*.

- Il numero di porta per la connessione al cluster utilizzando il protocollo HTTPS (generalmente la porta 443).
- Si dispone dei certificati richiesti. Unified Manager installa i certificati di sicurezza quando si aggiunge un cluster:

  Certificati server: Questo certificato è di proprietà di Unified Manager. Un certificato SSL (HTTPS) autofirmato predefinito viene generato con una nuova installazione di Unified Manager. NetApp consiglia di eseguire l'upgrade al certificato firmato CA per una maggiore sicurezza. Se il certificato del server scade, è necessario rigenerarlo e riavviare Unified Manager affinché i servizi incorporino il nuovo certificato. Per ulteriori informazioni sulla rigenerazione del certificato SSL, vedere "Generazione di un certificato di protezione HTTPS".

  Certificati per la comunicazione TLS reciproca: Utilizzati durante la comunicazione TLS reciproca tra Unified Manager e ONTAP. L'autenticazione basata su certificato è abilitata per un cluster, in base alla versione di ONTAP. Se il cluster che esegue la versione di ONTAP è inferiore alla 9.5, l'autenticazione basata su certificato non viene attivata.

  L'autenticazione basata su certificato non viene attivata automaticamente per un cluster, se si aggiorna una versione precedente di Unified Manager a Unified Manager 9.12. Tuttavia, è possibile abilitarla modificando e salvando i dettagli del cluster. Se il certificato scade, è necessario rigenerarlo per incorporare il nuovo certificato. Per ulteriori informazioni sulla visualizzazione e la rigenerazione del certificato, vedere "Modifica dei cluster".

  - L'autenticazione basata su certificato viene attivata automaticamente se si aggiunge un cluster dall'interfaccia utente Web. Se si aggiunge un cluster dalla console di manutenzione, l'autenticazione basata su certificato non viene attivata.
  - Se l'autenticazione basata su certificato è abilitata per un cluster e si esegue il backup di Unified Manager da un server e si esegue il ripristino su un altro server Unified Manager in cui viene modificato il nome host o l'indirizzo IP, il monitoraggio del cluster potrebbe non riuscire. Per evitare il guasto, modificare e salvare i dettagli del cluster. Per ulteriori informazioni sulla modifica dei dettagli del cluster, vedere "Modifica dei cluster".

  +
  Certificati client: Utilizzati durante l'autenticazione per i messaggi EMS ricevuti da ONTAP. Questo certificato è di proprietà di ONTAP e viene richiesto quando si aggiunge un cluster ONTAP a Unified Manager. Non è possibile aggiungere un cluster a Unified Manager con un certificato scaduto e, se il certificato client è già scaduto, è necessario rigenerarlo prima di aggiungere il cluster. Tuttavia, se il certificato scade per un cluster già aggiunto e viene utilizzato da Unified Manager, la messaggistica EMS continua a funzionare con il certificato scaduto. Per informazioni sulla generazione dei certificati, consultare l'articolo della Knowledge base (KB) "Come rinnovare un certificato autofirmato ONTAP nell'interfaccia utente di System Manager".

- È necessario disporre di spazio sufficiente sul server Unified Manager. Non è possibile aggiungere un cluster al server quando più del 90% dello spazio nella directory del database è già occupato.

Per una configurazione MetroCluster, è necessario aggiungere i cluster locali e remoti e i cluster devono essere configurati correttamente.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Cluster Setup**.
2. Nella pagina Cluster Setup, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo Add Cluster (Aggiungi cluster), specificare i valori richiesti, ad esempio il nome

host o l'indirizzo IP del cluster, il nome utente, la password e il numero di porta.

È possibile modificare l'indirizzo IP di gestione del cluster da IPv6 a IPv4 o da IPv4 a IPv6. Il nuovo indirizzo IP viene visualizzato nella griglia del cluster e nella pagina di configurazione del cluster al termine del successivo ciclo di monitoraggio.

4. Fare clic su **Invia**.
5. Nella finestra di dialogo Authorize host (autorizza host), fare clic su **View Certificate** (Visualizza certificato) per visualizzare le informazioni sul certificato del cluster.
6. Fare clic su **Sì**.

   In Unified Manager 9.12, dopo aver salvato i dettagli del cluster, è possibile visualizzare il certificato per la comunicazione TLS reciproca per un cluster.

   Se l'autenticazione basata su certificato non è abilitata, Unified Manager controlla il certificato solo quando il cluster viene aggiunto inizialmente. Unified Manager non controlla il certificato per ogni chiamata API a ONTAP.

Una volta individuati tutti gli oggetti di un nuovo cluster, Unified Manager inizia a raccogliere dati storici sulle performance per i 15 giorni precedenti. Queste statistiche vengono raccolte utilizzando la funzionalità di raccolta della continuità dei dati. Questa funzionalità fornisce oltre due settimane di informazioni sulle performance per un cluster subito dopo l'aggiunta. Una volta completato il ciclo di raccolta della continuità dei dati, i dati delle performance del cluster in tempo reale vengono raccolti, per impostazione predefinita, ogni cinque minuti.

Dato che la raccolta di 15 giorni di dati sulle performance richiede un uso intensivo della CPU, si consiglia di eseguire l'aggiunta di nuovi cluster in modo che i sondaggi per la raccolta della continuità dei dati non vengano eseguiti su troppi cluster contemporaneamente. Inoltre, se si riavvia Unified Manager durante il periodo di raccolta della continuità dei dati, la raccolta viene interrotta e vengono visualizzate lacune nei grafici delle performance per il periodo di tempo mancante.

Se viene visualizzato un messaggio di errore che indica che non è possibile aggiungere il cluster, controllare se gli orologi sui due sistemi non sono sincronizzati e se la data di inizio del certificato HTTPS di Unified Manager è successiva alla data sul cluster. È necessario assicurarsi che gli orologi siano sincronizzati utilizzando NTP o un servizio simile.

Informazioni correlate

"Installazione di un certificato HTTPS firmato e restituito dalla CA"

Configurazione di Unified Manager per l'invio di notifiche di avviso

È possibile configurare Unified Manager in modo che invii notifiche che avvisano l'utente in merito a eventi nel proprio ambiente. Prima di poter inviare le notifiche, è necessario configurare diverse altre opzioni di Unified Manager.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Dopo aver implementato Unified Manager e aver completato la configurazione iniziale, è necessario

configurare l'ambiente in modo da attivare avvisi e generare messaggi e-mail di notifica o trap SNMP in base alla ricezione degli eventi.

Fasi

1. "Configurare le impostazioni di notifica degli eventi".

   Se si desidera inviare notifiche di avviso quando si verificano determinati eventi nell'ambiente, è necessario configurare un server SMTP e fornire un indirizzo e-mail da cui inviare la notifica di avviso. Se si desidera utilizzare i trap SNMP, è possibile selezionare tale opzione e fornire le informazioni necessarie.

2. "Abilitare l'autenticazione remota".

   Se si desidera che gli utenti LDAP o Active Directory remoti accedano all'istanza di Unified Manager e ricevano notifiche di avviso, è necessario attivare l'autenticazione remota.

3. "Aggiungere server di autenticazione".

   È possibile aggiungere server di autenticazione in modo che gli utenti remoti all'interno del server di autenticazione possano accedere a Unified Manager.

4. "Aggiungere utenti".

   È possibile aggiungere diversi tipi di utenti locali o remoti e assegnare ruoli specifici. Quando si crea un avviso, si assegna a un utente la ricezione delle notifiche.

5. "Aggiungere avvisi".

   Dopo aver aggiunto l'indirizzo e-mail per l'invio delle notifiche, aver aggiunto gli utenti per la ricezione delle notifiche, aver configurato le impostazioni di rete e configurato le opzioni SMTP e SNMP necessarie per l'ambiente, è possibile assegnare gli avvisi.

Configurazione delle impostazioni di notifica degli eventi

È possibile configurare Unified Manager in modo che invii notifiche di avviso quando viene generato un evento o quando viene assegnato un evento a un utente. È possibile configurare il server SMTP utilizzato per inviare l'avviso e impostare vari meccanismi di notifica, ad esempio le notifiche di avviso possono essere inviate come e-mail o trap SNMP.

Cosa ti serve

È necessario disporre delle seguenti informazioni:

- Indirizzo e-mail da cui viene inviata la notifica di avviso

  L'indirizzo e-mail viene visualizzato nel campo "da" nelle notifiche di avviso inviate. Se non è possibile recapitarlo per qualsiasi motivo, questo indirizzo e-mail viene utilizzato anche come destinatario per la posta non recapitabile.

- Nome host del server SMTP, nome utente e password per accedere al server
- Nome host o indirizzo IP dell'host di destinazione trap che riceverà il trap SNMP, oltre alla versione SNMP, alla porta trap in uscita, alla community e ad altri valori di configurazione SNMP richiesti

Per specificare più destinazioni di trap, separare ciascun host con una virgola. In questo caso, tutte le altre impostazioni SNMP, ad esempio versione e porta trap in uscita, devono essere le stesse per tutti gli host dell'elenco.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Notifiche**.
2. Nella pagina Notifiche, configurare le impostazioni appropriate.

   Note:

   - Se l'indirizzo da è pre-compilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", devi cambiarlo in un indirizzo e-mail reale e funzionante per assicurarti che tutte le notifiche e-mail siano inviate correttamente.
   - Se il nome host del server SMTP non può essere risolto, è possibile specificare l'indirizzo IP (IPv4 o IPv6) del server SMTP invece del nome host.
3. Fare clic su **Save** (Salva).
4. Se è stata selezionata l'opzione **Use STARTTLS** or **Use SSL** (Usa STARTTLS* o **Use SSL**), dopo aver fatto clic sul pulsante **Save** (Salva) viene visualizzata una pagina del certificato. Verificare i dettagli del certificato e accettare il certificato per salvare le impostazioni di notifica.

   Per visualizzare i dettagli del certificato, fare clic sul pulsante **View Certificate Details** (Visualizza dettagli certificato). Se il certificato esistente è scaduto, deselezionare la casella **Usa STARTTLS** o **Usa SSL**, salvare le impostazioni di notifica e selezionare nuovamente la casella **Usa STARTTLS** o **Usa SSL** per visualizzare un nuovo certificato.

Attivazione dell'autenticazione remota

È possibile attivare l'autenticazione remota in modo che il server Unified Manager possa comunicare con i server di autenticazione. Gli utenti del server di autenticazione possono accedere all'interfaccia grafica di Unified Manager per gestire i dati e gli oggetti di storage.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Il server Unified Manager deve essere connesso direttamente al server di autenticazione. È necessario disattivare tutti i client LDAP locali come SSSD (System Security Services Daemon) o NSLCD (Name Service LDAP Caching Daemon).

È possibile attivare l'autenticazione remota utilizzando Open LDAP o Active Directory. Se l'autenticazione remota è disattivata, gli utenti remoti non possono accedere a Unified Manager.

L'autenticazione remota è supportata su LDAP e LDAPS (Secure LDAP). Unified Manager utilizza 389 come porta predefinita per le comunicazioni non protette e 636 come porta predefinita per le comunicazioni protette.

Il certificato utilizzato per autenticare gli utenti deve essere conforme al formato X.509.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare la casella **Enable remote Authentication…** (attiva autenticazione remota…).
3. Nel campo Servizio di autenticazione, selezionare il tipo di servizio e configurare il servizio di autenticazione.

Per tipo di autenticazione…	Inserire le seguenti informazioni…
Active Directory	• Nome dell'amministratore del server di autenticazione in uno dei seguenti formati: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Utilizzando la notazione LDAP appropriata) • Password dell'amministratore • Nome distinto di base (utilizzando la notazione LDAP appropriata)
Aprire LDAP	• Nome distinto di binding (nella notazione LDAP appropriata) • Associare la password • Nome distinto di base

Se l'autenticazione di un utente di Active Directory richiede molto tempo o si verifica un timeout, il server di autenticazione probabilmente impiega molto tempo per rispondere. La disattivazione del supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione.

Se si seleziona l'opzione Usa connessione protetta per il server di autenticazione, Unified Manager comunica con il server di autenticazione utilizzando il protocollo SSL (Secure Sockets Layer).

4. **Opzionale:** aggiungere server di autenticazione e verificare l'autenticazione.
5. Fare clic su **Save** (Salva).

Disattivazione dei gruppi nidificati dall'autenticazione remota

Se l'autenticazione remota è attivata, è possibile disattivare l'autenticazione dei gruppi nidificati in modo che solo i singoli utenti e non i membri del gruppo possano autenticarsi in remoto in Unified Manager. È possibile disattivare i gruppi nidificati quando si desidera migliorare i tempi di risposta per l'autenticazione di Active Directory.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione.
- La disattivazione dei gruppi nidificati è applicabile solo quando si utilizza Active Directory.

La disattivazione del supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione. Se il supporto di gruppi nidificati è disattivato e se un gruppo remoto viene aggiunto a Unified

Manager, i singoli utenti devono essere membri del gruppo remoto per autenticarsi in Unified Manager.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare la casella **Disable Nested Group Lookup** (Disattiva ricerca gruppi nidificati).
3. Fare clic su **Save** (Salva).

Impostazione dei servizi di autenticazione

I servizi di autenticazione consentono l'autenticazione di utenti remoti o gruppi remoti in un server di autenticazione prima di fornire loro l'accesso a Unified Manager. È possibile autenticare gli utenti utilizzando servizi di autenticazione predefiniti (ad esempio Active Directory o OpenLDAP) o configurando il proprio meccanismo di autenticazione.

Cosa ti serve

- È necessario aver attivato l'autenticazione remota.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare uno dei seguenti servizi di autenticazione:

Se si seleziona…	Quindi…
Active Directory	a. Immettere il nome e la password dell'amministratore. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.
OpenLDAP	a. Immettere il nome distinto e la password di bind. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.

Se si seleziona…	Quindi…
Altri	a. Immettere il nome distinto e la password di bind. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**. c. Specificare la versione del protocollo LDAP supportata dal server di autenticazione. d. Immettere il nome utente, l'appartenenza al gruppo, il gruppo di utenti e gli attributi del membro.

Se si desidera modificare il servizio di autenticazione, è necessario eliminare tutti i server di autenticazione esistenti e aggiungere nuovi server di autenticazione.

3. Fare clic su **Save** (Salva).

Aggiunta di server di autenticazione

È possibile aggiungere server di autenticazione e abilitare l'autenticazione remota sul server di gestione in modo che gli utenti remoti all'interno del server di autenticazione possano accedere a Unified Manager.

Cosa ti serve

- Devono essere disponibili le seguenti informazioni:
  - Nome host o indirizzo IP del server di autenticazione
  - Numero di porta del server di autenticazione
- È necessario aver attivato l'autenticazione remota e configurato il servizio di autenticazione in modo che il server di gestione possa autenticare utenti o gruppi remoti nel server di autenticazione.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Se il server di autenticazione che si sta aggiungendo fa parte di una coppia ad alta disponibilità (ha) (utilizzando lo stesso database), è possibile aggiungere anche il server di autenticazione partner. Ciò consente al server di gestione di comunicare con il partner quando uno dei server di autenticazione non è raggiungibile.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Attivare o disattivare l'opzione **Usa connessione protetta**:

Se si desidera…	Quindi…
Abilitarlo	a. Selezionare l'opzione **Usa connessione protetta**. b. Nella sezione Authentication Servers (Server di autenticazione), fare clic su **Add** (Aggiungi) c. Nella finestra di dialogo Add Authentication Server (Aggiungi server di autenticazione), immettere il nome di autenticazione o l'indirizzo IP (IPv4 o IPv6) del server. d. Nella finestra di dialogo autorizza host, fare clic su Visualizza certificato. e. Nella finestra di dialogo Visualizza certificato, verificare le informazioni del certificato, quindi fare clic su **Chiudi**. f. Nella finestra di dialogo autorizza host, fare clic su **Sì**. Quando si attiva l'opzione **Usa autenticazione connessione sicura**, Unified Manager comunica con il server di autenticazione e visualizza il certificato. Unified Manager utilizza 636 come porta predefinita per comunicazioni sicure e il numero di porta 389 per comunicazioni non sicure.
Disattivarlo	a. Deselezionare l'opzione **Usa connessione protetta**. b. Nella sezione Authentication Servers (Server di autenticazione), fare clic su **Add** (Aggiungi) c. Nella finestra di dialogo Add Authentication Server (Aggiungi server di autenticazione), specificare il nome host o l'indirizzo IP (IPv4 o IPv6) del server e i dettagli della porta. d. Fare clic su **Aggiungi**.

Il server di autenticazione aggiunto viene visualizzato nell'area Server.

3. Eseguire un'autenticazione di prova per confermare che è possibile autenticare gli utenti nel server di autenticazione aggiunto.

Verifica della configurazione dei server di autenticazione

È possibile convalidare la configurazione dei server di autenticazione per garantire che il server di gestione sia in grado di comunicare con essi. È possibile convalidare la

configurazione ricercando un utente remoto o un gruppo remoto dai server di autenticazione e autenticandoli utilizzando le impostazioni configurate.

Cosa ti serve

- È necessario aver attivato l'autenticazione remota e configurato il servizio di autenticazione in modo che il server Unified Manager possa autenticare l'utente remoto o il gruppo remoto.
- È necessario aggiungere i server di autenticazione in modo che il server di gestione possa cercare l'utente remoto o il gruppo remoto da questi server e autenticarli.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Se il servizio di autenticazione è impostato su Active Directory e si sta convalidando l'autenticazione degli utenti remoti che appartengono al gruppo primario del server di autenticazione, le informazioni sul gruppo primario non vengono visualizzate nei risultati dell'autenticazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Fare clic su **Test Authentication**.
3. Nella finestra di dialogo Test User, specificare il nome utente e la password dell'utente remoto o il nome utente del gruppo remoto, quindi fare clic su **Test**.

   Se si sta autenticando un gruppo remoto, non è necessario immettere la password.

Aggiunta di avvisi

È possibile configurare gli avvisi in modo che notifichino quando viene generato un determinato evento. È possibile configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un particolare tipo di severità. È possibile specificare la frequenza con cui si desidera ricevere una notifica e associare uno script all'avviso.

Cosa ti serve

- Per consentire al server Active IQ Unified Manager di utilizzare queste impostazioni per inviare notifiche agli utenti quando viene generato un evento, è necessario aver configurato le impostazioni di notifica, ad esempio l'indirizzo e-mail dell'utente, il server SMTP e l'host trap SNMP.
- È necessario conoscere le risorse e gli eventi per i quali si desidera attivare l'avviso, nonché i nomi utente o gli indirizzi e-mail degli utenti che si desidera notificare.
- Se si desidera eseguire uno script in base all'evento, è necessario aggiungere lo script a Unified Manager utilizzando la pagina script.
- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a creare un avviso dalla pagina Configurazione avviso, come descritto di seguito.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina Alert Setup, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo Aggiungi avviso, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.

4. Fare clic su **risorse** e selezionare le risorse da includere o escludere dall'avviso.

   È possibile impostare un filtro specificando una stringa di testo nel campo **Nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse corrispondenti alla regola di filtro. La stringa di testo specificata fa distinzione tra maiuscole e minuscole.

   Se una risorsa è conforme alle regole di inclusione ed esclusione specificate, la regola di esclusione ha la precedenza sulla regola di inclusione e l'avviso non viene generato per gli eventi correlati alla risorsa esclusa.

5. Fare clic su **Eventi** e selezionare gli eventi in base al nome dell'evento o al tipo di severità per cui si desidera attivare un avviso.

   Per selezionare più eventi, premere il tasto Ctrl mentre si effettuano le selezioni.

6. Fare clic su **azioni**, selezionare gli utenti che si desidera notificare, scegliere la frequenza di notifica, scegliere se inviare una trap SNMP al ricevitore della trap e assegnare uno script da eseguire quando viene generato un avviso.

   Se si modifica l'indirizzo di posta elettronica specificato per l'utente e si riapre l'avviso per la modifica, il campo Nome appare vuoto perché l'indirizzo di posta elettronica modificato non è più associato all'utente precedentemente selezionato. Inoltre, se l'indirizzo e-mail dell'utente selezionato è stato modificato dalla pagina utenti, l'indirizzo e-mail modificato non viene aggiornato per l'utente selezionato.

   È inoltre possibile scegliere di inviare una notifica agli utenti tramite trap SNMP.

7. Fare clic su **Save** (Salva).

Esempio di aggiunta di un avviso

Questo esempio mostra come creare un avviso che soddisfi i seguenti requisiti:

- Nome avviso: HealthTest
- Risorse: Include tutti i volumi il cui nome contiene "abc" ed esclude tutti i volumi il cui nome contiene "xyz"
- Eventi: Include tutti gli eventi sanitari critici
- Azioni: Include "sample@domain.com", uno script "Test" e l'utente deve ricevere una notifica ogni 15 minuti

Nella finestra di dialogo Aggiungi avviso, attenersi alla seguente procedura:

Fasi

1. Fare clic su **Nome** e immettere **HealthTest** nel campo **Nome avviso**.
2. Fare clic su **Resources** (risorse) e nella scheda include (Includi) selezionare **Volumes** (volumi) dall'elenco a discesa.
   a. Immettere **abc** nel campo **Nome contiene** per visualizzare i volumi il cui nome contiene "abc".
   b. Selezionare **<<All Volumes whose name contains 'abc'>>** dall'area risorse disponibili e spostarla nell'area risorse selezionate.
   c. Fare clic su **Escludi**, immettere **xyz** nel campo **Nome contiene**, quindi fare clic su **Aggiungi**.
3. Fare clic su **Eventi** e selezionare **critico** dal campo gravità evento.

4. Selezionare **All Critical Events** (tutti gli eventi critici) dall'area Matching Events (Eventi corrispondenti) e spostarla nell'area Selected Events (Eventi selezionati).
5. Fare clic su **azioni** e digitare **sample@domain.com** nel campo Avvisa questi utenti.
6. Selezionare **promemoria ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

   È possibile configurare un avviso per inviare ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario determinare l'ora in cui la notifica dell'evento è attiva per l'avviso.

7. Nel menu Select script to Execute (Seleziona script da eseguire), selezionare **Test** script.
8. Fare clic su **Save** (Salva).

Modifica della password utente locale

È possibile modificare la password di accesso utente locale per evitare potenziali rischi per la sicurezza.

Cosa ti serve

Devi essere connesso come utente locale.

Le password per l'utente di manutenzione e per gli utenti remoti non possono essere modificate seguendo questa procedura. Per modificare la password di un utente remoto, contattare l'amministratore della password. Per modificare la password utente per la manutenzione, vedere "Utilizzando la console di manutenzione".

Fasi

1. Accedere a Unified Manager.
2. Dalla barra dei menu superiore, fare clic sull'icona dell'utente, quindi fare clic su **Change Password** (Modifica password).

   L'opzione **Change Password** (Modifica password) non viene visualizzata se si è utenti remoti.

3. Nella finestra di dialogo Change Password (Modifica password), immettere la password corrente e la nuova password.
4. Fare clic su **Save** (Salva).

Se Unified Manager è configurato in una configurazione ad alta disponibilità, è necessario modificare la password sul secondo nodo dell'installazione. Entrambe le istanze devono avere la stessa password.

Impostazione del timeout di inattività della sessione

È possibile specificare il valore di timeout di inattività per Unified Manager in modo che la sessione venga terminata automaticamente dopo un determinato periodo di tempo. Per impostazione predefinita, il timeout è impostato su 4,320 minuti (72 ore).

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Questa impostazione ha effetto su tutte le sessioni utente registrate.

Questa opzione non è disponibile se è stata attivata l'autenticazione SAML (Security Assertion Markup Language).

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Feature Settings**, specificare il timeout di inattività scegliendo una delle seguenti opzioni:

Se si desidera…	Quindi…
Non impostare alcun timeout in modo che la sessione non venga mai chiusa automaticamente	Nel pannello **Timeout inattività**, spostare il dispositivo di scorrimento verso sinistra (Off) e fare clic su **Apply** (Applica).
Impostare un numero specifico di minuti come valore di timeout	Nel pannello **Timeout inattività**, spostare il cursore a destra (on), specificare il valore del timeout di inattività in minuti e fare clic su **Applica**.

Modifica del nome host di Unified Manager

A un certo punto, potrebbe essere necessario modificare il nome host del sistema su cui è stato installato Unified Manager. Ad esempio, è possibile rinominare l'host per identificare più facilmente i server Unified Manager in base al tipo, al gruppo di lavoro o al gruppo di cluster monitorato.

I passaggi necessari per modificare il nome host variano a seconda che Unified Manager sia in esecuzione su un server VMware ESXi, Red Hat o CentOS Linux o Microsoft Windows.

Modifica del nome host dell'appliance virtuale Unified Manager

All'host di rete viene assegnato un nome quando l'appliance virtuale di Unified Manager viene implementata per la prima volta. È possibile modificare il nome host dopo l'implementazione. Se si modifica il nome host, è necessario rigenerare anche il certificato HTTPS.

Cosa ti serve

Per eseguire queste attività, è necessario essere connessi a Unified Manager come utente di manutenzione o avere il ruolo di amministratore dell'applicazione assegnato.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web di Unified Manager. Se durante l'implementazione è stato configurato un indirizzo IP statico per la rete, sarebbe stato designato un nome per l'host di rete. Se la rete è stata configurata utilizzando DHCP, il nome host deve essere preso dal DNS. Se DHCP o DNS non sono configurati correttamente, il nome host "Unified Manager" viene assegnato automaticamente e associato al certificato di protezione.

Indipendentemente dalla modalità di assegnazione del nome host, se si modifica il nome host e si intende utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario generare un nuovo certificato di protezione.

Se si accede all'interfaccia utente Web utilizzando l'indirizzo IP del server invece del nome host, non è

necessario generare un nuovo certificato se si modifica il nome host. Tuttavia, è consigliabile aggiornare il certificato in modo che il nome host del certificato corrisponda al nome host effettivo.

Se si modifica il nome host in Unified Manager, è necessario aggiornare manualmente il nome host in OnCommand Workflow Automation (Wfa). Il nome host non viene aggiornato automaticamente in WFA.

Il nuovo certificato non ha effetto fino al riavvio della macchina virtuale di Unified Manager.

Fasi

1. Generare un certificato di protezione HTTPS

   Se si desidera utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario rigenerare il certificato HTTPS per associarlo al nuovo nome host.

2. Riavviare la macchina virtuale di Unified Manager

   Dopo aver rigenerato il certificato HTTPS, è necessario riavviare la macchina virtuale di Unified Manager.

Generazione di un certificato di protezione HTTPS

Quando Active IQ Unified Manager viene installato per la prima volta, viene installato un certificato HTTPS predefinito. È possibile generare un nuovo certificato di protezione HTTPS che sostituisce il certificato esistente.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Possono esserci diversi motivi per rigenerare il certificato, ad esempio se si desidera ottenere valori migliori per Nome distinto (DN) o se si desidera una dimensione della chiave più elevata o un periodo di scadenza più lungo o se il certificato corrente è scaduto.

Se non si dispone dell'accesso all'interfaccia utente Web di Unified Manager, è possibile rigenerare il certificato HTTPS con gli stessi valori utilizzando la console di manutenzione. Durante la rigenerazione dei certificati, è possibile definire la dimensione della chiave e la durata della validità della chiave. Se si utilizza `Reset Server Certificate` Dalla console di manutenzione, viene creato un nuovo certificato HTTPS valido per 397 giorni. Questo certificato avrà una chiave RSA di 2048 bit.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.
2. Fare clic su **Rigenera certificato HTTPS**.

   Viene visualizzata la finestra di dialogo Rigenera certificato HTTPS.

3. Selezionare una delle seguenti opzioni a seconda della modalità di generazione del certificato:

Se si desidera…	Eseguire questa operazione…
Rigenera il certificato con i valori correnti	Fare clic sull'opzione **Rigenera using Current Certificate Attributes**.

Se si desidera…	Eseguire questa operazione…
Generare il certificato utilizzando valori diversi	Fare clic sull'opzione **Update the Current Certificate Attributes** (Aggiorna attributi del certificato corrente). I campi Nome comune e nomi alternativi utilizzano i valori del certificato esistente se non vengono immessi nuovi valori. Il campo "Common Name" deve essere impostato sull'FQDN dell'host. Gli altri campi non richiedono valori, ma è possibile inserire valori, ad esempio, per L'EMAIL, LA SOCIETÀ, IL REPARTO, Città, Stato e Paese se si desidera inserire tali valori nel certificato. È inoltre possibile selezionare una DELLE DIMENSIONI DELLA CHIAVE disponibili (l'algoritmo della chiave è "RSA"). E PERIODO di validità. • I valori consentiti per la dimensione della chiave sono `2048`, `3072` e. `4096`. • I periodi di validità vanno da un minimo di 1 giorno a un massimo di 36500 giorni. Anche se è consentito un periodo di validità di 36500 giorni, si consiglia di utilizzare un periodo di validità non superiore a 397 giorni o 13 mesi. Poiché se si seleziona un periodo di validità superiore a 397 giorni e si prevede di esportare una CSR per questo certificato e di ottenerla firmata da una CA nota, la validità del certificato firmato restituito dalla CA sarà ridotta a 397 giorni. • Selezionare la casella di controllo "Escludi informazioni di identificazione locali (ad es. Host locale)" se si desidera rimuovere le informazioni di identificazione locali dal campo dei nomi alternativi del certificato. Quando questa casella di controllo è selezionata, nel campo nomi alternativi viene utilizzato solo il valore immesso nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo di nomi alternativi.

4. Fare clic su **Sì** per rigenerare il certificato.
5. Riavviare il server Unified Manager in modo che il nuovo certificato abbia effetto.
6. Verificare le informazioni sul nuovo certificato visualizzando il certificato HTTPS.

Riavvio della macchina virtuale di Unified Manager

È possibile riavviare la macchina virtuale dalla console di manutenzione di Unified Manager. Riavviare dopo aver generato un nuovo certificato di protezione o in caso di problemi con la macchina virtuale.

Cosa ti serve

L'appliance virtuale è accesa.

Si è connessi alla console di manutenzione come utente di manutenzione.

È inoltre possibile riavviare la macchina virtuale da vSphere utilizzando l'opzione **Restart Guest**. Per ulteriori informazioni, consultare la documentazione di VMware.

Fasi

1. Accedere alla console di manutenzione.
2. Selezionare **Configurazione del sistema** > **riavvio della macchina virtuale**.

Modifica del nome host di Unified Manager sui sistemi Linux

A un certo punto, potrebbe essere necessario modificare il nome host della macchina Red Hat Enterprise Linux o CentOS su cui è stato installato Unified Manager. Ad esempio, è possibile rinominare l'host per identificare più facilmente i server Unified Manager in base al tipo, al gruppo di lavoro o al gruppo di cluster monitorato quando si elencano i computer Linux.

Cosa ti serve

È necessario disporre dell'accesso utente root al sistema Linux su cui è installato Unified Manager.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web di Unified Manager. Se durante l'implementazione è stato configurato un indirizzo IP statico per la rete, sarebbe stato designato un nome per l'host di rete. Se la rete è stata configurata utilizzando DHCP, il nome host deve essere preso dal server DNS.

Indipendentemente dalla modalità di assegnazione del nome host, se si modifica il nome host e si intende utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario generare un nuovo certificato di protezione.

Se si accede all'interfaccia utente Web utilizzando l'indirizzo IP del server invece del nome host, non è necessario generare un nuovo certificato se si modifica il nome host. Tuttavia, è consigliabile aggiornare il certificato in modo che il nome host del certificato corrisponda al nome host effettivo. Il nuovo certificato non ha effetto fino al riavvio della macchina Linux.

Se si modifica il nome host in Unified Manager, è necessario aggiornare manualmente il nome host in OnCommand Workflow Automation (Wfa). Il nome host non viene aggiornato automaticamente in WFA.

Fasi

1. Accedere come utente root al sistema Unified Manager che si desidera modificare.
2. Arrestare il software Unified Manager e il software MySQL associato immettendo il seguente comando:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Modificare il nome host utilizzando Linux `hostnamectl` comando:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Rigenerare il certificato HTTPS per il server:

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

5. Riavviare il servizio di rete:

   ```
   service network restart
   ```

6. Una volta riavviato il servizio, verificare se il nuovo nome host è in grado di eseguire il ping:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Questo comando dovrebbe restituire lo stesso indirizzo IP precedentemente impostato per il nome host originale.

7. Dopo aver completato e verificato la modifica del nome host, riavviare Unified Manager immettendo il seguente comando:

   ```
   systemctl start mysqld ocie ocieau
   ```

Attivazione e disattivazione della gestione dello storage basata su policy

A partire da Unified Manager 9.7, è possibile eseguire il provisioning dei carichi di lavoro dello storage (volumi e LUN) sui cluster ONTAP e gestire tali carichi di lavoro in base ai livelli di servizio delle performance assegnati. Questa funzionalità è simile alla creazione di carichi di lavoro in Gestione di sistema ONTAP e al collegamento di policy di qualità del servizio, ma se applicata con Gestione unificata è possibile eseguire il provisioning e la gestione dei carichi di lavoro in tutti i cluster monitorati dall'istanza di Gestione unificata.

È necessario disporre del ruolo di amministratore dell'applicazione.

Questa opzione è attivata per impostazione predefinita, ma è possibile disattivarla se non si desidera eseguire il provisioning e la gestione dei carichi di lavoro utilizzando Unified Manager.

Se attivata, questa opzione fornisce molti nuovi elementi nell'interfaccia utente:

Nuovi contenuti	Posizione
Una pagina per il provisioning di nuovi workload	Disponibile da **attività comuni** > **Provisioning**
Una pagina per creare policy sui livelli di servizio per le performance	Disponibile in **Impostazioni** > **politiche** > **livelli di servizio delle performance**
Una pagina per creare policy di efficienza dello storage per le performance	Disponibile in **Impostazioni** > **politiche** > **efficienza dello storage**
Pannelli che descrivono gli IOPS correnti relativi a workload Performance e workload	Disponibile nella dashboard

Per ulteriori informazioni su queste pagine e su questa funzionalità, consultare la guida in linea del prodotto.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Feature Settings**, disattivare o attivare la gestione dello storage basata su policy scegliendo una delle seguenti opzioni:

Se si desidera…	Quindi…
Disattiva la gestione dello storage basata su policy	Nel pannello **Policy-based storage management** (Gestione dello storage basata su policy), spostare il pulsante di scorrimento verso sinistra.
Gestione dello storage basata su policy	Nel pannello **Policy-based storage management** (Gestione dello storage basata su policy), spostare il pulsante di scorrimento verso destra.

Configurazione del backup di Unified Manager

È possibile configurare la funzionalità di backup su Unified Manager attraverso una serie di procedure di configurazione da eseguire sui sistemi host e sulla console di manutenzione.

Per informazioni sulla procedura di configurazione, vedere "Gestione delle operazioni di backup e ripristino".

Gestione delle impostazioni delle funzioni

La pagina Impostazioni funzionalità consente di attivare e disattivare funzioni specifiche in Active IQ Unified Manager. Ciò include la creazione e la gestione di oggetti di storage in base a policy, l'abilitazione del gateway API e del banner di accesso, il caricamento di script per la gestione degli avvisi, il timeout di una sessione dell'interfaccia utente Web in base al tempo di inattività e la disattivazione della ricezione degli eventi della piattaforma Active IQ.

La pagina Feature Settings (Impostazioni funzionalità) è disponibile solo per gli utenti con ruolo di amministratore dell'applicazione.

Per informazioni sul caricamento degli script, vedere "Attivazione e disattivazione del caricamento degli script".

Gestione dello storage basata su policy

L'opzione **Gestione dello storage basata su policy** consente la gestione dello storage in base agli obiettivi del livello di servizio (SLO). Questa opzione è attivata per impostazione predefinita.

Attivando questa funzionalità, è possibile eseguire il provisioning dei carichi di lavoro dello storage sui cluster ONTAP aggiunti alla propria istanza di Active IQ Unified Manager e gestire questi carichi di lavoro in base ai livelli di servizio delle performance assegnati e alle policy di efficienza dello storage.

Puoi scegliere di attivare o disattivare questa funzione da **Generale** > **Impostazioni funzionalità** > **Gestione dello storage basata su policy**. All'attivazione di questa funzione, sono disponibili le seguenti pagine per il funzionamento e il monitoraggio:

- Provisioning (provisioning del carico di lavoro dello storage)
- **Policy** > **Performance Service level**
- **Criteri** > **efficienza dello storage**
- Workload gestiti da Performance Service Level nella pagina Clusters Setup
- Pannello delle performance del carico di lavoro sul pannello **Dashboard**

È possibile utilizzare le schermate per creare livelli di servizio delle performance e policy di efficienza dello storage e per eseguire il provisioning dei carichi di lavoro dello storage. È inoltre possibile monitorare i carichi di lavoro dello storage conformi ai livelli di Performance Service assegnati, nonché quelli non conformi. Il pannello Workload Performance and workload IOPS (IOPS workload Performance e workload IOPS) consente inoltre di valutare la capacità e le performance totali, disponibili e utilizzate dei cluster nel data center in base ai carichi di lavoro storage su di essi forniti.

Dopo aver attivato questa funzione, è possibile eseguire le API REST di Unified Manager per eseguire alcune di queste funzioni dalla **barra dei menu** > **pulsante della Guida** > **documentazione API** > **categoria storage-provider**. In alternativa, è possibile inserire il nome host o l'indirizzo IP e l'URL per accedere alla pagina API REST nel formato https://<hostname>/docs/api/

Per ulteriori informazioni sulle API, vedere "Introduzione alle API REST di Active IQ Unified Manager".

Abilitazione di API Gateway

La funzione gateway API consente a Active IQ Unified Manager di essere un singolo piano di controllo da cui è possibile gestire più cluster ONTAP, senza dover effettuare l'accesso singolarmente.

È possibile attivare questa funzione dalle pagine di configurazione visualizzate quando si accede per la prima volta a Unified Manager. In alternativa, è possibile attivare o disattivare questa funzione da **Generale** > **Impostazioni funzionalità** > **Gateway API**.

Le API REST di Unified Manager sono diverse dalle API REST di ONTAP e non tutte le funzionalità delle API REST di ONTAP possono essere utilizzate utilizzando le API REST di Unified Manager. Tuttavia, se si dispone

di un requisito di business specifico per l'accesso alle API di ONTAP per la gestione di funzionalità specifiche non esposte a Unified Manager, è possibile attivare la funzione di gateway API ed eseguire le API di ONTAP. Il gateway funge da proxy per il tunneling delle richieste API mantenendo le richieste di intestazione e corpo nello stesso formato delle API ONTAP. È possibile utilizzare le credenziali di Unified Manager ed eseguire le API specifiche per accedere e gestire i cluster ONTAP senza passare le credenziali dei singoli cluster. Unified Manager funziona come un singolo punto di gestione per l'esecuzione delle API nei cluster ONTAP gestiti dall'istanza di Unified Manager. La risposta restituita dalle API è la stessa della risposta restituita dalle rispettive API REST ONTAP eseguite direttamente da ONTAP.

Dopo aver attivato questa funzione, è possibile eseguire le API REST di Unified Manager da **barra dei menu** > **pulsante della Guida** > **documentazione API** > **gateway** categoria. In alternativa, è possibile inserire il nome host o l'indirizzo IP e l'URL per accedere alla pagina API REST nel formato `https://<hostname>/docs/api/`

Per ulteriori informazioni sulle API, vedere "Introduzione alle API REST di Active IQ Unified Manager".

Specifica del timeout di inattività

È possibile specificare il valore di timeout di inattività per Active IQ Unified Manager. Dopo un periodo di inattività pari al tempo specificato, l'applicazione viene disconnessa automaticamente. Questa opzione è attivata per impostazione predefinita.

È possibile disattivare questa funzione o modificare l'ora da **Generale** > **Impostazioni funzionalità** > **Timeout inattività**. Una volta attivata questa funzione, specificare il limite di tempo di inattività (in minuti) nel campo **DISCONNETTI DOPO**, dopodiché il sistema si disconnette automaticamente. Il valore predefinito è 4320 minuti (72 ore).

Questa opzione non è disponibile se è stata attivata l'autenticazione SAML (Security Assertion Markup Language).

Attivazione degli eventi del portale Active IQ

È possibile specificare se si desidera attivare o disattivare gli eventi del portale Active IQ. Questa impostazione consente al portale Active IQ di rilevare e visualizzare eventi aggiuntivi relativi alla configurazione del sistema, al cablaggio e così via. Questa opzione è attivata per impostazione predefinita.

Attivando questa funzione, Active IQ Unified Manager visualizza gli eventi rilevati dal portale Active IQ. Questi eventi vengono creati eseguendo una serie di regole per i messaggi AutoSupport generati da tutti i sistemi di storage monitorati. Questi eventi sono diversi dagli altri eventi di Unified Manager e identificano incidenti o rischi correlati a problemi di configurazione del sistema, cablaggio, Best practice e disponibilità.

Puoi scegliere di attivare o disattivare questa funzione da **Generale** > **Impostazioni funzionalità** > **Eventi portale Active IQ**. Nei siti senza accesso alla rete esterna, è necessario caricare manualmente le regole da **Storage Management** > **Event Setup** > **Upload Rules**.

Questa funzione è attivata per impostazione predefinita. La disattivazione di questa funzione impedisce il rilevamento o la visualizzazione degli eventi Active IQ in Unified Manager. Se disattivata, questa funzione consente a Unified Manager di ricevere gli eventi Active IQ su un cluster a un'ora predefinita di 00:15 per quel fuso orario del cluster.

Attivazione e disattivazione delle impostazioni di sicurezza per la conformità

Utilizzando il pulsante **Customize** (Personalizza) nel pannello **Security Dashboard** della pagina Features Settings (Impostazioni funzionalità), è possibile attivare o disattivare i parametri di sicurezza per il monitoraggio della conformità in Unified Manager.

Le impostazioni attivate o disattivate in questa pagina regolano lo stato di conformità generale dei cluster e delle VM di storage su Unified Manager. In base alle selezioni, le colonne corrispondenti sono visibili nella vista **sicurezza: Tutti i cluster** della pagina di inventario dei cluster e nella vista **sicurezza: Tutte le macchine virtuali di storage** della pagina di inventario delle macchine virtuali di storage.

Solo gli utenti con ruolo di amministratore possono modificare queste impostazioni.

I criteri di sicurezza per i cluster ONTAP, le VM di storage e i volumi vengono valutati in base alle raccomandazioni definite nella "Guida al rafforzamento della sicurezza per NetApp ONTAP 9". Il pannello Security (sicurezza) della dashboard e la pagina Security (sicurezza) visualizzano lo stato di conformità di sicurezza predefinito di cluster, storage VM e volumi. Vengono inoltre generati eventi di sicurezza e attivate azioni di gestione per i cluster e le VM di storage che presentano violazioni della sicurezza.

Personalizzazione delle impostazioni di sicurezza

Per personalizzare le impostazioni per il monitoraggio della conformità in base all'ambiente ONTAP in uso, attenersi alla seguente procedura:

Fasi

1. Fare clic su **General > Feature Settings > Security Dashboard > Customize** (Generale > Impostazioni funzionalità > pannello di protezione > Personalizza) Viene visualizzata la finestra a comparsa **Customize Security Dashboard Settings** (Personalizza impostazioni dashboard di protezione).

   I parametri di conformità della sicurezza che si abilitano o disabilitano possono influire direttamente sulle viste di sicurezza predefinite, sui report e sui report pianificati nelle schermate Clusters e Storage VM. Se è stato caricato un report excel da queste schermate prima di modificare i parametri di sicurezza, i report excel scaricati potrebbero essere errati.

2. Per attivare o disattivare le impostazioni personalizzate per i cluster ONTAP, selezionare l'impostazione generale richiesta in **cluster**. Per informazioni sulle opzioni di personalizzazione della conformità del cluster, vedere "Categorie di compliance del cluster".
3. Per attivare o disattivare le impostazioni personalizzate per le VM di storage, selezionare l'impostazione generale richiesta in **Storage VM**. Per informazioni sulle opzioni di personalizzazione della conformità delle macchine virtuali dello storage, vedere "Categorie di conformità delle VM di storage".

Personalizzazione delle impostazioni di autenticazione e AutoSupport

Nella sezione **Impostazioni AutoSupport**, è possibile specificare se utilizzare il trasporto HTTPS per l'invio di messaggi AutoSupport da ONTAP.

Dalla sezione **Impostazioni di autenticazione**, è possibile attivare gli avvisi di Unified Manager per l'utente amministratore ONTAP predefinito.

Attivazione e disattivazione del caricamento degli script

Per impostazione predefinita, è attivata la possibilità di caricare gli script in Unified Manager ed eseguirli. Se l'organizzazione non desidera consentire questa attività per motivi di sicurezza, è possibile disattivare questa funzionalità.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Impostazioni funzionalità**, disattivare o attivare lo scripting scegliendo una delle seguenti opzioni:

Se si desidera…	Quindi…
Disattivare gli script	Nel pannello **script Upload**, spostare il cursore verso sinistra.
Abilitare gli script	Nel pannello **script Upload**, spostare il cursore verso destra.

Aggiunta banner di accesso

L'aggiunta di un banner di accesso consente all'organizzazione di visualizzare qualsiasi informazione, ad esempio chi ha accesso al sistema e i termini e le condizioni di utilizzo durante l'accesso e la disconnessione.

Qualsiasi utente, ad esempio gli operatori di storage o gli amministratori, può visualizzare questa finestra a comparsa del banner di accesso durante l'accesso, la disconnessione e il timeout della sessione.

Utilizzando la console di manutenzione

È possibile utilizzare la console di manutenzione per configurare le impostazioni di rete, configurare e gestire il sistema su cui è installato Unified Manager ed eseguire altre attività di manutenzione che consentono di prevenire e risolvere eventuali problemi.

Quali funzionalità offre la console di manutenzione

La console di manutenzione di Unified Manager consente di mantenere le impostazioni del sistema Unified Manager e di apportare le modifiche necessarie per evitare che si verifichino problemi.

A seconda del sistema operativo su cui è stato installato Unified Manager, la console di manutenzione offre le seguenti funzioni:

- Risolvere eventuali problemi relativi all'appliance virtuale, in particolare se l'interfaccia Web di Unified

Manager non è disponibile

- Eseguire l'aggiornamento alle versioni più recenti di Unified Manager
- Generare pacchetti di supporto da inviare al supporto tecnico
- Configurare le impostazioni di rete
- Modificare la password utente per la manutenzione
- Connettersi a un provider di dati esterno per inviare statistiche sulle prestazioni
- Modificare la raccolta di dati sulle performance interna
- Ripristinare il database e le impostazioni di configurazione di Unified Manager da una versione precedentemente sottoposta a backup.

Cosa fa l'utente che effettua la manutenzione

L'utente di manutenzione viene creato durante l'installazione di Unified Manager su un sistema Red Hat Enterprise Linux o CentOS. Il nome utente per la manutenzione è l'utente "umadmin". L'utente di manutenzione ha il ruolo di amministratore dell'applicazione nell'interfaccia utente Web e può creare utenti successivi e assegnarli ruoli.

L'utente di manutenzione, o umadmin, può anche accedere alla console di manutenzione di Unified Manager.

Funzionalità diagnostiche per l'utente

Lo scopo dell'accesso diagnostico è quello di consentire al supporto tecnico di fornire assistenza nella risoluzione dei problemi e utilizzarlo solo quando richiesto dal supporto tecnico.

L'utente della diagnostica può eseguire comandi a livello di sistema operativo quando richiesto dal supporto tecnico, a scopo di risoluzione dei problemi.

Accesso alla console di manutenzione

Se l'interfaccia utente di Unified Manager non è in funzione o se è necessario eseguire funzioni non disponibili nell'interfaccia utente, è possibile accedere alla console di manutenzione per gestire il sistema Unified Manager.

Cosa ti serve

Unified Manager deve essere installato e configurato.

Dopo 15 minuti di inattività, la console di manutenzione si disconnette.

> Una volta installato su VMware, se si è già effettuato l'accesso come utente di manutenzione tramite la console VMware, non è possibile effettuare l'accesso simultaneo utilizzando Secure Shell.

Fase

1. Per accedere alla console di manutenzione, procedere come segue:

Su questo sistema operativo…	Attenersi alla procedura descritta di seguito…
VMware	a. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo dell'appliance virtuale Unified Manager. b. Accedere alla console di manutenzione utilizzando il nome utente e la password di manutenzione.
Linux	a. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo del sistema Unified Manager. b. Accedere al sistema con il nome utente di manutenzione (umadmin) e la password. c. Immettere il comando `maintenance_console` E premere Invio.
Windows	a. Accedere al sistema Unified Manager con le credenziali di amministratore. b. Avviare PowerShell come amministratore di Windows. c. Immettere il comando `maintenance_console` E premere Invio.

Viene visualizzato il menu della console di manutenzione di Unified Manager.

Accesso alla console di manutenzione mediante la console vSphere VM

Se l'interfaccia utente di Unified Manager non è in funzione o se è necessario eseguire funzioni non disponibili nell'interfaccia utente, è possibile accedere alla console di manutenzione per riconfigurare l'appliance virtuale.

Cosa ti serve

- È necessario essere l'utente che esegue la manutenzione.
- L'appliance virtuale deve essere accesa per accedere alla console di manutenzione.

Fasi

1. In vSphere Client, individuare l'appliance virtuale Unified Manager.
2. Fare clic sulla scheda **Console**.
3. Fare clic all'interno della finestra della console per accedere.
4. Accedere alla console di manutenzione utilizzando il nome utente e la password.

   Dopo 15 minuti di inattività, la console di manutenzione si disconnette.

Menu della console di manutenzione

La console di manutenzione è composta da diversi menu che consentono di gestire e gestire funzioni speciali e impostazioni di configurazione del server Unified Manager.

A seconda del sistema operativo su cui è stato installato Unified Manager, la console di manutenzione è composta dai seguenti menu:

- Upgrade di Unified Manager (solo VMware)
- Configurazione di rete (solo VMware)
- Configurazione del sistema (solo VMware)
  a. Supporto/Diagnostica
  b. Reimposta certificato server
  c. Provider di dati esterno
  d. Backup Restore (Ripristino backup
  e. Configurazione dell'intervallo di polling delle performance
  f. Disattiva l'autenticazione SAML
  g. Visualizzare/modificare le porte dell'applicazione
  h. Configurazione del registro di debug
  i. Controlla l'accesso alla porta MySQL 3306
  j. Esci

Selezionare il numero dall'elenco per accedere all'opzione di menu specifica. Ad esempio, per il backup e il ripristino, selezionare *4*.

Menu Network Configuration (Configurazione di rete)

Il menu Configurazione di rete consente di gestire le impostazioni di rete. Utilizzare questo menu quando l'interfaccia utente di Unified Manager non è disponibile.

Questo menu non è disponibile se Unified Manager è installato su Red Hat Enterprise Linux, CentOS o Microsoft Windows.

Sono disponibili le seguenti opzioni di menu.

- **Visualizza impostazioni indirizzo IP**

  Visualizza le impostazioni di rete correnti per l'appliance virtuale, inclusi indirizzo IP, rete, indirizzo di trasmissione, netmask, gateway, E server DNS.

- **Modifica delle impostazioni dell'indirizzo IP**

  Consente di modificare le impostazioni di rete dell'appliance virtuale, inclusi l'indirizzo IP, la netmask, il gateway o i server DNS. Se si passa dalle impostazioni di rete DHCP alle reti statiche utilizzando la console di manutenzione, non è possibile modificare il nome host. Per apportare le modifiche, selezionare **Conferma modifiche**.

- **Visualizza impostazioni di ricerca nome dominio**

Visualizza l'elenco di ricerca dei nomi di dominio utilizzato per risolvere i nomi host.

- **Modifica impostazioni di ricerca nome dominio**

  Consente di modificare i nomi di dominio di cui si desidera eseguire la ricerca durante la risoluzione dei nomi host. Per apportare le modifiche, selezionare **Conferma modifiche**.

- **Visualizza percorsi statici**

  Visualizza i percorsi di rete statici correnti.

- **Modifica percorsi statici**

  Consente di aggiungere o eliminare percorsi di rete statici. Per apportare le modifiche, selezionare **Conferma modifiche**.

  - **Aggiungi percorso**

    Consente di aggiungere un percorso statico.

  - **Elimina percorso**

    Consente di eliminare un percorso statico.

  - **Indietro**

    Consente di tornare al **Menu principale**.

  - **Esci**

    Consente di uscire dalla console di manutenzione.

- **Disattiva interfaccia di rete**

  Disattiva tutte le interfacce di rete disponibili. Se è disponibile una sola interfaccia di rete, non è possibile disattivarla. Per apportare le modifiche, selezionare **Conferma modifiche**.

- **Attiva interfaccia di rete**

  Abilita le interfacce di rete disponibili. Per apportare le modifiche, selezionare **Conferma modifiche**.

- **Conferma modifiche**

  Applica le modifiche apportate alle impostazioni di rete dell'appliance virtuale. È necessario selezionare questa opzione per applicare le modifiche apportate, altrimenti le modifiche non si verificano.

- **Ping di un host**

  Esegue il ping di un host di destinazione per confermare le modifiche dell'indirizzo IP o le configurazioni DNS.

- **Ripristina impostazioni predefinite**

  Ripristina tutte le impostazioni predefinite. Per apportare le modifiche, selezionare **Conferma modifiche**.

- **Indietro**

Consente di tornare al **Menu principale**.

- **Esci**

  Consente di uscire dalla console di manutenzione.

Menu Configurazione di sistema

Il menu System Configuration (Configurazione di sistema) consente di gestire l'appliance virtuale fornendo varie opzioni, ad esempio la visualizzazione dello stato del server, il riavvio e l'arresto della macchina virtuale.

> Quando Unified Manager è installato su un sistema Linux o Microsoft Windows, da questo menu è disponibile solo l'opzione "Restore from a Unified Manager Backup" (Ripristina da un backup di Unified Manager).

Sono disponibili le seguenti opzioni di menu:

- **Visualizza stato server**

  Visualizza lo stato corrente del server. Le opzioni di stato includono in esecuzione e non in esecuzione.

  Se il server non è in esecuzione, potrebbe essere necessario contattare il supporto tecnico.

- **Riavviare la macchina virtuale**

  Riavvia la macchina virtuale, interrompendo tutti i servizi. Dopo il riavvio, la macchina virtuale e i servizi vengono riavviati.

- **Spegnere la macchina virtuale**

  Arresta la macchina virtuale, interrompendo tutti i servizi.

  È possibile selezionare questa opzione solo dalla console della macchina virtuale.

- **Modifica password utente <logged in user>**

  Modifica la password dell'utente attualmente connesso, che può essere solo l'utente di manutenzione.

- **Aumentare le dimensioni del disco dati**

  Aumenta le dimensioni del disco dati (disco 3) nella macchina virtuale.

- **Aumentare le dimensioni del disco di swap**

  Aumenta le dimensioni del disco di swap (disco 2) nella macchina virtuale.

- **Modifica fuso orario**

  Consente di modificare il fuso orario in base alla posizione.

- **Cambia server NTP**

  Modifica le impostazioni del server NTP, ad esempio l'indirizzo IP o il nome di dominio completo (FQDN).

- **Cambia servizio NTP**

  Consente di passare da `ntp` e. `systemd-timesyncd` servizi.

- **Ripristino da un backup di Unified Manager**

  Ripristina il database e le impostazioni di configurazione di Unified Manager da una versione precedentemente sottoposta a backup.

- **Ripristina certificato server**

  Ripristina il certificato di sicurezza del server.

- **Modifica nome host**

  Modifica il nome dell'host su cui è installata l'appliance virtuale.

- **Indietro**

  Consente di uscire dal menu Configurazione di sistema e tornare al menu principale.

- **Esci**

  Consente di uscire dal menu della console di manutenzione.

Menu Support and Diagnostics (supporto e diagnostica)

Il menu Support and Diagnostics (supporto e diagnostica) consente di generare un pacchetto di supporto che è possibile inviare al supporto tecnico per ottenere assistenza per la risoluzione dei problemi.

Sono disponibili le seguenti opzioni di menu:

- **Genera bundle di supporto leggero**

  Consente di produrre un bundle di supporto leggero che contiene solo 30 giorni di registri e record del database di configurazione, escludendo i dati sulle performance, i file di registrazione dell'acquisizione e il dump dell'heap del server.

- **Genera bundle di supporto**

  Consente di creare un bundle di supporto completo (file 7-zip) contenente informazioni diagnostiche nella home directory dell'utente di diagnostica. Se il sistema è connesso a Internet, è anche possibile caricare il pacchetto di supporto su NetApp.

  Il file include le informazioni generate da un messaggio AutoSupport, il contenuto del database di Unified Manager, i dati dettagliati sugli interni del server di Unified Manager e i registri a livello dettagliato non normalmente inclusi nei messaggi AutoSupport o nel bundle di supporto leggero.

Opzioni di menu aggiuntive

Le seguenti opzioni di menu consentono di eseguire varie attività amministrative sul server Unified Manager.

Sono disponibili le seguenti opzioni di menu:

- **Ripristina certificato server**

  Rigenera il certificato del server HTTPS.

  È possibile rigenerare il certificato del server nella GUI di Unified Manager facendo clic su **Generale** > **certificati HTTPS** > **Rigenera certificato HTTPS**.

- **Disattiva autenticazione SAML**

  Disattiva l'autenticazione SAML in modo che il provider di identità (IdP) non fornisca più l'autenticazione di accesso per gli utenti che accedono alla GUI di Unified Manager. Questa opzione della console viene generalmente utilizzata quando un problema con il server IdP o la configurazione SAML impedisce agli utenti di accedere alla GUI di Unified Manager.

- **Fornitore di dati esterno**

  Fornisce opzioni per la connessione di Unified Manager a un provider di dati esterno. Una volta stabilita la connessione, i dati delle performance vengono inviati a un server esterno in modo che gli esperti delle performance dello storage possano tracciare le metriche delle performance utilizzando software di terze parti. Vengono visualizzate le seguenti opzioni:

  - **Display Server Configuration**-: Visualizza le impostazioni di connessione e configurazione correnti per un provider di dati esterno.
  - **Aggiungi / Modifica connessione server**--consente di inserire nuove impostazioni di connessione per un provider di dati esterno o di modificare le impostazioni esistenti.
  - **Modifica configurazione server**--consente di inserire nuove impostazioni di configurazione per un provider di dati esterno o di modificare le impostazioni esistenti.
  - **Delete Server Connection**--Elimina la connessione a un provider di dati esterno.

    Una volta eliminata la connessione, Unified Manager perde la connessione al server esterno.

- **Backup Restore**

  Per ulteriori informazioni, consultare gli argomenti della sezione "Gestione delle operazioni di backup e ripristino".

- **Configurazione dell'intervallo di polling delle prestazioni**

  Fornisce un'opzione per configurare la frequenza con cui Unified Manager raccoglie i dati statistici delle performance dai cluster. L'intervallo di raccolta predefinito è di 5 minuti.

  È possibile modificare questo intervallo in 10 o 15 minuti se si scopre che le raccolte di cluster di grandi dimensioni non vengono completate in tempo.

- **Visualizza/Modifica porte applicazione**

  Fornisce un'opzione per modificare le porte predefinite utilizzate da Unified Manager per i protocolli HTTP e HTTPS, se necessario per motivi di sicurezza. Le porte predefinite sono 80 per HTTP e 443 per HTTPS.

- **Controlla l'accesso alla porta MySQL 3306**

  Controlla l'accesso degli host alla porta MySQL predefinita 3306. Per motivi di sicurezza, l'accesso tramite

questa porta è limitato solo all'host locale durante una nuova installazione di Unified Manager su sistemi Linux, Windows e VMware vSphere. Questa opzione consente di alternare la visibilità di questa porta tra l'host locale e gli host remoti, vale a dire che se è abilitata per l'host locale solo nel proprio ambiente, è possibile rendere questa porta disponibile anche agli host remoti. In alternativa, se attivata per tutti gli host, è possibile limitare l'accesso a questa porta solo a localhost. Se l'accesso era stato precedentemente attivato sugli host remoti, la configurazione viene mantenuta in uno scenario di aggiornamento.

- **Esci**

  Consente di uscire dal menu della console di manutenzione.

Modifica della password utente per la manutenzione in Windows

Se necessario, è possibile modificare la password utente per la manutenzione di Unified Manager.

Fasi

1. Dalla pagina di accesso all'interfaccia utente Web di Unified Manager, fare clic su **Password dimenticata**.

   Viene visualizzata una pagina che richiede il nome dell'utente di cui si desidera reimpostare la password.

2. Inserire il nome utente e fare clic su **Submit** (Invia).

   Un'e-mail con un collegamento per reimpostare la password viene inviata all'indirizzo e-mail definito per tale nome utente.

3. Fare clic sul collegamento **reset password** nell'e-mail e definire la nuova password.
4. Tornare all'interfaccia utente Web e accedere a Unified Manager utilizzando la nuova password.

Modifica della password di umadmin sui sistemi Linux

Per motivi di sicurezza, è necessario modificare la password predefinita per l'utente di Unified Manager umadmin subito dopo aver completato il processo di installazione. Se necessario, è possibile modificare nuovamente la password in un secondo momento.

Cosa ti serve

- Unified Manager deve essere installato su un sistema Red Hat Enterprise Linux o CentOS Linux.
- È necessario disporre delle credenziali utente root per il sistema Linux su cui è installato Unified Manager.

Fasi

1. Accedere come utente root al sistema Linux su cui è in esecuzione Unified Manager.
2. Modificare la password di umadmin:

   ```
   passwd umadmin
   ```

   Il sistema richiede di inserire una nuova password per l'utente umadmin.

Modifica delle porte utilizzate da Unified Manager per i protocolli HTTP e HTTPS

Le porte predefinite utilizzate da Unified Manager per i protocolli HTTP e HTTPS possono essere modificate dopo l'installazione, se necessario per motivi di sicurezza. Le porte predefinite sono 80 per HTTP e 443 per HTTPS.

Cosa ti serve

Per accedere alla console di manutenzione del server Unified Manager, è necessario disporre di un ID utente e di una password autorizzati.

> Alcune porte sono considerate non sicure quando si utilizzano i browser Mozilla Firefox o Google Chrome. Verificare con il browser prima di assegnare un nuovo numero di porta per il traffico HTTP e HTTPS. La selezione di una porta non sicura potrebbe rendere il sistema inaccessibile, il che richiederebbe di contattare il supporto clienti per una risoluzione.

L'istanza di Unified Manager viene riavviata automaticamente dopo aver modificato la porta, quindi assicurarsi che questo sia il momento giusto per spegnere il sistema per un breve periodo di tempo.

1. Accedere utilizzando SSH come utente di manutenzione all'host di Unified Manager.

   Vengono visualizzati i prompt della console di Unified Managermaintenance.

2. Digitare il numero dell'opzione di menu **View/Change Application Ports** (Visualizza/Modifica porte applicazione), quindi premere Invio.
3. Se richiesto, inserire nuovamente la password utente per la manutenzione.
4. Digitare i nuovi numeri di porta per le porte HTTP e HTTPS, quindi premere Invio.

   Lasciando vuoto un numero di porta, viene assegnata la porta predefinita per il protocollo.

   Viene richiesto se si desidera modificare le porte e riavviare Unified Manager ora.

5. Digitare **y** per modificare le porte e riavviare Unified Manager.
6. Uscire dalla console di manutenzione.

Dopo questa modifica, gli utenti devono includere il nuovo numero di porta nell'URL per accedere all'interfaccia utente Web di Unified Manager, ad esempio https://host.company.com:1234, https://12.13.14.15:1122 o https://[2001:db8:0:1]:2123.

Aggiunta di interfacce di rete

È possibile aggiungere nuove interfacce di rete se è necessario separare il traffico di rete.

Cosa ti serve

È necessario aggiungere l'interfaccia di rete all'appliance virtuale utilizzando vSphere.

L'appliance virtuale deve essere accesa.

> Non è possibile eseguire questa operazione se Unified Manager è installato su Red Hat Enterprise Linux o su Microsoft Windows.

Fasi

1. Nel menu principale della console vSphere, selezionare **Configurazione di sistema** > **riavvio del sistema operativo**.

   Dopo il riavvio, la console di manutenzione è in grado di rilevare la nuova interfaccia di rete aggiunta.

2. Accedere alla console di manutenzione.
3. Selezionare **Network Configuration** (Configurazione di rete) > **Enable Network Interface** (attiva interfaccia di rete).
4. Selezionare la nuova interfaccia di rete e premere **Invio**.

   Selezionare **eth1** e premere **Invio**.

5. Digitare **y** per attivare l'interfaccia di rete.
6. Immettere le impostazioni di rete.

   Viene richiesto di inserire le impostazioni di rete se si utilizza un'interfaccia statica o se DHCP non viene rilevato.

   Una volta inserite le impostazioni di rete, si torna automaticamente al menu **Configurazione di rete**.

7. Selezionare **Conferma modifiche**.

   Per aggiungere l'interfaccia di rete, è necessario salvare le modifiche.

Aggiunta di spazio su disco alla directory del database di Unified Manager

La directory del database di Unified Manager contiene tutti i dati relativi allo stato e alle performance raccolti dai sistemi ONTAP. In alcuni casi, potrebbe essere necessario aumentare le dimensioni della directory del database.

Ad esempio, la directory del database potrebbe essere piena se Unified Manager sta raccogliendo dati da un gran numero di cluster in cui ciascun cluster ha molti nodi. Si riceverà un avviso quando la directory del database è piena al 90% e un evento critico quando la directory è piena al 95%.

Non vengono raccolti dati aggiuntivi dai cluster dopo che la directory raggiunge il 95% di riempimento.

I passaggi necessari per aggiungere capacità alla directory dei dati sono diversi a seconda che Unified Manager sia in esecuzione su un server VMware ESXi, Red Hat o CentOS Linux o su un server Microsoft Windows.

Aggiunta di spazio alla directory dei dati dell'host Linux

Se è stato assegnato spazio su disco insufficiente a `/opt/netapp/data` Directory per supportare Unified Manager quando si configura originariamente l'host Linux e si installa Unified Manager, è possibile aggiungere spazio su disco dopo l'installazione aumentando lo spazio su disco su `/opt/netapp/data` directory.

Cosa ti serve

È necessario disporre dell'accesso utente root alla macchina Red Hat Enterprise Linux o CentOS Linux su cui è installato Unified Manager.

Si consiglia di eseguire il backup del database di Unified Manager prima di aumentare le dimensioni della directory dei dati.

Fasi

1. Accedere come utente root alla macchina Linux su cui si desidera aggiungere spazio su disco.
2. Arrestare il servizio Unified Manager e il software MySQL associato nell'ordine indicato:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Creare una cartella di backup temporanea (ad esempio, `/backup-data`) con spazio su disco sufficiente per contenere i dati nella corrente `/opt/netapp/data` directory.
4. Copiare il contenuto e la configurazione dei privilegi dell'esistente `/opt/netapp/data` directory nella directory dei dati di backup:

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

5. Se Linux è attivato:

   a. Ottenere il tipo di se Linux per le cartelle esistenti `/opt/netapp/data` cartella:

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      Il sistema restituisce una conferma simile a quanto segue:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Eseguire il comando chcon per impostare il tipo di se Linux per la directory di backup:

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. Rimuovere il contenuto di `/opt/netapp/data` directory:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. Espandere le dimensioni di `/opt/netapp/data` Directory fino a un minimo di 150 GB tramite comandi LVM o aggiungendo dischi aggiuntivi.

   Se hai creato `/opt/netapp/data` da un disco, quindi non si dovrebbe provare a montare `/opt/netapp/data` Come condivisione NFS o CIFS. Perché, in questo caso, se si tenta di espandere lo spazio su disco, alcuni comandi LVM, ad esempio `resize` e. `extend` potrebbe non funzionare come previsto.

8. Verificare che il `/opt/netapp/data` il proprietario della directory (mysql) e il gruppo (root) rimangono invariati:

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

Il sistema restituisce una conferma simile a quanto segue:

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

9. Se Linux è attivato, verificare che il contesto per `/opt/netapp/data` la directory è ancora impostata su mysqld_db_t:

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

      Il sistema restituisce una conferma simile a quanto segue:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Eliminare il file abc in modo che questo file estraneo non causi un errore di database in futuro.
11. Copiare di nuovo i contenuti dai dati di backup all'espansione `/opt/netapp/data` directory:

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

12. Se Linux è attivato, eseguire il seguente comando:

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

13. Avviare il servizio MySQL:

```
systemctl start mysqld
```

14. Una volta avviato il servizio MySQL, avviare i servizi ocie e ocieau nell'ordine indicato:

```
systemctl start ocie ocieau
```

15. Una volta avviati tutti i servizi, eliminare la cartella di backup `/backup-data`:

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

Aggiunta di spazio al disco dati della macchina virtuale VMware

Se è necessario aumentare la quantità di spazio sul disco dati per il database di Unified Manager, è possibile aggiungere capacità dopo l'installazione aumentando lo spazio su disco utilizzando la console di manutenzione di Unified Manager.

Cosa ti serve

- È necessario disporre dell'accesso al client vSphere.

- La macchina virtuale non deve contenere snapshot memorizzate localmente.
- È necessario disporre delle credenziali utente di manutenzione.

Si consiglia di eseguire il backup della macchina virtuale prima di aumentare le dimensioni dei dischi virtuali.

Fasi

1. Nel client vSphere, selezionare la macchina virtuale Unified Manager, quindi aggiungere ulteriore capacità del disco ai dati `disk 3`. Per ulteriori informazioni, consultare la documentazione di VMware.

   In alcuni rari casi, l'implementazione di Unified Manager utilizza "Hard Disk 2" per il disco dati invece di "Hard Disk 3". Se questo si è verificato durante l'implementazione, aumentare lo spazio di qualsiasi disco più grande. Il disco dati avrà sempre più spazio rispetto all'altro disco.

2. Nel client vSphere, selezionare la macchina virtuale Unified Manager, quindi selezionare la scheda **Console**.
3. Fare clic su nella finestra della console, quindi accedere alla console di manutenzione utilizzando il nome utente e la password.
4. Nel menu principale, inserire il numero dell'opzione **Configurazione di sistema**.
5. Nel menu System Configuration (Configurazione di sistema), inserire il numero dell'opzione **aumenta dimensioni disco dati**.

Aggiunta di spazio all'unità logica del server Microsoft Windows

Se è necessario aumentare la quantità di spazio su disco per il database di Unified Manager, è possibile aggiungere capacità all'unità logica su cui è installato Unified Manager.

Cosa ti serve

È necessario disporre dei privilegi di amministratore di Windows.

Si consiglia di eseguire il backup del database di Unified Manager prima di aggiungere spazio su disco.

Fasi

1. Accedere come amministratore al server Windows su cui si desidera aggiungere spazio su disco.
2. Seguire la procedura corrispondente al metodo che si desidera utilizzare per aggiungere ulteriore spazio:

Opzione	Descrizione
Su un server fisico, aggiungere capacità all'unità logica su cui è installato il server Unified Manager.	Seguire la procedura descritta nell'argomento Microsoft: "Estensione di un volume di base"
Su un server fisico, aggiungere un disco rigido.	Seguire la procedura descritta nell'argomento Microsoft: "Aggiunta di dischi rigidi"

Opzione	Descrizione
Su una macchina virtuale, aumentare le dimensioni di una partizione del disco.	Seguire la procedura descritta nell'argomento VMware: "Aumento delle dimensioni di una partizione del disco"

Gestione dell'accesso degli utenti

È possibile creare ruoli e assegnare funzionalità per controllare l'accesso degli utenti a Active IQ Unified Manager. È possibile identificare gli utenti che dispongono delle funzionalità necessarie per accedere agli oggetti selezionati in Unified Manager. Solo gli utenti che dispongono di questi ruoli e funzionalità possono gestire gli oggetti in Unified Manager.

Aggiunta di utenti

È possibile aggiungere utenti locali o utenti di database utilizzando la pagina utenti. È inoltre possibile aggiungere utenti o gruppi remoti appartenenti a un server di autenticazione. È possibile assegnare ruoli a questi utenti e, in base ai privilegi dei ruoli, gli utenti possono gestire gli oggetti e i dati di storage con Unified Manager o visualizzare i dati in un database.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione.
- Per aggiungere un utente o un gruppo remoto, è necessario aver attivato l'autenticazione remota e configurato il server di autenticazione.
- Se si prevede di configurare l'autenticazione SAML in modo che un provider di identità (IdP) autentichi gli utenti che accedono all'interfaccia grafica, assicurarsi che questi utenti siano definiti come utenti "remote".

  L'accesso all'interfaccia utente non è consentito per gli utenti di tipo "local" o "maintenance" quando l'autenticazione SAML è attivata.

Se si aggiunge un gruppo da Windows Active Directory, tutti i membri diretti e i sottogruppi nidificati possono autenticarsi in Unified Manager, a meno che i sottogruppi nidificati non siano disattivati. Se si aggiunge un gruppo da OpenLDAP o altri servizi di autenticazione, solo i membri diretti di tale gruppo possono autenticarsi in Unified Manager.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.
2. Nella pagina utenti, fare clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi utente, selezionare il tipo di utente che si desidera aggiungere e immettere le informazioni richieste.

   Quando si immettono le informazioni utente richieste, è necessario specificare un indirizzo e-mail univoco per l'utente. Evitare di specificare indirizzi e-mail condivisi da più utenti.

4. Fare clic su **Aggiungi**.

Creazione di un utente di database

Per supportare una connessione tra Workflow Automation e Unified Manager, o per accedere alle viste del database, è necessario innanzitutto creare un utente del database con il ruolo Schema di integrazione o Schema report nell'interfaccia utente Web di Unified Manager.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Gli utenti dei database forniscono integrazione con Workflow Automation e accesso a viste di database specifiche per i report. Gli utenti del database non hanno accesso all'interfaccia utente Web di Unified Manager o alla console di manutenzione e non possono eseguire chiamate API.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.
2. Nella pagina utenti, fare clic su **Aggiungi**.
3. Nella finestra di dialogo Add User (Aggiungi utente), selezionare **Database User** (utente database) nell'elenco a discesa **Type** (tipo).
4. Digitare un nome e una password per l'utente del database.
5. Nell'elenco a discesa **ruolo**, selezionare il ruolo appropriato.

Se sei…	Scegliere questo ruolo
Connessione di Unified Manager con Workflow Automation	Schema di integrazione
Accesso a report e altre viste del database	Schema del report

6. Fare clic su **Aggiungi**.

Modifica delle impostazioni utente

È possibile modificare le impostazioni utente, ad esempio l'indirizzo e-mail e il ruolo, specificate da ciascun utente. Ad esempio, è possibile modificare il ruolo di un utente che è un operatore di storage e assegnare all'utente i privilegi di amministratore dello storage.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Quando si modifica il ruolo assegnato a un utente, le modifiche vengono applicate quando si verifica una delle seguenti azioni:

- L'utente si disconnette e si connette nuovamente a Unified Manager.
- È stato raggiunto il timeout della sessione di 24 ore.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.
2. Nella pagina utenti, selezionare l'utente per cui si desidera modificare le impostazioni e fare clic su **Modifica**.
3. Nella finestra di dialogo Edit User (Modifica utente), modificare le impostazioni appropriate specificate per l'utente.
4. Fare clic su **Save** (Salva).

Visualizzazione degli utenti

È possibile utilizzare la pagina utenti per visualizzare l'elenco degli utenti che gestiscono gli oggetti e i dati di storage utilizzando Unified Manager. È possibile visualizzare i dettagli relativi agli utenti, ad esempio il nome utente, il tipo di utente, l'indirizzo e-mail e il ruolo assegnato agli utenti.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Fase

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.

Eliminazione di utenti o gruppi

È possibile eliminare uno o più utenti dal database del server di gestione per impedire a utenti specifici di accedere a Unified Manager. È inoltre possibile eliminare i gruppi in modo che tutti gli utenti del gruppo non possano più accedere al server di gestione.

Cosa ti serve

- Quando si eliminano gruppi remoti, è necessario riassegnare gli eventi assegnati agli utenti dei gruppi remoti.

  Se si eliminano utenti locali o remoti, gli eventi assegnati a tali utenti vengono automaticamente disassegnati.

- È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.
2. Nella pagina utenti, selezionare gli utenti o i gruppi che si desidera eliminare, quindi fare clic su **Elimina**.
3. Fare clic su **Sì** per confermare l'eliminazione.

Cos'è RBAC

RBAC (role-based access control) consente di controllare chi ha accesso a varie funzionalità e risorse nel server Active IQ Unified Manager.

Che cosa fa il controllo degli accessi basato sui ruoli

RBAC (role-based access control) consente agli amministratori di gestire gruppi di utenti definendo i ruoli. Se è necessario limitare l'accesso per funzionalità specifiche agli amministratori selezionati, è necessario impostare account amministratore per tali amministratori. Se si desidera limitare le informazioni che gli amministratori possono visualizzare e le operazioni che possono eseguire, è necessario applicare i ruoli agli account amministratore creati.

Il server di gestione utilizza RBAC per le autorizzazioni di accesso utente e ruolo. Se non sono state modificate le impostazioni predefinite del server di gestione per l'accesso dell'utente amministrativo, non è necessario effettuare l'accesso per visualizzarle.

Quando si avvia un'operazione che richiede privilegi specifici, il server di gestione richiede di effettuare l'accesso. Ad esempio, per creare account amministratore, è necessario effettuare l'accesso con l'account amministratore dell'applicazione.

Definizioni dei tipi di utente

Un tipo di utente specifica il tipo di account che l'utente possiede e include utenti remoti, gruppi remoti, utenti locali, utenti di database e utenti di manutenzione. Ciascuno di questi tipi ha un proprio ruolo, assegnato da un utente con il ruolo di Amministratore.

I tipi di utenti di Unified Manager sono i seguenti:

- **Utente manutenzione**

  Creato durante la configurazione iniziale di Unified Manager. L'utente di manutenzione crea quindi utenti aggiuntivi e assegna ruoli. L'utente che esegue la manutenzione è anche l'unico utente ad avere accesso alla console di manutenzione. Quando Unified Manager viene installato su un sistema Red Hat Enterprise Linux o CentOS, all'utente che esegue la manutenzione viene assegnato il nome utente "umadmin".

- **Utente locale**

  Accede all'interfaccia utente di Unified Manager ed esegue le funzioni in base al ruolo assegnato dall'utente di manutenzione o da un utente con il ruolo di amministratore dell'applicazione.

- **Gruppo remoto**

  Gruppo di utenti che accedono all'interfaccia utente di Unified Manager utilizzando le credenziali memorizzate sul server di autenticazione. Il nome di questo account deve corrispondere al nome di un gruppo memorizzato nel server di autenticazione. A tutti gli utenti del gruppo remoto viene concesso l'accesso all'interfaccia utente di Unified Manager utilizzando le proprie credenziali utente individuali. I gruppi remoti possono eseguire le funzioni in base ai ruoli assegnati.

- **Utente remoto**

  Consente di accedere all'interfaccia utente di Unified Manager utilizzando le credenziali memorizzate nel server di autenticazione. Un utente remoto esegue le funzioni in base al ruolo assegnato dall'utente di manutenzione o da un utente con il ruolo di amministratore dell'applicazione.

- **Utente database**

Dispone di accesso in sola lettura ai dati nel database di Unified Manager, non ha accesso all'interfaccia Web di Unified Manager o alla console di manutenzione e non può eseguire chiamate API.

Definizioni dei ruoli utente

L'utente addetto alla manutenzione o l'amministratore dell'applicazione assegna un ruolo a ogni utente. Ogni ruolo contiene alcuni privilegi. L'ambito delle attività che è possibile eseguire in Unified Manager dipende dal ruolo assegnato e dai privilegi contenuti nel ruolo.

Unified Manager include i seguenti ruoli utente predefiniti:

- **Operatore**

  Visualizza le informazioni sul sistema storage e altri dati raccolti da Unified Manager, incluse cronologie e tendenze della capacità. Questo ruolo consente all'operatore di storage di visualizzare, assegnare, riconoscere, risolvere e aggiungere note per gli eventi.

- **Storage Administrator**

  Configura le operazioni di gestione dello storage in Unified Manager. Questo ruolo consente all'amministratore dello storage di configurare le soglie e di creare avvisi e altre opzioni e policy specifiche per la gestione dello storage.

- **Amministratore dell'applicazione**

  Configura impostazioni non correlate alla gestione dello storage. Questo ruolo consente la gestione di utenti, certificati di sicurezza, accesso al database e opzioni amministrative, tra cui autenticazione, SMTP, networking e AutoSupport.

  Quando Unified Manager viene installato sui sistemi Linux, l'utente iniziale con il ruolo di amministratore dell'applicazione viene automaticamente chiamato "umadmin".

- **Schema di integrazione**

  Questo ruolo consente l'accesso in sola lettura alle viste del database di Unified Manager per l'integrazione di Unified Manager con OnCommand Workflow Automation (Wfa).

- **Schema report**

  Questo ruolo consente l'accesso in sola lettura ai report e ad altre viste del database direttamente dal database di Unified Manager. I database visualizzabili includono:

  - vista_modello_netapp
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

Ruoli e funzionalità degli utenti di Unified Manager

In base al ruolo utente assegnato, è possibile determinare le operazioni che è possibile eseguire in Unified Manager.

Nella tabella seguente sono riportate le funzioni che ciascun ruolo utente può eseguire:

Funzione	Operatore	Amministratore dello storage	Amministratore dell'applicazione	Schema di integrazione	Schema del report
Visualizzare le informazioni sul sistema di storage	•	•	•	•	•
Visualizzare altri dati, ad esempio cronologie e trend di capacità	•	•	•	•	•
Visualizzare, assegnare e risolvere gli eventi	•	•	•		
Visualizzare gli oggetti del servizio di storage, ad esempio le associazioni SVM e i pool di risorse	•	•	•		
Visualizzare i criteri di soglia	•	•	•		
Gestire gli oggetti del servizio di storage, come associazioni SVM e pool di risorse		•	•		
Definire gli avvisi		•	•		

Funzione	Operatore	Amministratore dello storage	Amministratore dell'applicazione	Schema di integrazione	Schema del report
Gestire le opzioni di gestione dello storage		•	•		
Gestire le policy di gestione dello storage		•	•		
Gestire gli utenti			•		
Gestire le opzioni amministrative			•		
Definire i criteri di soglia			•		
Gestire l'accesso al database			•		
Gestire l'integrazione con WFA e fornire l'accesso alle viste del database				•	
Pianificare e salvare i report		•	•		
Eseguire le operazioni "Fix it" dalle azioni di gestione		•	•		
Fornire l'accesso in sola lettura alle viste del database					•

Gestione delle impostazioni di autenticazione SAML

Dopo aver configurato le impostazioni di autenticazione remota, è possibile attivare l'autenticazione SAML (Security Assertion Markup Language) in modo che gli utenti

remoti vengano autenticati da un provider di identità sicuro (IdP) prima di poter accedere all'interfaccia utente Web di Unified Manager.

Tenere presente che solo gli utenti remoti avranno accesso all'interfaccia utente grafica di Unified Manager dopo l'attivazione dell'autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all'interfaccia utente. Questa configurazione non influisce sugli utenti che accedono alla console di manutenzione.

Requisiti del provider di identità

Quando si configura Unified Manager per utilizzare un provider di identità (IdP) per eseguire l'autenticazione SAML per tutti gli utenti remoti, è necessario conoscere alcune impostazioni di configurazione necessarie per consentire la connessione a Unified Manager.

È necessario immettere l'URI e i metadati di Unified Manager nel server IdP. È possibile copiare queste informazioni dalla pagina autenticazione SAML di Unified Manager. Unified Manager è considerato il service provider (SP) nello standard SAML (Security Assertion Markup Language).

Standard di crittografia supportati

- AES (Advanced Encryption Standard): AES-128 e AES-256
- Secure Hash Algorithm (SHA): SHA-1 e SHA-256

Provider di identità validati

- Shibboleth
- Active Directory Federation Services (ADFS)

Requisiti di configurazione di ADFS

- È necessario definire tre regole per le attestazioni nell'ordine seguente, necessarie affinché Unified Manager analizzi le risposte SAML di ADFS per questa voce di trust della parte che si basa.

Regola della richiesta di rimborso	Valore
Nome-account-SAM	ID nome
Nome-account-SAM	urn:oid:0.9.2342.19200300.100.1.1
Gruppi di token — Nome non qualificato	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- È necessario impostare il metodo di autenticazione su "Forms Authentication" (autenticazione moduli), altrimenti gli utenti potrebbero ricevere un errore durante la disconnessione da Unified Manager . Attenersi alla seguente procedura:
  a. Aprire la console di gestione ADFS.
  b. Fare clic sulla cartella Authentication Policies (Criteri di autenticazione) nella vista ad albero a sinistra.
  c. Nella sezione azioni a destra, fare clic su Modifica policy di autenticazione primaria globale.

d. Impostare il metodo di autenticazione Intranet su “Forms Authentication” invece di “Windows Authentication” predefinito.

- In alcuni casi, l’accesso tramite IdP viene rifiutato quando il certificato di sicurezza di Unified Manager è firmato dalla CA. Esistono due soluzioni alternative per risolvere questo problema:
  - Seguire le istruzioni indicate nel collegamento per disattivare il controllo di revoca sul server ADFS per la parte di base associata al certificato CA concatenato:

    "Disattiva il controllo di revoca per fiducia della parte che si basa"

  - Fare in modo che il server CA si trovi all’interno del server ADFS per firmare la richiesta di certificazione del server Unified Manager.

Altri requisiti di configurazione

- L’inclinazione dell’orologio di Unified Manager è impostata su 5 minuti, quindi la differenza di tempo tra il server IdP e il server Unified Manager non può superare i 5 minuti o l’autenticazione non riesce.

Attivazione dell’autenticazione SAML

È possibile attivare l’autenticazione SAML (Security Assertion Markup Language) in modo che gli utenti remoti vengano autenticati da un provider di identità sicuro (IdP) prima di poter accedere all’interfaccia utente Web di Unified Manager.

Cosa ti serve

- È necessario aver configurato l’autenticazione remota e verificato che sia stata eseguita correttamente.
- È necessario aver creato almeno un utente remoto o un gruppo remoto con il ruolo di amministratore dell’applicazione.
- Il provider di identità (IdP) deve essere supportato da Unified Manager e deve essere configurato.
- È necessario disporre dell’URL IdP e dei metadati.
- È necessario disporre dell’accesso al server IdP.

Dopo aver abilitato l’autenticazione SAML da Unified Manager, gli utenti non possono accedere all’interfaccia utente grafica fino a quando IdP non è stato configurato con le informazioni sull’host del server Unified Manager. Pertanto, è necessario essere pronti a completare entrambe le parti della connessione prima di avviare il processo di configurazione. L’IdP può essere configurato prima o dopo la configurazione di Unified Manager.

Solo gli utenti remoti avranno accesso all’interfaccia utente grafica di Unified Manager dopo l’attivazione dell’autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all’interfaccia utente. Questa configurazione non influisce sugli utenti che accedono alla console di manutenzione, ai comandi di Unified Manager o alle ZAPI.

Unified Manager viene riavviato automaticamente dopo aver completato la configurazione SAML in questa pagina.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **General** > **SAML Authentication**.
2. Selezionare la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML).

Vengono visualizzati i campi necessari per configurare la connessione IdP.

3. Immettere l'URI IdP e i metadati IdP richiesti per connettere il server Unified Manager al server IdP.

   Se il server IdP è accessibile direttamente dal server Unified Manager, è possibile fare clic sul pulsante **Fetch IdP Metadata** (Scarica metadati IdP) dopo aver immesso l'URI IdP per popolare automaticamente il campo IdP Metadata (metadati IdP).

4. Copiare l'URI dei metadati host di Unified Manager o salvare i metadati host in un file di testo XML.

   In questo momento è possibile configurare il server IdP con queste informazioni.

5. Fare clic su **Save** (Salva).

   Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

6. Fare clic su **Confirm and Logout** (Conferma e Disconnetti) per riavviare Unified Manager.

La volta successiva che gli utenti remoti autorizzati tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella pagina di accesso di IdP anziché nella pagina di accesso di Unified Manager.

Se non è già stato completato, accedere all'IdP e immettere l'URI e i metadati del server Unified Manager per completare la configurazione.

> Quando si utilizza ADFS come provider di identità, la GUI di Unified Manager non rispetta il timeout ADFS e continuerà a funzionare fino al raggiungimento del timeout della sessione di Unified Manager. È possibile modificare il timeout della sessione GUI facendo clic su **General** > **Feature Settings** > **Inactivity Timeout**.

Modifica del provider di identità utilizzato per l'autenticazione SAML

È possibile modificare il provider di identità (IdP) utilizzato da Unified Manager per autenticare gli utenti remoti.

Cosa ti serve

- È necessario disporre dell'URL IdP e dei metadati.
- È necessario disporre dell'accesso all'IdP.

Il nuovo IdP può essere configurato prima o dopo la configurazione di Unified Manager.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **General** > **SAML Authentication**.
2. Inserire il nuovo URI IdP e i metadati IdP richiesti per connettere il server Unified Manager all'IdP.

   Se l'IdP è accessibile direttamente dal server di Unified Manager, è possibile fare clic sul pulsante **Fetch IdP Metadata** (Scarica metadati IdP) dopo aver immesso l'URL IdP per compilare automaticamente il campo IdP Metadata (metadati IdP).

3. Copiare l'URI dei metadati di Unified Manager o salvare i metadati in un file di testo XML.

4. Fare clic su **Save Configuration** (Salva configurazione).

   Viene visualizzata una finestra di messaggio per confermare che si desidera modificare la configurazione.

5. Fare clic su **OK**.

Accedere al nuovo IdP e immettere l'URI e i metadati del server Unified Manager per completare la configurazione.

La volta successiva che gli utenti remoti autorizzati tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella nuova pagina di accesso IdP anziché nella vecchia pagina di accesso IdP.

Aggiornamento delle impostazioni di autenticazione SAML dopo la modifica del certificato di protezione di Unified Manager

Qualsiasi modifica al certificato di protezione HTTPS installato sul server Unified Manager richiede l'aggiornamento delle impostazioni di configurazione per l'autenticazione SAML. Il certificato viene aggiornato se si rinomina il sistema host, si assegna un nuovo indirizzo IP al sistema host o si modifica manualmente il certificato di protezione del sistema.

Una volta modificato il certificato di protezione e riavviato il server Unified Manager, l'autenticazione SAML non funzionerà e gli utenti non potranno accedere all'interfaccia grafica di Unified Manager. Per riattivare l'accesso all'interfaccia utente, è necessario aggiornare le impostazioni di autenticazione SAML sul server IdP e sul server Unified Manager.

Fasi

1. Accedere alla console di manutenzione.
2. Nel **Menu principale**, inserire il numero dell'opzione **Disattiva autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che si desidera disattivare l'autenticazione SAML e riavviare Unified Manager.

3. Avviare l'interfaccia utente di Unified Manager utilizzando l'FQDN o l'indirizzo IP aggiornato, accettare il certificato del server aggiornato nel browser e accedere utilizzando le credenziali utente di manutenzione.
4. Nella pagina **Setup/Authentication**, selezionare la scheda **SAML Authentication** e configurare la connessione IdP.
5. Copiare l'URI dei metadati host di Unified Manager o salvare i metadati host in un file di testo XML.
6. Fare clic su **Save** (Salva).

   Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

7. Fare clic su **Confirm and Logout** (Conferma e Disconnetti) per riavviare Unified Manager.
8. Accedere al server IdP e immettere l'URI e i metadati del server Unified Manager per completare la configurazione.

Provider di identità	Fasi di configurazione
ADFS	a. Eliminare la voce di trust esistente della parte che si basa nella GUI di gestione di ADFS. b. Aggiungere una nuova voce di attendibilità della parte che si basa utilizzando `saml_sp_metadata.xml` Dal server Unified Manager aggiornato. c. Definire le tre regole di attestazione richieste da Unified Manager per analizzare le risposte SAML di ADFS per questa voce di attendibilità della parte che si basa. d. Riavviare il servizio Windows di ADFS.
Shibboleth	a. Aggiornare il nuovo FQDN del server Unified Manager in `attribute-filter.xml` e. `relying-party.xml` file. b. Riavviare il server Web Apache Tomcat e attendere che la porta 8005 sia online.

9. Accedere a Unified Manager e verificare che l'autenticazione SAML funzioni come previsto attraverso l'IdP.

Disattivazione dell'autenticazione SAML

È possibile disattivare l'autenticazione SAML quando si desidera interrompere l'autenticazione degli utenti remoti tramite un provider di identità sicuro (IdP) prima che possano accedere all'interfaccia utente Web di Unified Manager. Quando l'autenticazione SAML è disattivata, i provider di servizi di directory configurati, ad esempio Active Directory o LDAP, eseguono l'autenticazione di accesso.

Una volta disattivata l'autenticazione SAML, gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia grafica utente oltre agli utenti remoti configurati.

Se non si dispone dell'accesso all'interfaccia utente grafica, è possibile disattivare l'autenticazione SAML anche utilizzando la console di manutenzione di Unified Manager.

Unified Manager viene riavviato automaticamente dopo la disattivazione dell'autenticazione SAML.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **General** > **SAML Authentication**.
2. Deselezionare la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML).
3. Fare clic su **Save** (Salva).

   Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

4. Fare clic su **Confirm and Logout** (Conferma e Disconnetti) per riavviare Unified Manager.

La volta successiva che gli utenti remoti tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella pagina di accesso di Unified Manager anziché nella pagina di accesso di IdP.

Accedere all'ID ed eliminare l'URI e i metadati del server Unified Manager.

Disattivazione dell'autenticazione SAML dalla console di manutenzione

Potrebbe essere necessario disattivare l'autenticazione SAML dalla console di manutenzione quando non è possibile accedere alla GUI di Unified Manager. Ciò potrebbe verificarsi in caso di errata configurazione o se l'IdP non è accessibile.

Cosa ti serve

È necessario avere accesso alla console di manutenzione come utente di manutenzione.

Quando l'autenticazione SAML è disattivata, i provider di servizi di directory configurati, ad esempio Active Directory o LDAP, eseguono l'autenticazione di accesso. Gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica oltre agli utenti remoti configurati.

È inoltre possibile disattivare l'autenticazione SAML dalla pagina Setup/Authentication (Configurazione/autenticazione) dell'interfaccia utente.

> Unified Manager viene riavviato automaticamente dopo la disattivazione dell'autenticazione SAML.

Fasi

1. Accedere alla console di manutenzione.
2. Nel **Menu principale**, inserire il numero dell'opzione **Disattiva autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che si desidera disattivare l'autenticazione SAML e riavviare Unified Manager.

3. Digitare **y**, quindi premere Invio per riavviare Unified Manager.

La volta successiva che gli utenti remoti tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella pagina di accesso di Unified Manager anziché nella pagina di accesso di IdP.

Se necessario, accedere all'IdP ed eliminare l'URL e i metadati del server Unified Manager.

Pagina SAML Authentication

È possibile utilizzare la pagina SAML Authentication per configurare Unified Manager in modo che autentichi gli utenti remoti utilizzando SAML tramite un provider di identità sicuro (IdP) prima che possano accedere all'interfaccia utente Web di Unified Manager.

- Per creare o modificare la configurazione SAML, è necessario disporre del ruolo di amministratore dell'applicazione.
- È necessario aver configurato l'autenticazione remota.
- È necessario aver configurato almeno un utente remoto o un gruppo remoto.

Dopo aver configurato l'autenticazione remota e gli utenti remoti, selezionare la casella di controllo Enable SAML Authentication (attiva autenticazione SAML) per abilitare l'autenticazione utilizzando un provider di identità sicuro.

- **IDP URI**

  L'URI per accedere all'IdP dal server Unified Manager. Di seguito sono elencati gli URI di esempio.

  URI di esempio ADFS:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  URI di esempio Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Metadati IdP**

  I metadati IdP in formato XML.

  Se l'URL IdP è accessibile dal server di Unified Manager, fare clic sul pulsante **Fetch IdP Metadata** (Scarica metadati IdP) per compilare questo campo.

- **Sistema host (FQDN)**

  L'FQDN del sistema host di Unified Manager come definito durante l'installazione. Se necessario, è possibile modificare questo valore.

- **URI host**

  L'URI per accedere al sistema host di Unified Manager da IdP.

- **Metadati host**

  I metadati del sistema host in formato XML.

Gestione dell'autenticazione

È possibile attivare l'autenticazione utilizzando LDAP o Active Directory sul server Unified Manager e configurarlo per l'utilizzo con i server per l'autenticazione degli utenti remoti.

Per abilitare l'autenticazione remota, impostare i servizi di autenticazione e aggiungere server di autenticazione, vedere la sezione precedente su **Configurazione di Unified Manager per l'invio di notifiche di avviso**.

Modifica dei server di autenticazione

È possibile modificare la porta utilizzata dal server Unified Manager per comunicare con il server di autenticazione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare la casella **Disable Nested Group Lookup** (Disattiva ricerca gruppi nidificati).
3. Nell'area **Authentication Servers** (Server di autenticazione), selezionare il server di autenticazione che si desidera modificare, quindi fare clic su **Edit** (Modifica).
4. Nella finestra di dialogo **Edit Authentication Server** (Modifica server di autenticazione), modificare i dettagli della porta.
5. Fare clic su **Save** (Salva).

Eliminazione dei server di autenticazione

È possibile eliminare un server di autenticazione se si desidera impedire al server Unified Manager di comunicare con il server di autenticazione. Ad esempio, se si desidera modificare un server di autenticazione con cui il server di gestione sta comunicando, è possibile eliminare il server di autenticazione e aggiungere un nuovo server di autenticazione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Quando si elimina un server di autenticazione, gli utenti remoti o i gruppi del server di autenticazione non potranno più accedere a Unified Manager.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare uno o più server di autenticazione che si desidera eliminare, quindi fare clic su **Delete** (Elimina).
3. Fare clic su **Sì** per confermare la richiesta di eliminazione.

   Se l'opzione **Usa connessione sicura** è attivata, i certificati associati al server di autenticazione vengono cancellati insieme al server di autenticazione.

Autenticazione con Active Directory o OpenLDAP

È possibile attivare l'autenticazione remota sul server di gestione e configurare il server di gestione per comunicare con i server di autenticazione in modo che gli utenti all'interno dei server di autenticazione possano accedere a Unified Manager.

È possibile utilizzare uno dei seguenti servizi di autenticazione predefiniti o specificare un servizio di autenticazione personalizzato:

- Microsoft Active Directory

  Non è possibile utilizzare Microsoft Lightweight Directory Services.

- OpenLDAP

È possibile selezionare il servizio di autenticazione richiesto e aggiungere i server di autenticazione appropriati per consentire agli utenti remoti nel server di autenticazione di accedere a Unified Manager. Le credenziali per utenti o gruppi remoti vengono gestite dal server di autenticazione. Il server di gestione utilizza il protocollo LDAP (Lightweight Directory Access Protocol) per autenticare gli utenti remoti all'interno del server di autenticazione configurato.

Per gli utenti locali creati in Unified Manager, il server di gestione gestisce il proprio database di nomi utente e password. Il server di gestione esegue l'autenticazione e non utilizza Active Directory o OpenLDAP per l'autenticazione.

Registrazione dell'audit

È possibile rilevare se i registri di controllo sono stati compromessi con l'utilizzo dei registri di controllo. Tutte le attività eseguite da un utente vengono monitorate e registrate nei registri di controllo. I controlli vengono eseguiti per tutte le funzionalità dell'interfaccia utente e delle API` esposte pubblicamente di Active IQ Unified Manager.

È possibile utilizzare il registro di controllo: Visualizzazione file* per visualizzare e accedere a tutti i file di registro di controllo disponibili in Active IQ Unified Manager. I file nella visualizzazione file del registro di controllo sono elencati in base alla data di creazione. Questa vista visualizza le informazioni di tutti i log di controllo acquisiti dall'installazione o dall'aggiornamento al presente nel sistema. Ogni volta che si esegue un'azione in Unified Manager, le informazioni vengono aggiornate e sono disponibili nei registri. Lo stato di ciascun file di log viene acquisito utilizzando l'attributo "file Integrity Status", che viene monitorato attivamente per rilevare la manomissione o l'eliminazione del file di log. I registri di controllo possono avere uno dei seguenti stati quando i registri di controllo sono disponibili nel sistema:

Stato	Descrizione
ATTIVO	File in cui vengono attualmente registrati i log.
NORMALE	File inattivo, compresso e memorizzato nel sistema.
MANOMESSO	File che è stato compromesso da un utente che ha modificato manualmente il file.
MANUAL_DELETE	File eliminato da un utente autorizzato.
ROLLOVER_DELETE	File che è stato eliminato a causa dell'annullamento in base a criteri di configurazione a rotazione.
UNEXPECTED_DELETE	File eliminato per motivi sconosciuti.

La pagina Registro di controllo include i seguenti pulsanti di comando:

- Configurare
- Eliminare
- Scarica

Il pulsante **DELETE** consente di eliminare qualsiasi registro di controllo elencato nella vista registri di controllo. È possibile eliminare un registro di controllo e, facoltativamente, fornire un motivo per eliminare il file, in modo da poter determinare un'eliminazione valida in futuro. La colonna REASON (MOTIVO) elenca il motivo insieme al nome dell'utente che ha eseguito l'operazione di eliminazione.

L'eliminazione di un file di log causerà l'eliminazione del file dal sistema, ma la voce nella tabella DB non verrà eliminata.

È possibile scaricare i registri di controllo da Active IQ Unified Manager utilizzando il pulsante **DOWNLOAD** nella sezione registri di controllo ed esportare i file di registro di controllo. I file contrassegnati con "NORMAL" o "MANOMESSI" vengono scaricati in un file compresso `.gzip` formato.

I file di log di audit vengono archiviati periodicamente e salvati nel database per riferimento. Prima dell'archiviazione, i registri di controllo sono dotati di firma digitale per garantire la sicurezza e l'integrità.

Quando viene generato un bundle AutoSupport completo, il bundle di supporto include file di log di audit sia archiviati che attivi. Tuttavia, quando viene generato un bundle di supporto leggero, include solo i registri di controllo attivi. I registri di controllo archiviati non sono inclusi.

Configurazione dei registri di audit

È possibile utilizzare il pulsante **Configura** nella sezione registri di controllo per configurare i criteri di rolling per i file di registro di controllo e per attivare la registrazione remota per i registri di controllo.

È possibile impostare i valori nei CAMPI **MAX FILE SIZE** e **AUDIT LOG RETENTION DAYS** in base alla quantità e alla frequenza desiderate dei dati che si desidera memorizzare nel sistema. Il valore nel campo **TOTAL AUDIT LOG SIZE** (DIMENSIONE TOTALE REGISTRO DI CONTROLLO) è la dimensione dei dati totali del registro di controllo presenti nel sistema. La policy di rollover è determinata dai valori nel campo **GIORNI DI CONSERVAZIONE DEL REGISTRO DI CONTROLLO**, **dimensione DEL FILE MAX** e **DIMENSIONE TOTALE DEL REGISTRO DI CONTROLLO**. Quando la dimensione del backup del registro di controllo raggiunge il valore configurato in **TOTAL AUDIT LOG SIZE**, il file archiviato per primo viene cancellato. Ciò significa che il file meno recente viene cancellato. Tuttavia, la voce del file continua a essere disponibile nel database ed è contrassegnata come "Elimina rollover". Il valore **GIORNI di CONSERVAZIONE del REGISTRO DI CONTROLLO** corrisponde al numero di giorni in cui i file di registro di controllo vengono conservati. Viene eseguito il rollover di qualsiasi file precedente al valore impostato in questo campo.

Fasi

1. Fare clic su **Audit Logs** > > **Configure**.
2. Inserire i valori nelle voci **MAX FILE SIZE**, **TOTAL AUDIT LOG SIZE** e **AUDIT LOG RETENTION DAYS**.

   Se si desidera attivare la registrazione remota, selezionare **Enable Remote Logging** (attiva registrazione remota).

Abilitazione della registrazione remota dei registri di controllo

È possibile selezionare la casella di controllo **Enable Remote Logging** (attiva registrazione remota) nella finestra di dialogo Configure Audit Logs (Configura registri di controllo) per attivare la registrazione remota dell'audit. È possibile utilizzare questa funzione per trasferire i registri di controllo a un server Syslog remoto. In questo modo, è possibile gestire i registri di controllo in caso di limiti di spazio.

La registrazione remota dei registri di controllo fornisce un backup a prova di manomissione nel caso in cui i file di registro di controllo sul server Active IQ Unified Manager vengano manomessi.

Fasi

1. Nella finestra di dialogo **Configura registri di controllo**, selezionare la casella di controllo **attiva registrazione remota**.

   Vengono visualizzati ulteriori campi per configurare la registrazione remota.

2. Immettere il **NOME HOST** e la **PORTA** del server remoto a cui si desidera connettersi.
3. Nel campo **CERTIFICATO CA DEL SERVER**, fare clic su **SFOGLIA** per selezionare un certificato pubblico del server di destinazione.

   Il certificato deve essere caricato in `.pem` formato. Questo certificato deve essere ottenuto dal server Syslog di destinazione e non deve essere scaduto. Il certificato deve contenere il "hostname" selezionato come parte di `SubjectAltName` (SAN).

4. Immettere i valori per i seguenti campi: **CHARSET**, **TIMEOUT CONNESSIONE**, **RITARDO DI RICONNESSIONE**.

   I valori devono essere espressi in millisecondi per questi campi.

5. Selezionare il formato Syslog e la versione del protocollo TLS richiesti nei campi **FORMAT** e **PROTOCOL**.
6. Selezionare la casella di controllo **Enable Client Authentication** (attiva autenticazione client) se il server Syslog di destinazione richiede l'autenticazione basata su certificato.

   Prima di salvare la configurazione del registro di controllo, sarà necessario scaricare il certificato di autenticazione del client e caricarlo sul server Syslog, altrimenti la connessione non avrà esito positivo. A seconda del tipo di server Syslog, potrebbe essere necessario creare un hash del certificato di autenticazione del client.

   Esempio: Syslog-ng richiede la creazione di un <hash> del certificato utilizzando il comando `openssl x509 -noout -hash -in cert.pem`, quindi collegare simbolicamente il certificato di autenticazione del client a un file denominato dopo <hash> .0.

7. Fare clic su **Save** (Salva) per configurare la connessione con il server e attivare la registrazione remota.

   Verrà reindirizzato alla pagina Audit Logs (registri di controllo).

Pagina Remote Authentication (autenticazione remota

È possibile utilizzare la pagina Remote Authentication (autenticazione remota) per configurare Unified Manager in modo che comunichi con il server di autenticazione per autenticare gli utenti remoti che tentano di accedere all'interfaccia utente Web di Unified Manager.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Dopo aver selezionato la casella di controllo Enable remote Authentication (attiva autenticazione remota), è possibile attivare l'autenticazione remota utilizzando un server di autenticazione.

- **Servizio di autenticazione**

Consente di configurare il server di gestione per autenticare gli utenti nei provider di servizi di directory, ad esempio Active Directory, OpenLDAP o specificare il proprio meccanismo di autenticazione. È possibile specificare un servizio di autenticazione solo se è stata attivata l'autenticazione remota.

- **Active Directory**
  - Nome amministratore

    Specifica il nome dell'amministratore del server di autenticazione.

  - Password

    Specifica la password per accedere al server di autenticazione.

  - Nome distinto di base

    Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.

  - Disattiva ricerca gruppi nidificati

    Specifica se attivare o disattivare l'opzione di ricerca di gruppi nidificati. Per impostazione predefinita, questa opzione è disattivata. Se si utilizza Active Directory, è possibile accelerare l'autenticazione disattivando il supporto per i gruppi nidificati.

  - USA connessione sicura

    Specifica il servizio di autenticazione utilizzato per comunicare con i server di autenticazione.

- **OpenLDAP**
  - Associa nome distinto

    Specifica il nome distinto di binding utilizzato insieme al nome distinto di base per trovare gli utenti remoti nel server di autenticazione.

  - Password bind

    Specifica la password per accedere al server di autenticazione.

  - Nome distinto di base

    Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.

  - USA connessione sicura

    Specifica che il protocollo LDAP protetto viene utilizzato per comunicare con i server di autenticazione LDAP.

- **Altri**
  - Associa nome distinto

    Specifica il nome distinto di binding utilizzato insieme al nome distinto di base per trovare gli utenti

remoti nel server di autenticazione configurato.

- Password bind

  Specifica la password per accedere al server di autenticazione.

- Nome distinto di base

  Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.

- Versione del protocollo

  Specifica la versione LDAP (Lightweight Directory Access Protocol) supportata dal server di autenticazione. È possibile specificare se la versione del protocollo deve essere rilevata automaticamente o impostata su 2 o 3.

- Attributo User Name

  Specifica il nome dell'attributo nel server di autenticazione che contiene i nomi di accesso dell'utente da autenticare dal server di gestione.

- Attributo Group Membership

  Specifica un valore che assegna l'appartenenza al gruppo di server di gestione agli utenti remoti in base a un attributo e a un valore specificati nel server di autenticazione dell'utente.

- UGID

  Se gli utenti remoti sono inclusi come membri di un oggetto GroupOfUniqueNames nel server di autenticazione, questa opzione consente di assegnare l'appartenenza al gruppo di server di gestione agli utenti remoti in base a un attributo specificato nell'oggetto GroupOfUniqueNames.

- Disattiva ricerca gruppi nidificati

  Specifica se attivare o disattivare l'opzione di ricerca di gruppi nidificati. Per impostazione predefinita, questa opzione è disattivata. Se si utilizza Active Directory, è possibile accelerare l'autenticazione disattivando il supporto per i gruppi nidificati.

- Membro

  Specifica il nome dell'attributo utilizzato dal server di autenticazione per memorizzare informazioni sui singoli membri di un gruppo.

- User Object Class (Classe oggetto utente)

  Specifica la classe di oggetti di un utente nel server di autenticazione remoto.

- Group Object Class (Classe oggetti gruppo)

  Specifica la classe di oggetti di tutti i gruppi nel server di autenticazione remoto.

I valori immessi per gli attributi *Member*, *User Object Class* e *Group Object Class* devono coincidere con quelli aggiunti nelle configurazioni Active Directory, OpenLDAP e LDAP. In caso contrario, l'autenticazione potrebbe non riuscire.

- USA connessione sicura

  Specifica il servizio di autenticazione utilizzato per comunicare con i server di autenticazione.

Se si desidera modificare il servizio di autenticazione, assicurarsi di eliminare tutti i server di autenticazione esistenti e aggiungere nuovi server di autenticazione.

Area Authentication Servers

L'area Authentication Servers (Server di autenticazione) visualizza i server di autenticazione con cui il server di gestione comunica per individuare e autenticare gli utenti remoti. Le credenziali per utenti o gruppi remoti vengono gestite dal server di autenticazione.

- **Pulsanti di comando**

  Consente di aggiungere, modificare o eliminare i server di autenticazione.

  - Aggiungi

    Consente di aggiungere un server di autenticazione.

  Se il server di autenticazione che si sta aggiungendo fa parte di una coppia ad alta disponibilità (utilizzando lo stesso database), è possibile aggiungere anche il server di autenticazione partner. Ciò consente al server di gestione di comunicare con il partner quando uno dei server di autenticazione non è raggiungibile.

  - Modifica

    Consente di modificare le impostazioni di un server di autenticazione selezionato.

  - Eliminare

    Elimina i server di autenticazione selezionati.

- **Nome o indirizzo IP**

  Visualizza il nome host o l'indirizzo IP del server di autenticazione utilizzato per autenticare l'utente sul server di gestione.

- **Porta**

  Visualizza il numero di porta del server di autenticazione.

- **Verifica dell'autenticazione**

  Questo pulsante convalida la configurazione del server di autenticazione autenticando un utente o un gruppo remoto.

  Durante il test, se si specifica solo il nome utente, il server di gestione ricerca l'utente remoto nel server di autenticazione, ma non autenticare l'utente. Se si specificano sia il nome utente che la password, il server

di gestione ricerca e autentica l'utente remoto.

Non è possibile verificare l'autenticazione se l'autenticazione remota è disattivata.

Gestione dei certificati di sicurezza

È possibile configurare HTTPS nel server Unified Manager per monitorare e gestire i cluster su una connessione sicura.

Visualizzazione del certificato di protezione HTTPS

È possibile confrontare i dettagli del certificato HTTPS con il certificato recuperato nel browser per garantire che la connessione crittografata del browser a Unified Manager non venga intercettata.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

La visualizzazione del certificato consente di verificare il contenuto di un certificato rigenerato o di visualizzare i nomi Alt (SAN) del soggetto da cui è possibile accedere a Unified Manager.

Fase

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.

   Il certificato HTTPS viene visualizzato nella parte superiore della pagina

Per visualizzare informazioni più dettagliate sul certificato di protezione rispetto a quelle visualizzate nella pagina del certificato HTTPS, è possibile visualizzare il certificato di connessione nel browser.

Download di una richiesta di firma del certificato HTTPS

È possibile scaricare una richiesta di firma della certificazione per il certificato di protezione HTTPS corrente in modo da fornire il file a un'autorità di certificazione da firmare. Un certificato con firma CA aiuta a prevenire gli attacchi man-in-the-middle e offre una protezione migliore rispetto a un certificato autofirmato.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.
2. Fare clic su **Scarica richiesta firma certificato HTTPS**.
3. Salvare `<hostname>.csr` file.

È possibile fornire il file a un'autorità di certificazione per firmare e installare il certificato firmato.

Installazione di un certificato HTTPS firmato e restituito dalla CA

È possibile caricare e installare un certificato di sicurezza dopo che un'autorità di certificazione ha firmato e restituito il certificato. Il file caricato e installato deve essere una versione firmata del certificato autofirmato esistente. Un certificato con firma CA aiuta a prevenire gli attacchi man-in-the-middle e offre una protezione migliore rispetto a un certificato autofirmato.

Cosa ti serve

È necessario aver completato le seguenti operazioni:

- Il file Certificate Signing Request è stato scaricato e firmato da un'autorità di certificazione
- La catena di certificati è stata salvata in formato PEM
- Inclusi tutti i certificati nella catena, dal certificato del server Unified Manager al certificato di firma root, inclusi eventuali certificati intermedi presenti

È necessario disporre del ruolo di amministratore dell'applicazione.

> Se la validità del certificato per il quale è stata creata una CSR è superiore a 397 giorni, la validità verrà ridotta a 397 giorni dalla CA prima della firma e della restituzione del certificato

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.
2. Fare clic su **Installa certificato HTTPS**.
3. Nella finestra di dialogo visualizzata, fare clic su **Scegli file…** per individuare il file da caricare.
4. Selezionare il file, quindi fare clic su **Installa** per installarlo.

   Per ulteriori informazioni, vedere "Installazione di un certificato HTTPS generato utilizzando strumenti esterni".

Esempio di catena di certificati

Nell'esempio seguente viene illustrato come potrebbe essere visualizzato il file di catena del certificato:

```
-----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-----
```

Installazione di un certificato HTTPS generato utilizzando strumenti esterni

È possibile installare i certificati autofirmati o con firma CA e generati utilizzando uno strumento esterno come OpenSSL, BoringSSL, LetsEncrypt.

È necessario caricare la chiave privata insieme alla catena di certificati, poiché questi certificati sono coppia di chiavi pubbliche e private generate esternamente. Gli algoritmi di coppia di chiavi consentiti sono “RSA” e “EC”. L’opzione **Installa certificato HTTPS** è disponibile nella pagina certificati HTTPS nella sezione Generale. Il file caricato deve essere nel seguente formato di input.

1. Chiave privata del server che appartiene all’host Active IQ Unified Manager
2. Certificato del server che corrisponde alla chiave privata
3. Certificato delle CA invertito fino alla root, che vengono utilizzate per firmare il certificato di cui sopra

Formato per il caricamento di un certificato con una coppia di chiavi EC

Le curve consentite sono “prime256v1” e “secp384r1”. Esempio di certificato con una coppia EC generata esternamente:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

Formato per il caricamento di un certificato con una coppia di chiavi RSA

Le dimensioni delle chiavi consentite per la coppia di chiavi RSA appartenente al certificato host sono 2048, 3072 e 4096. Certificato con una coppia di chiavi * RSA generata esternamente*:

```
-----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-----
```

Una volta caricato il certificato, riavviare l'istanza di Active IQ Unified Manager per rendere effettive le modifiche.

Verifica durante il caricamento dei certificati generati esternamente

Il sistema esegue controlli durante il caricamento di un certificato generato mediante strumenti esterni. Se uno dei controlli non riesce, il certificato viene rifiutato. Sono incluse anche le validazioni per i certificati generati dalla CSR all'interno del prodotto e per i certificati generati utilizzando strumenti esterni.

- La chiave privata nell'input viene convalidata in base al certificato host nell'input.
- Il nome comune (CN) nel certificato host viene verificato in base all'FQDN dell'host.

- Il nome comune (CN) del certificato host non deve essere vuoto o vuoto e non deve essere impostato su localhost.
- La data di inizio della validità non deve essere futura e la data di scadenza del certificato non deve essere passata.
- Se esiste una CA o una CA intermedia, la data di inizio della validità del certificato non deve essere futura e la data di scadenza della validità non deve essere passata.

La chiave privata nell'input non deve essere crittografata. Se sono presenti chiavi private crittografate, queste vengono rifiutate dal sistema.

Esempio 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Esempio 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Esempio 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Descrizioni delle pagine per la gestione dei certificati

È possibile utilizzare la pagina HTTPS Certificate (certificato HTTPS) per visualizzare i certificati di protezione correnti e generare nuovi certificati HTTPS.

Pagina del certificato HTTPS

La pagina HTTPS Certificate (certificato HTTPS) consente di visualizzare il certificato di protezione corrente, scaricare una richiesta di firma del certificato, generare un nuovo certificato HTTPS autofirmato o installare un nuovo certificato HTTPS.

Se non è stato generato un nuovo certificato HTTPS autofirmato, il certificato visualizzato in questa pagina corrisponde al certificato generato durante l'installazione.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Scarica richiesta firma certificato HTTPS**

  Scarica una richiesta di certificazione per il certificato HTTPS attualmente installato. Il browser richiede di salvare il file <hostname>.csr in modo da fornire il file a un'autorità di certificazione per la firma.

- **Installare il certificato HTTPS**

  Consente di caricare e installare un certificato di sicurezza dopo che un'autorità di certificazione ha firmato e restituito il certificato. Il nuovo certificato è in vigore dopo il riavvio del server di gestione.

- **Rigenera certificato HTTPS**

  Consente di generare un nuovo certificato HTTPS autofirmato, che sostituisce il certificato di protezione corrente. Il nuovo certificato è in vigore dopo il riavvio di Unified Manager.

Finestra di dialogo Rigenera certificato HTTPS

La finestra di dialogo Rigenera certificato HTTPS consente di personalizzare le informazioni di protezione e generare un nuovo certificato HTTPS con tali informazioni.

In questa pagina vengono visualizzate le informazioni sul certificato corrente.

La selezione "Regenerate using Current Certificate Attributes" e "Update the Current Certificate Attributes" consente di rigenerare il certificato con le informazioni correnti o di generare un certificato con nuove informazioni.

- **Nome comune**

  Obbligatorio. Il nome di dominio completo (FQDN) che si desidera proteggere.

  Nelle configurazioni ad alta disponibilità di Unified Manager, utilizzare l'indirizzo IP virtuale.

- **E-mail**

  Opzionale. Un indirizzo e-mail per contattare l'organizzazione, in genere l'indirizzo e-mail dell'amministratore dei certificati o del reparto IT.

- **Azienda**

  Opzionale. In genere, il nome della società.

- **Reparto**

  Opzionale. Il nome del reparto della società.

- **Città**

  Opzionale. La località della tua azienda.

- **Stato**

Opzionale. L’ubicazione dello stato o della provincia, non abbreviata, dell’azienda.

- **Paese**

  Opzionale. L’ubicazione del paese dell’azienda. Si tratta in genere di un codice ISO di due lettere del paese.

- **Nomi alternativi**

  Obbligatorio. Nomi di dominio aggiuntivi non primari che possono essere utilizzati per accedere a questo server oltre all’host locale o ad altri indirizzi di rete esistenti. Separare ciascun nome alternativo con una virgola.

  Selezionare la casella di controllo “Exclude local identifying information (e.g. localhost)” (Escludi informazioni di identificazione locale) se si desidera rimuovere le informazioni di identificazione locale dal campo dei nomi alternativi nel certificato. Quando questa casella di controllo è selezionata, solo i dati immessi nel campo vengono utilizzati nel campo nomi alternativi. Se lasciato vuoto, il certificato risultante non avrà alcun campo di nomi alternativi.

- **DIMENSIONE DELLA CHIAVE (ALGORITMO CHIAVE: RSA)**

  L’algoritmo delle chiavi è impostato su RSA. È possibile selezionare una delle dimensioni delle chiavi: 2048, 3072 o 4096 bit. La dimensione predefinita della chiave è impostata su 2048 bit.

- **PERIODO DI VALIDITÀ**

  Il periodo di validità predefinito è 397 giorni. Se è stato eseguito l’aggiornamento da una versione precedente, la validità del certificato precedente potrebbe essere invariata.

Per ulteriori informazioni, vedere "Generazione di certificati HTTPS".

Monitorare e gestire lo storage

Introduzione a Active IQ Unified Manager

Active IQ Unified Manager (in precedenza Unified Manager di OnCommand) consente di monitorare e gestire lo stato di salute e le performance dei sistemi storage ONTAP da una singola interfaccia.

Unified Manager offre le seguenti funzionalità:

- Rilevamento, monitoraggio e notifiche per i sistemi installati con il software ONTAP.
- Dashboard per mostrare lo stato di capacità, sicurezza e performance dell'ambiente.
- Miglioramento dell'infrastruttura di avvisi, eventi e soglie.
- Visualizza grafici dettagliati che illustrano l'attività dei carichi di lavoro nel tempo, inclusi IOPS (operazioni), Mbps (throughput), latenza (tempo di risposta), utilizzo, capacità delle performance e rapporto cache.
- Identifica i carichi di lavoro che stanno utilizzando in eccesso i componenti del cluster e i carichi di lavoro le cui performance sono influenzate dall'aumento dell'attività.
- Fornisce le azioni correttive suggerite che possono essere eseguite per risolvere determinati incidenti ed eventi e un pulsante "Correggi" per alcuni eventi, in modo da poter risolvere il problema immediatamente.
- Si integra con OnCommand Workflow Automation per eseguire flussi di lavoro di protezione automatizzati.
- Possibilità di creare nuovi carichi di lavoro, come una LUN o una condivisione di file, direttamente da Unified Manager e assegnare un livello di servizio delle performance per definire gli obiettivi di performance e storage per gli utenti che accedono all'applicazione utilizzando tale carico di lavoro.

Introduzione al monitoraggio dello stato di salute di Active IQ Unified Manager

Active IQ Unified Manager (in precedenza Unified Manager di OnCommand) consente di monitorare un gran numero di sistemi che eseguono il software ONTAP attraverso un'interfaccia utente centralizzata. L'infrastruttura server di Unified Manager offre scalabilità, supportabilità e funzionalità avanzate di monitoraggio e notifica.

Le funzionalità chiave di Unified Manager includono il monitoraggio, gli avvisi, la gestione della disponibilità e della capacità dei cluster, la gestione delle funzionalità di protezione e il raggruppamento dei dati diagnostici e l'invio al supporto tecnico.

È possibile utilizzare Unified Manager per monitorare i cluster. Quando si verificano problemi nel cluster, Unified Manager notifica all'utente i dettagli di tali problemi attraverso gli eventi. Alcuni eventi forniscono anche un'azione correttiva che è possibile intraprendere per risolvere i problemi. È possibile configurare gli avvisi per gli eventi in modo che, quando si verificano problemi, si riceva una notifica tramite e-mail e trap SNMP.

È possibile utilizzare Unified Manager per gestire gli oggetti di storage nel proprio ambiente associandoli alle annotazioni. È possibile creare annotazioni personalizzate e associare dinamicamente cluster, storage virtual machine (SVM) e volumi con le annotazioni attraverso le regole.

È inoltre possibile pianificare i requisiti di storage degli oggetti cluster utilizzando le informazioni fornite nei grafici di capacità e integrità per il rispettivo oggetto cluster.

Capacità fisica e logica

Unified Manager utilizza i concetti di spazio fisico e logico utilizzati per gli oggetti di storage ONTAP.

- Capacità fisica: Lo spazio fisico si riferisce ai blocchi fisici di storage utilizzati nel volume. La "capacità fisica utilizzata" è generalmente inferiore alla capacità logica utilizzata a causa della riduzione dei dati dalle funzionalità di efficienza dello storage (come deduplica e compressione).
- Capacità logica: Lo spazio logico si riferisce allo spazio utilizzabile (i blocchi logici) in un volume. Lo spazio logico si riferisce al modo in cui lo spazio teorico può essere utilizzato, senza tenere conto dei risultati della deduplica o della compressione. "Spazio logico utilizzato" è lo spazio fisico utilizzato e i risparmi derivanti dalle funzionalità di efficienza dello storage (come deduplica e compressione) configurate. Questa misurazione appare spesso più grande della capacità fisica utilizzata perché include copie Snapshot, cloni e altri componenti e non riflette la compressione dei dati e altre riduzioni dello spazio fisico. Pertanto, la capacità logica totale potrebbe essere superiore allo spazio fornito.

Unità di misura della capacità

Unified Manager calcola la capacità dello storage in base a unità binarie di 1024 (2^{10}) byte. In ONTAP 9.10.0 e versioni precedenti, queste unità venivano visualizzate come KB, MB, GB, TB e PB. A partire da ONTAP 9.10.1, vengono visualizzati in Unified Manager come KiB, MiB, GiB, TIB e PIB.

Le unità utilizzate per il throughput continuano a essere kilobyte per secondo (Kbps), Megabyte per secondo (Mbps), Gigabyte per secondo (Gbps) o terabyte per secondo (Tbps) e così via, per tutte le versioni di ONTAP.

Unità di capacità visualizzata in Unified Manager per ONTAP 9.10.0 e versioni precedenti	Unità di capacità visualizzata in Unified Manager per ONTAP 9.10.1	Calcolo	Valore in byte
KB	KiB	1024	1024 byte
MB	MIB	1024 * 1024	1,048,576 byte
GB	Gib	1024 * 1024 * 1024	1,073,741,824 byte
TB	TIB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 byte

Introduzione al monitoraggio delle performance di Active IQ Unified Manager

Active IQ Unified Manager (in precedenza Unified Manager di OnCommand) offre funzionalità di monitoraggio delle performance e analisi delle cause principali degli eventi per i sistemi che eseguono il software NetApp ONTAP.

Unified Manager ti aiuta a identificare i carichi di lavoro che stanno utilizzando in eccesso i componenti del cluster e a ridurre le performance di altri carichi di lavoro sul cluster. La definizione dei criteri di soglia delle performance consente inoltre di specificare i valori massimi per determinati contatori delle performance in modo che gli eventi vengano generati quando la soglia viene superata. Unified Manager avvisa l'utente in merito a questi eventi di performance in modo da poter intraprendere azioni correttive e riportare le

performance ai normali livelli operativi. È possibile visualizzare e analizzare gli eventi nell'interfaccia utente di Unified Manager.

Unified Manager monitora le performance di due tipi di carichi di lavoro:

- Carichi di lavoro definiti dall'utente

  Questi carichi di lavoro sono costituiti da volumi FlexVol e volumi FlexGroup creati nel cluster.

- Carichi di lavoro definiti dal sistema

  Questi carichi di lavoro sono costituiti da attività di sistema interne.

Utilizzo delle API REST di Unified Manager

Active IQ Unified Manager offre API REST per visualizzare le informazioni relative al monitoraggio e alla gestione dell'ambiente di storage. Le API consentono inoltre il provisioning e la gestione degli oggetti storage in base alle policy.

È inoltre possibile eseguire API ONTAP su tutti i cluster gestiti da ONTAP utilizzando il gateway API supportato da Unified Manager.

Per informazioni sulle API REST di Unified Manager, vedere "Introduzione alle API REST di Active IQ Unified Manager".

Funzioni del server Unified Manager

L'infrastruttura server di Unified Manager è costituita da un'unità di raccolta dati, un database e un server applicazioni. Fornisce servizi di infrastruttura come rilevamento, monitoraggio, RBAC (role-based access control), audit e logging.

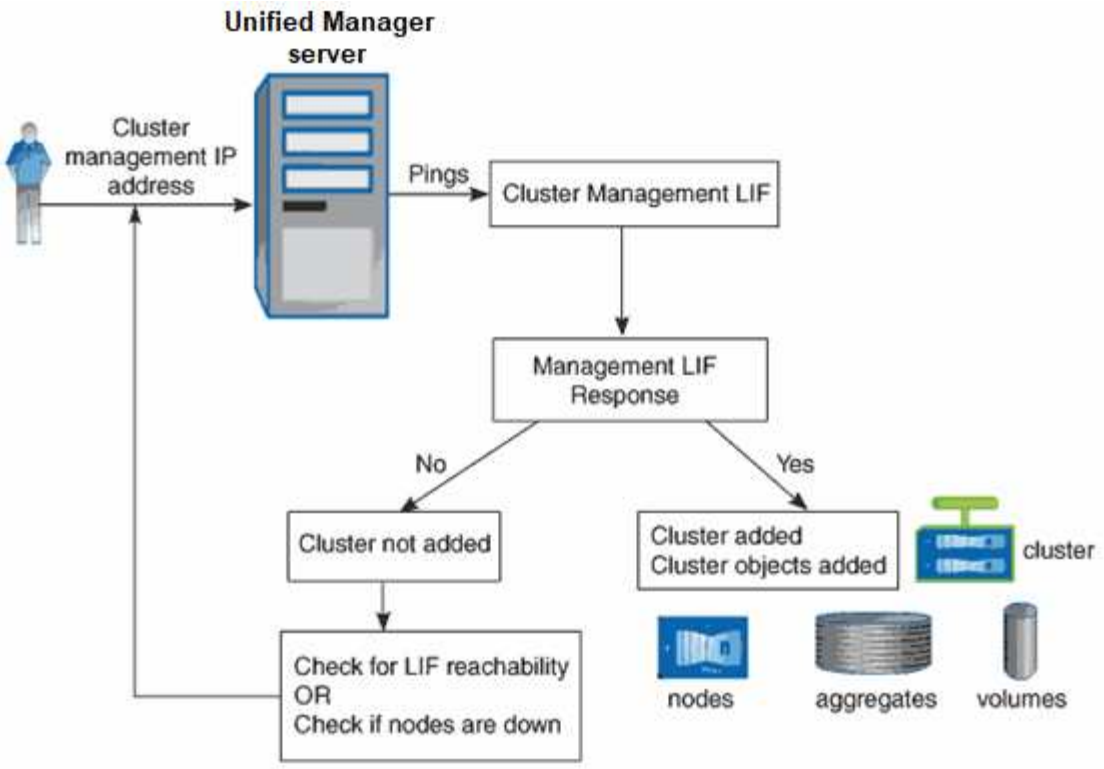
Unified Manager raccoglie le informazioni sul cluster, memorizza i dati nel database e li analizza per verificare l'eventuale presenza di problemi nel cluster.

Come funziona il processo di rilevamento

Dopo aver aggiunto il cluster a Unified Manager, il server rileva gli oggetti del cluster e li aggiunge al database. La comprensione del funzionamento del processo di rilevamento consente di gestire i cluster dell'organizzazione e i relativi oggetti.

L'intervallo di monitoraggio predefinito è di 15 minuti: Se si aggiunge un cluster al server Unified Manager, sono necessari 15 minuti per visualizzare i dettagli del cluster nell'interfaccia utente di Unified Manager.

La seguente immagine illustra il processo di rilevamento in Active IQ Unified Manager:



Comprensione dell'interfaccia utente

L'interfaccia utente di Unified Manager è costituita principalmente da una dashboard che fornisce una vista a colpo d'occhio degli oggetti monitorati. L'interfaccia utente consente inoltre di visualizzare tutti gli oggetti del cluster.

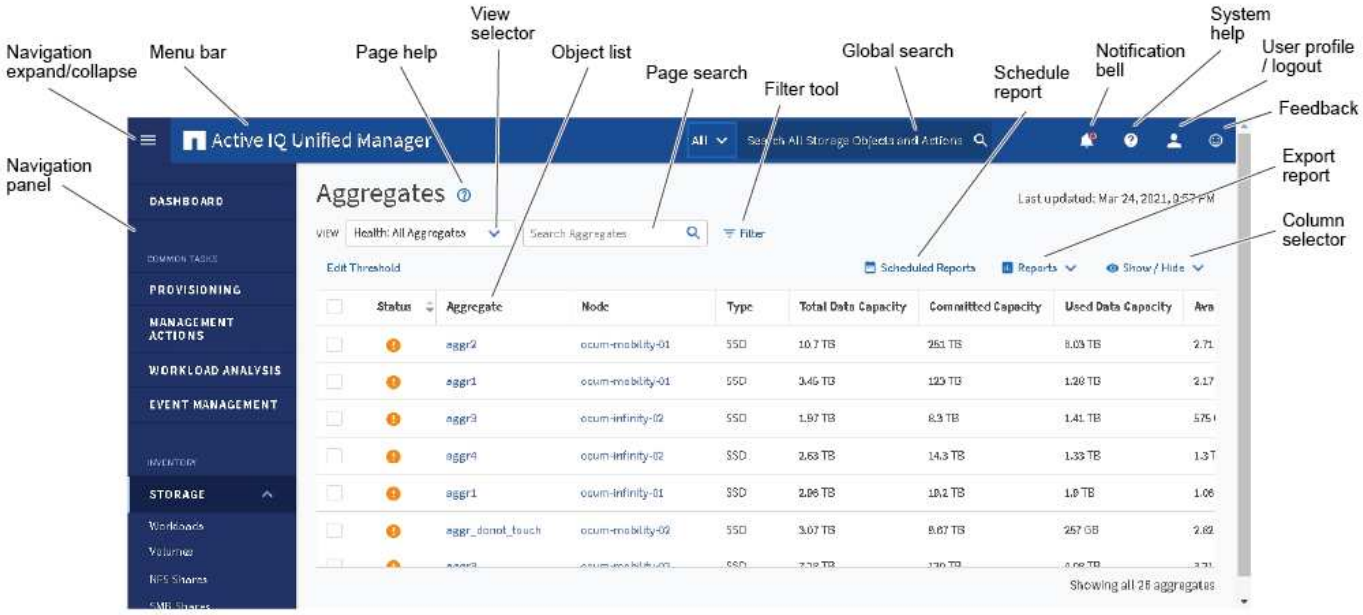
È possibile selezionare una vista preferita e utilizzare i pulsanti di azione, se necessario. La configurazione dello schermo viene salvata in un'area di lavoro in modo che tutte le funzionalità richieste siano disponibili all'avvio di Unified Manager. Tuttavia, quando si passa da una vista all'altra e poi si torna indietro, la vista potrebbe non essere la stessa.

Layout tipici delle finestre

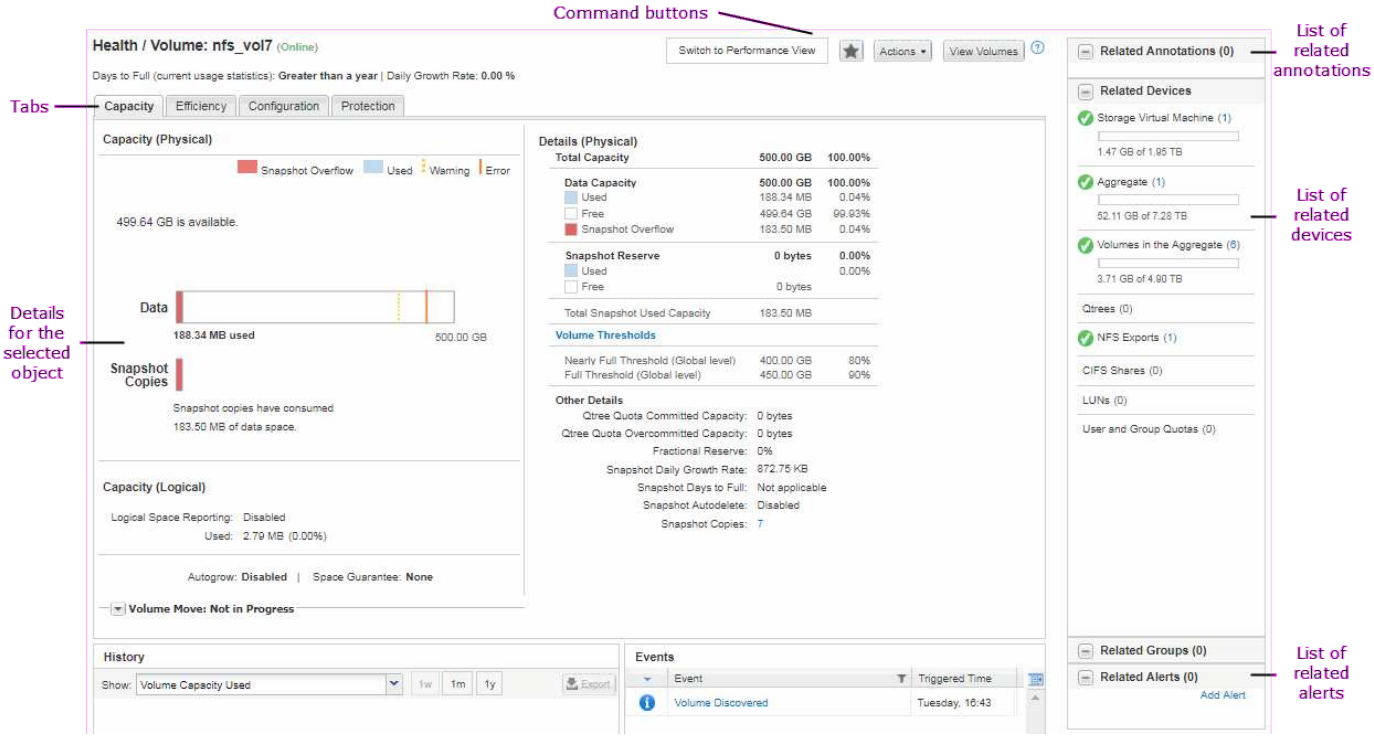
La comprensione dei layout tipici delle finestre consente di navigare e utilizzare Active IQ Unified Manager in modo efficace. La maggior parte delle finestre di Unified Manager sono simili a uno dei due layout generali: Elenco oggetti o dettagli. L'impostazione di visualizzazione consigliata è di almeno 1280 x 1024 pixel.

Non tutte le finestre contengono tutti gli elementi dei seguenti diagrammi.

Layout della finestra dell'elenco oggetti



Layout della finestra Dettagli oggetto



Personalizzazione del layout delle finestre

Active IQ Unified Manager consente di personalizzare il layout delle informazioni nelle pagine degli oggetti di storage e di rete. Personalizzando le finestre, è possibile controllare quali dati visualizzare e come visualizzarli.

- **Ordinamento**

  È possibile fare clic sull'intestazione della colonna per modificare l'ordinamento delle voci della colonna.

Quando si fa clic sull'intestazione della colonna, le frecce di ordinamento (e.) viene visualizzato per la colonna.

- **Filtraggio**

  È possibile fare clic sull'icona del filtro ( ) per applicare filtri per personalizzare la visualizzazione delle informazioni sulle pagine degli oggetti di storage e di rete in modo che vengano visualizzate solo le voci corrispondenti alle condizioni fornite. I filtri vengono applicati dal riquadro filtri.

  Il pannello filtri consente di filtrare la maggior parte delle colonne in base alle opzioni selezionate. Ad esempio, nella vista Health: All Volumes (Salute: Tutti i volumi), è possibile utilizzare il pannello Filters (filtri) per visualizzare tutti i volumi offline selezionando l'opzione di filtro appropriata in state (Stato).

  Le colonne relative alla capacità in qualsiasi elenco visualizzano sempre i dati della capacità in unità appropriate arrotondate a due punti decimali. Ciò vale anche quando si filtrano le colonne di capacità. Ad esempio, se si utilizza il filtro nella colonna capacità totale dei dati nella vista Salute: Tutti gli aggregati per filtrare i dati superiori a 20.45 GB, la capacità effettiva di 20.454 GB viene visualizzata come 20.45 GB. Analogamente, se si filtrano dati inferiori a 20.45 GB, la capacità effettiva di 20.449 GB viene visualizzata come 20.45 GB.

  Se si utilizza il filtro nella colonna Available Data % nella vista Health: All aggregates (Salute: Tutti gli aggregati) per filtrare i dati superiori al 20.45%, la capacità effettiva del 20.454% viene visualizzata come 20.45%. Analogamente, se si filtrano dati inferiori al 20.45%, la capacità effettiva del 20.449% viene visualizzata come 20.45%.

- **Nascondere o mostrare le colonne**

  È possibile fare clic sull'icona di visualizzazione delle colonne (**Mostra/Nascondi**) per selezionare le colonne da visualizzare. Una volta selezionate le colonne appropriate, è possibile riordinarle trascinandole con il mouse.

- **Ricerca in corso**

  È possibile utilizzare la casella di ricerca per cercare determinati attributi degli oggetti per perfezionare l'elenco degli elementi nella pagina di inventario. Ad esempio, puoi inserire "cloud" per perfezionare l'elenco dei volumi nella pagina di inventario dei volumi e visualizzare tutti i volumi che contengono la parola "cloud".

- **Esportazione dei dati**

  È possibile fare clic sul pulsante **Report** (o sul pulsante **Esporta**) per esportare i dati in valori separati da virgole `(.csv)` file, `(.pdf)` O Microsoft Excel `(.xlsx)` archiviare e utilizzare i dati esportati per creare report.

Utilizzo della Guida di Unified Manager

La Guida contiene informazioni su tutte le funzioni incluse in Active IQ Unified Manager. È possibile utilizzare il sommario, l'indice o lo strumento di ricerca per trovare informazioni sulle funzionalità e su come utilizzarle.

La Guida è disponibile da ciascuna scheda e dalla barra dei menu dell'interfaccia utente di Unified Manager.

Lo strumento di ricerca nella Guida non funziona per parole parziali.

- Per informazioni su campi o parametri specifici, fare clic su .
- Per visualizzare tutti i contenuti della Guida, fare clic su > **Guida/documentazione** nella barra dei menu.

  È possibile trovare informazioni più dettagliate espandendo qualsiasi parte del sommario nel riquadro di navigazione.

- Per cercare nel contenuto della Guida, fare clic sulla scheda **Cerca** nel riquadro di navigazione, digitare la parola o la serie di parole che si desidera trovare e fare clic su **Vai!**
- Per stampare gli argomenti della Guida, fare clic sull'icona della stampante.

Aggiunta di segnalibri agli argomenti della guida preferiti

Nella scheda Help Favorites (Preferiti della Guida), è possibile aggiungere ai preferiti gli argomenti della Guida utilizzati di frequente. I segnalibri di aiuto consentono di accedere rapidamente ai tuoi argomenti preferiti.

Fasi

1. Accedere all'argomento della Guida che si desidera aggiungere come preferito.
2. Fare clic su **Preferiti**, quindi su **Aggiungi**.

Ricerca di oggetti storage

Per accedere rapidamente a un oggetto specifico, è possibile utilizzare il campo **Search All Storage Objects** (Cerca tutti gli oggetti di storage) nella parte superiore della barra dei menu. Questo metodo di ricerca globale in tutti gli oggetti consente di individuare rapidamente oggetti specifici in base al tipo. I risultati della ricerca sono ordinati in base al tipo di oggetto di storage ed è possibile filtrarli ulteriormente in base all'oggetto utilizzando il menu a discesa.

Cosa ti serve

- Per eseguire questa attività, è necessario disporre di uno dei seguenti ruoli: Operatore, Amministratore dell'applicazione o Amministratore dello storage.
- Una ricerca valida deve contenere almeno tre caratteri.

Quando si utilizza il valore del menu a discesa "all", la ricerca globale visualizza il numero totale di risultati trovati in tutte le categorie di oggetti, con un massimo di 25 risultati di ricerca per ciascuna categoria di oggetti. È possibile selezionare un tipo di oggetto specifico dal menu a discesa per perfezionare la ricerca all'interno di un tipo di oggetto specifico. In questo caso, l'elenco restituito non è limitato ai primi 25 oggetti.

I tipi di oggetti che è possibile cercare includono:

- Cluster
- Nodi
- VM di storage
- Aggregati
- Volumi

- Qtree
- Condivisioni SMB
- Condivisioni NFS
- Quote utente o di gruppo
- LUN
- NVMe Namespace
- Gruppi di iniziatori
- Iniziatori
- Gruppo di coerenza

L'immissione del nome di un workload restituisce l'elenco dei workload nella categoria dei volumi o LUN appropriata.

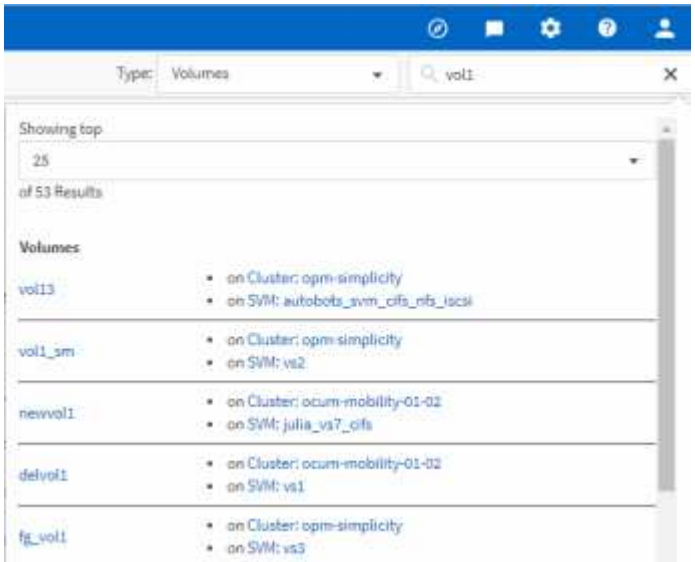
È possibile fare clic su qualsiasi oggetto nei risultati della ricerca per accedere alla pagina Health details relativa all'oggetto. Se non esiste una pagina di integrità diretta per un oggetto, viene visualizzata la pagina di integrità dell'oggetto padre. Ad esempio, durante la ricerca di un LUN specifico, viene visualizzata la pagina dei dettagli SVM in cui risiede il LUN.

Le porte e i LIF non sono ricercabili nella barra di ricerca globale.

Fasi

1. Selezionare un tipo di oggetto dal menu per perfezionare i risultati della ricerca solo per un singolo tipo di oggetto.
2. Digitare almeno tre caratteri del nome dell'oggetto nel campo **Cerca tutti gli oggetti di storage**.

   In questo esempio, nella casella a discesa è selezionato il tipo di oggetto Volumes. Digitando "vol1" nel campo **Search All Storage Objects** viene visualizzato un elenco di tutti i volumi i cui nomi contengono questi caratteri.



Esportazione dei dati di storage come report

È possibile esportare i dati di storage in diversi formati di output e quindi utilizzare i dati esportati per creare report. Ad esempio, se sono presenti 10 eventi critici che non sono stati risolti, è possibile esportare i dati dalla pagina dell'inventario di Event Management per creare un report, quindi inviare il report agli amministratori che possono risolvere i problemi.

È possibile esportare i dati in un `.csv` file, `.xlsx` file, o. `.pdf` Documentare dalle pagine di inventario **Storage** e **Network** e utilizzare i dati esportati per creare report. Esistono altre posizioni nel prodotto, solo dove `.csv` oppure `.pdf` è possibile generare file.

Fasi

1. Eseguire una delle seguenti operazioni:

Se si desidera esportare…	Eseguire questa operazione…
Dettagli dell'inventario degli oggetti di storage	Fare clic su **Storage** o **Network** dal menu di navigazione a sinistra, quindi selezionare un oggetto di storage. Scegliere una delle viste fornite dal sistema o qualsiasi vista personalizzata creata.
Dettagli del gruppo di policy QoS	Fare clic su **Storage** > **QoS Policy Groups** (gruppi policy QoS) dal menu di navigazione a sinistra.
Dettagli sulla capacità dello storage e sulla cronologia della protezione	Fare clic su **Storage** > **Aggregates** o **Storage** > **Volumes**, quindi selezionare un singolo aggregato o volume.
Dettagli dell'evento	Fare clic su **Event Management** (Gestione eventi) dal menu di navigazione a sinistra.
Primi 10 dettagli sulle performance dell'oggetto storage	Fare clic su **Storage** > **Clusters** > **Performance:All Clusters**, quindi selezionare un cluster e scegliere la scheda **Top Performers**. Quindi selezionare un oggetto di storage e un contatore delle performance.

2. Fare clic sul pulsante **Report** (o sul pulsante **Export** in alcune pagine dell'interfaccia utente).
3. Fare clic su **Download CSV**, **Download PDF** o **Download Excel** per confermare la richiesta di esportazione.

   Dalla scheda Top Performer è possibile scegliere di scaricare un report delle statistiche per il singolo cluster visualizzato o per tutti i cluster del data center.

   Il file viene scaricato.

4. Aprire il file nell'applicazione appropriata.

Informazioni correlate

"Pagina di inventario di salute/cluster"

"Pianificazione di un report"

Filtraggio del contenuto della pagina di inventario

È possibile filtrare i dati delle pagine di inventario in Unified Manager per individuare rapidamente i dati in base a criteri specifici. È possibile utilizzare il filtraggio per restringere il contenuto delle pagine di Unified Manager e visualizzare solo i risultati desiderati. Questo offre un metodo molto efficiente per visualizzare solo i dati che ti interessano.

Utilizzare **Filtering** per personalizzare la vista griglia in base alle proprie preferenze. Le opzioni di filtro disponibili si basano sul tipo di oggetto visualizzato nella griglia. Se i filtri sono attualmente applicati, il numero di filtri applicati viene visualizzato a destra del pulsante Filter (filtro).

Sono supportati tre tipi di parametri di filtro.

Parametro	Convalida
Stringa (testo)	Gli operatori sono **contains**, **inizia con**, **termina con** e **non contiene**.
Numero	Gli operatori sono **maggiori di**, **minori di**, **negli ultimi** e **tra**.
Enum (testo)	Gli operatori sono **IS** e **non**.

I campi Column (colonna), Operator (operatore) e Value (valore) sono obbligatori per ciascun filtro; i filtri disponibili riflettono le colonne filtrabili nella pagina corrente. Il numero massimo di filtri che è possibile applicare è quattro. I risultati filtrati si basano su parametri di filtro combinati. I risultati filtrati si applicano a tutte le pagine della ricerca filtrata, non solo alla pagina attualmente visualizzata.

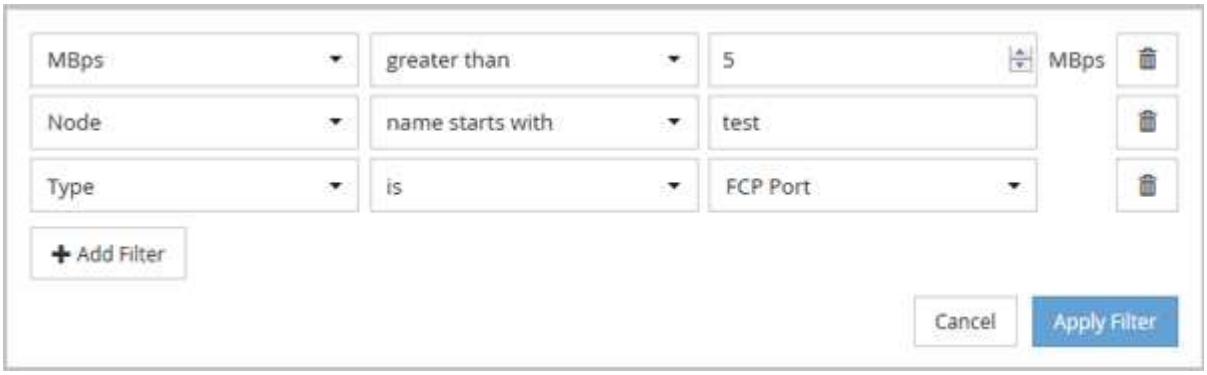
È possibile aggiungere filtri utilizzando il pannello di filtraggio.

1. Nella parte superiore della pagina, fare clic sul pulsante **Filter** (filtro). Viene visualizzato il pannello Filtering (filtraggio).
2. Fare clic sull'elenco a discesa a sinistra e selezionare un oggetto, ad esempio *Cluster* o un contatore delle prestazioni.
3. Fare clic sull'elenco a discesa centrale e selezionare l'operatore che si desidera utilizzare.
4. Nell'ultimo elenco, selezionare o inserire un valore per completare il filtro per l'oggetto.
5. Per aggiungere un altro filtro, fare clic su **+Aggiungi filtro**. Viene visualizzato un campo di filtro aggiuntivo. Completare questo filtro seguendo la procedura descritta nei passaggi precedenti. Si noti che quando si aggiunge il quarto filtro, il pulsante **+Aggiungi filtro** non viene più visualizzato.
6. Fare clic su **Applica filtro**. Le opzioni di filtro vengono applicate alla griglia e il numero di filtri viene visualizzato a destra del pulsante Filter (filtro).
7. Utilizzare il pannello di filtraggio per rimuovere i singoli filtri facendo clic sull'icona del cestino a destra del filtro da rimuovere.

8. Per rimuovere tutti i filtri, fare clic su **Reset** nella parte inferiore del pannello di filtraggio.

Esempio di filtraggio

La figura mostra il pannello di filtraggio con tre filtri. Il pulsante **+Aggiungi filtro** viene visualizzato quando si dispone di un numero inferiore al massimo di quattro filtri.



Dopo aver fatto clic su **Apply Filter** (Applica filtro), il pannello Filtering (filtraggio) si chiude, applica i filtri e mostra il numero di filtri applicati (3).

Visualizzazione degli eventi attivi dal campanello di notifica

Il campanello di notifica ( ) Nella barra dei menu fornisce un modo rapido per visualizzare gli eventi attivi più importanti che Unified Manager sta monitorando.

L'elenco degli eventi attivi consente di visualizzare il numero totale di eventi critici, di errore, di avviso e di aggiornamento su tutti i cluster. Questo elenco include gli eventi dei 7 giorni precedenti e non gli eventi relativi alle informazioni. È possibile fare clic su un collegamento per visualizzare l'elenco degli eventi più interessati.

Si noti che quando un cluster non è raggiungibile, Unified Manager visualizza queste informazioni in questa pagina. È possibile visualizzare informazioni dettagliate su un cluster non raggiungibile facendo clic sul pulsante **Dettagli**. Questa azione apre la pagina Dettagli evento. In questa pagina vengono visualizzati anche i problemi di monitoraggio della scalabilità, come lo spazio insufficiente o la RAM sulla stazione di gestione.

Fasi

1. Dalla barra dei menu, fare clic su .
2. Per visualizzare i dettagli relativi agli eventi attivi, fare clic sul collegamento di testo dell'evento, ad esempio "capacità 2" o "prestazioni 4".

Monitoraggio e gestione dei cluster dalla dashboard

La dashboard fornisce informazioni cumulative a colpo d'occhio sullo stato attuale dei sistemi ONTAP monitorati. La dashboard fornisce "panel" che consentono di valutare la capacità, le performance e lo stato di sicurezza generale dei cluster monitorati.

Inoltre, è possibile risolvere alcuni problemi di ONTAP direttamente dall'interfaccia utente di Unified Manager invece di dover utilizzare Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP.

Nella parte superiore della dashboard è possibile scegliere se visualizzare le informazioni per tutti i cluster monitorati o per un singolo cluster. È possibile iniziare visualizzando lo stato di tutti i cluster e quindi eseguire il

drill-down dei singoli cluster quando si desidera visualizzare informazioni dettagliate.

Alcuni dei pannelli elencati di seguito potrebbero non essere visualizzati nella pagina in base alla configurazione.

Pannelli	Descrizione
Azioni di gestione	Quando Unified Manager è in grado di diagnosticare e determinare una singola risoluzione di un problema, tali risoluzioni vengono visualizzate in questo pannello con il pulsante **Correggi**.
Capacità	Visualizza la capacità totale e utilizzata per il Tier locale e il Tier cloud, oltre al numero di giorni in cui la capacità locale raggiunge il limite massimo.
Capacità delle performance	Visualizza il valore della capacità delle performance per ciascun cluster e il numero di giorni in cui la capacità delle performance raggiunge il limite massimo.
IOPS del carico di lavoro	Visualizza il numero totale di workload attualmente in esecuzione in un determinato intervallo di IOPS.
Performance del carico di lavoro	Visualizza il numero totale di carichi di lavoro conformi e non conformi assegnati a ciascun livello di servizio delle performance definito.
Sicurezza	Visualizza il numero di cluster conformi o non conformi, il numero di SVM conformi o non conformi e il numero di volumi crittografati o non crittografati.
Protezione	Visualizza il numero di VM storage protette dalla relazione SVM-DR, i volumi protetti dalla relazione SnapMirror, i volumi protetti da Snapshot e i cluster protetti da MetroCluster.
Panoramica sull'utilizzo	Visualizza i cluster ordinati per IOPS più elevati, throughput più elevato (Mbps) o capacità fisica più elevata utilizzata.

Pagina del dashboard

La pagina Dashboard contiene "pannelli" che visualizzano l'elevato livello di capacità, performance e sicurezza dei cluster monitorati. Questa pagina fornisce anche un pannello azioni di gestione che elenca le correzioni che Unified Manager può apportare per risolvere determinati eventi.

La maggior parte dei pannelli visualizza anche il numero di eventi attivi in tale categoria e il numero di nuovi

eventi aggiunti nelle 24 ore precedenti. Queste informazioni consentono di decidere quali cluster è necessario analizzare ulteriormente per risolvere gli eventi. Facendo clic sugli eventi vengono visualizzati gli eventi principali e viene fornito un collegamento alla pagina dell'inventario Gestione eventi filtrata per visualizzare gli eventi attivi in tale categoria.

Nella parte superiore della dashboard è possibile selezionare se visualizzare le informazioni per tutti i cluster monitorati ("tutti i cluster") o per un singolo cluster. È possibile iniziare visualizzando lo stato di tutti i cluster e quindi eseguire il drill-down dei singoli cluster quando si desidera visualizzare informazioni dettagliate.

Alcuni dei pannelli elencati di seguito vengono visualizzati sulla dashboard in base alla configurazione.

Pannello azioni di gestione

Unified Manager può diagnosticare accuratamente alcuni problemi e fornire una singola soluzione. Quando disponibili, queste risoluzioni vengono visualizzate in questo pannello con un pulsante **Fix it** o **Fix all**. È possibile risolvere questi problemi immediatamente da Unified Manager invece di dover utilizzare Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP. Per visualizzare tutti i problemi, fare clic su Vedi "Risoluzione dei problemi di ONTAP direttamente da Unified Manager" per ulteriori informazioni.

Pannello capacità

Durante la visualizzazione di tutti i cluster, questo pannello visualizza la capacità fisica utilizzata (dopo aver applicato il risparmio di efficienza dello storage) e la capacità fisica disponibile (senza includere il potenziale risparmio di efficienza dello storage) per ciascun cluster, il numero di giorni in cui i dischi sono previsti per essere pieni, E il rapporto di riduzione dei dati basato sulle impostazioni di efficienza dello storage ONTAP configurate. Inoltre, elenca la capacità utilizzata per qualsiasi Tier cloud configurato. Facendo clic sul grafico a barre si accede alla pagina di inventario degli aggregati per quel cluster. Facendo clic sul testo "Days to Full" (giorni da completare) viene visualizzato un messaggio che identifica l'aggregato con il numero minimo di giorni di capacità rimanenti; fare clic sul nome dell'aggregato per visualizzare ulteriori dettagli.

Durante la visualizzazione di un singolo cluster, questo pannello visualizza la capacità fisica utilizzata e la capacità fisica disponibile per gli aggregati di dati ordinati per ciascun tipo di disco nel Tier locale e per il Tier cloud. Facendo clic sul grafico a barre di un tipo di disco, si accede alla pagina di inventario dei volumi per i volumi che utilizzano quel tipo di disco.

Pannello Performance Capacity (capacità delle performance)

Durante la visualizzazione di tutti i cluster, questo pannello visualizza il valore della capacità delle performance per ciascun cluster (media nell'ora precedente) e il numero di giorni fino a quando la capacità delle performance non raggiunge il limite massimo (in base al tasso di crescita giornaliero). Facendo clic sul grafico a barre si accede alla pagina di inventario dei nodi per quel cluster. Si noti che la pagina di inventario dei nodi visualizza la capacità di performance media nelle 72 ore precedenti. Facendo clic sul testo "Days to Full" (giorni da completare) viene visualizzato un messaggio che identifica il nodo con il numero minimo di giorni di capacità delle performance rimanenti; fare clic sul nome del nodo per visualizzare ulteriori dettagli.

Durante la visualizzazione di un singolo cluster, questo pannello visualizza i valori relativi alla percentuale di utilizzo della capacità di performance del cluster, agli IOPS totali e al throughput totale (MB/s) e il numero di giorni in cui ciascuna di queste tre metriche deve raggiungere il limite massimo.

Pannello IOPS del carico di lavoro

Durante la visualizzazione di un singolo cluster, questo pannello visualizza il numero totale di carichi di lavoro attualmente in esecuzione in un determinato intervallo di IOPS e indica il numero di ciascun tipo di disco

quando si sposta il cursore sul grafico.

Pannello delle performance del carico di lavoro

Questo pannello visualizza il numero totale di carichi di lavoro conformi e non conformi assegnati a ciascuna policy PSL (Performance Service Level). Visualizza anche il numero di workload a cui non è assegnato un PSL. Facendo clic su un grafico a barre si accede ai carichi di lavoro conformi assegnati a tale policy nella pagina carichi di lavoro. Facendo clic sul numero che segue il grafico a barre si passa ai carichi di lavoro conformi e non conformi assegnati a tale policy.

Pannello di sicurezza

Il pannello Security (sicurezza) presenta lo stato di sicurezza di alto livello per tutti i cluster o per un singolo cluster, a seconda della vista corrente. Questo pannello visualizza:

- un elenco degli eventi di sicurezza ricevuti nelle ultime 24 ore. Fare clic su un evento per visualizzare i dettagli nella pagina Dettagli evento
- lo stato di sicurezza del cluster (numero di cluster conformi e non conformi)
- Lo stato di sicurezza delle macchine virtuali dello storage (numero di macchine virtuali dello storage conformi e non conformi)
- lo stato di crittografia del volume (conteggio dei volumi crittografati o non crittografati)
- lo stato anti-ransomware del volume (numero di volumi con anti-ransomware attivati o disattivati)

È possibile fare clic sui grafici a barre dei cluster conformi e non conformi, dei VMS di storage, dei volumi crittografati e non crittografati e dello stato anti-ransomware del volume per accedere alle rispettive pagine e visualizzare i dettagli di sicurezza dei cluster filtrati, delle VM di storage e dei volumi.

La conformità è basata su "Guida al rafforzamento della sicurezza di NetApp per ONTAP 9". Fare clic sulla freccia destra nella parte superiore del pannello per visualizzare i dettagli di sicurezza per tutti i cluster nella pagina Security (sicurezza). Per informazioni, vedere "Visualizzazione dettagliata dello stato di sicurezza per cluster e VM di storage".

Pannello Data Protection (protezione dati)

Questo pannello visualizza il riepilogo della protezione dei dati per uno o tutti i cluster di un data center. Visualizza il numero totale di eventi di protezione dei dati, eventi MetroCluster e numero di eventi attivi generati nelle ultime 24 ore in ONTAP. Facendo clic sul link da ciascuno di questi eventi si accede alla pagina Dettagli evento. È possibile fare clic sul collegamento **View All** (Visualizza tutto) per visualizzare tutti gli eventi di protezione attivi nella pagina Event Management Inventory (inventario gestione eventi). Il pannello visualizza:

- Il numero di volumi in un cluster o di tutti i cluster in un data center protetti dalle copie Snapshot.
- Il numero di volumi in un cluster o di tutti i cluster in un data center protetti dalle relazioni SnapMirror. Per le relazioni SnapMirror, viene preso in considerazione il numero di volumi nel cluster di origine.
- Il numero di cluster o di tutti i cluster di un data center protetti dalla configurazione MetroCluster su IP o FC.
- Il numero di relazioni di volume con il ritardo RPO (Recovery Point Objective) di SnapMirror in base allo stato di ritardo.

Puoi passare il mouse per visualizzare i rispettivi conteggi e legende. È possibile fare clic sulla freccia destra nella parte superiore del pannello per visualizzare i dettagli di uno o di tutti i cluster nella pagina Data Protection (protezione dati). Inoltre, è possibile fare clic su:

- I grafici a barre dei volumi non protetti e dei volumi protetti dalle copie Snapshot consentono di accedere alla pagina volumi e visualizzare i dettagli.
- I grafici a barre dei cluster protetti o non protetti dalla configurazione MetroCluster consentono di accedere alla pagina Clusters e visualizzare i dettagli.
- I grafici a barre per tutte le relazioni vanno alla pagina Relazioni, dove i dettagli vengono filtrati in base al cluster di origine.

Per ulteriori informazioni, vedere "Visualizzazione dello stato di protezione del volume".

Pannello Panoramica sull'utilizzo

Durante la visualizzazione di tutti i cluster, è possibile scegliere di visualizzare i cluster in base agli IOPS più elevati, al throughput più elevato (MB/s) o alla capacità fisica più elevata utilizzata.

Durante la visualizzazione di un singolo cluster, è possibile scegliere di visualizzare i carichi di lavoro in base agli IOPS più elevati, al throughput più elevato (MB/s) o alla capacità logica più elevata utilizzata.

Informazioni correlate

"Risoluzione dei problemi con le soluzioni automatiche di Unified Manager"

"Visualizzazione di informazioni sugli eventi relativi alle performance"

"Gestire le performance utilizzando la capacità delle performance e le informazioni IOPS disponibili"

"Pagina dei dettagli relativi a volume/salute"

"Analisi e notifica degli eventi relativi alle performance"

"Descrizione dei tipi di severità degli eventi"

"Fonti di eventi relativi alle performance"

"Gestione degli obiettivi di sicurezza del cluster"

"Monitoraggio delle performance del cluster dalla pagina di destinazione del cluster di performance"

"Monitoraggio delle performance tramite le pagine Performance Inventory"

Gestione dei problemi o delle funzionalità di ONTAP direttamente da Unified Manager

È possibile risolvere alcuni problemi di ONTAP o gestire alcune funzionalità di ONTAP direttamente dall'interfaccia utente di Unified Manager, invece di dover utilizzare Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP. L'opzione "Mazioni di gestione" fornisce correzioni a una serie di problemi di ONTAP che hanno attivato eventi di Unified Manager.

È possibile risolvere i problemi direttamente dalla pagina azioni di gestione selezionando l'opzione **azioni di gestione** nel riquadro di navigazione a sinistra. Le azioni di gestione sono disponibili anche nel pannello azioni di gestione del dashboard, nella pagina Dettagli evento e nella selezione analisi carico di lavoro nel menu di navigazione a sinistra.

Unified Manager può diagnosticare accuratamente alcuni problemi e fornire una singola soluzione. Per alcune funzionalità di ONTAP, come il monitoraggio anti-ransomware, Unified Manager esegue controlli interni e consiglia azioni specifiche. Quando disponibili, tali risoluzioni vengono visualizzate in azioni di gestione con un pulsante **Correggi**. Fare clic sul pulsante **Correggi** per risolvere il problema. È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Unified Manager invia comandi ONTAP al cluster per eseguire la correzione richiesta. Una volta completata la correzione, l'evento diventa obsoleto.

Alcune azioni di gestione consentono di risolvere lo stesso problema su più oggetti di storage utilizzando il pulsante **Correggi tutto**. Ad esempio, potrebbero esserci 5 volumi con l'evento "Volume Space Full" (spazio volume pieno) che potrebbe essere risolto facendo clic sull'azione di gestione **Fix all** per "Enable volume autow" (attiva crescita automatica volume). Un click ti consente di risolvere questo problema su 5 volumi.

Per informazioni sui problemi e sulle funzionalità di ONTAP che è possibile gestire utilizzando la correzione automatica, vedere "Quali problemi possono risolvere Unified Manager".

Quali sono le opzioni disponibili quando viene visualizzato il pulsante Fix it o Fix All (Correggi tutto)

La pagina delle azioni di gestione fornisce il pulsante **Fix it** o **Fix all** per risolvere i problemi di cui Unified Manager è stato informato attraverso un evento.

Si consiglia di fare clic sui pulsanti per risolvere un problema, secondo necessità. Tuttavia, se non si è sicuri di voler risolvere il problema come consigliato da Unified Manager, è possibile eseguire le seguenti operazioni:

Cosa vuoi fare?	Azione
Chiedere a Unified Manager di risolvere il problema su tutti gli oggetti identificati.	Fare clic sul pulsante **Correggi tutto**.
Non risolvere il problema per nessuno degli oggetti identificati in questo momento e nascondere questa azione di gestione fino a quando l'evento non viene generato di nuovo.	Fare clic sulla freccia verso il basso e fare clic su **Elimina tutto**.
Risolvere il problema solo su alcuni degli oggetti identificati.	Fare clic sul nome dell'azione di gestione per espandere l'elenco e visualizzare tutte le singole azioni **Fix it**.quindi seguire la procedura per correggere o eliminare singole azioni di gestione.

Cosa vuoi fare?	Azione
Chiedere a Unified Manager di risolvere il problema.	Fare clic sul pulsante **Correggi**.
Non risolvere il problema in questo momento e nascondere questa azione di gestione fino a quando l'evento non viene generato di nuovo.	Fare clic sulla freccia verso il basso e fare clic su **Elimina**.

Cosa vuoi fare?	Azione
Visualizza i dettagli dell'evento per comprendere meglio il problema.	• Fare clic sul pulsante **Correggi** e rivedere la correzione che verrà applicata nella finestra di dialogo risultante. • Fare clic sulla freccia verso il basso e fare clic su **View Event Detail** (Visualizza dettagli evento) per visualizzare la pagina Event Details (Dettagli evento). Quindi, fare clic su **Correggi** da una di queste pagine se si desidera risolvere il problema.
Visualizzare i dettagli di questo oggetto di storage in modo da comprendere meglio il problema.	Fare clic sul nome dell'oggetto di storage per visualizzare i dettagli nella pagina Performance Explorer (Esplora prestazioni) o Health Details (Dettagli integrità).

In alcuni casi, la correzione viene riflessa nel successivo polling di configurazione di 15 minuti. In altri casi, la verifica della modifica della configurazione e l'obsoleto dell'evento possono richiedere fino a molte ore.

Per visualizzare l'elenco delle azioni di gestione completate o in corso, fare clic sull'icona del filtro e selezionare **completato** o **in corso**.

Correggere tutte le operazioni eseguite in modo seriale, in modo che quando si visualizza il pannello **in corso** alcuni oggetti avranno lo stato **in corso**, mentre altri avranno lo stato **pianificato**, il che significa che sono ancora in attesa di essere implementati.

Visualizzazione dello stato delle azioni di gestione che si è scelto di correggere

È possibile visualizzare lo stato di tutte le azioni di gestione che si è scelto di correggere nella pagina azioni di gestione. La maggior parte delle azioni viene visualizzata come **completata** abbastanza rapidamente dopo che Unified Manager ha inviato il comando ONTAP al cluster. Tuttavia, alcune operazioni, ad esempio lo spostamento di un volume, possono richiedere più tempo.

Nella pagina delle azioni di gestione sono disponibili tre filtri:

- **Completed** mostra sia le azioni di gestione completate correttamente che quelle non riuscite. Le azioni **Failed** forniscono un motivo per l'errore, in modo da poter risolvere il problema manualmente.
- **In Progress** mostra sia le azioni di gestione in corso di implementazione che quelle pianificate per l'implementazione.
- **Recommended** mostra tutte le azioni di gestione attualmente attive per tutti i cluster monitorati.

Fasi

1. Fare clic su **azioni di gestione** nel riquadro di navigazione a sinistra. In alternativa, fare clic su Nella parte superiore del pannello **azioni di gestione** del pannello **Dashboard** e selezionare la vista che si desidera visualizzare.

   Viene visualizzata la pagina Management Actions (azioni di gestione).

2. Puoi fare clic sull'icona caret accanto all'azione di gestione nel campo **Descrizione** per visualizzare i dettagli sul problema e sul comando utilizzato per risolvere il problema.
3. Per visualizzare le azioni **non riuscite**, ordinare la colonna **Status** nella vista **Completed**. È possibile utilizzare lo strumento **Filter** per lo stesso scopo.
4. Se si desidera visualizzare ulteriori informazioni su un'azione di gestione non riuscita o se si decide di correggere un'azione di gestione consigliata, è possibile fare clic su **View Event Detail** (Visualizza dettagli evento) nell'area espansa dopo aver fatto clic sull'icona caret accanto all'azione di gestione. Da questa pagina è disponibile un pulsante **Correggi**.

Quali problemi possono risolvere Unified Manager

Utilizzando la funzionalità di correzione automatica di Active IQ Unified Manager, è possibile scegliere di risolvere alcuni problemi di ONTAP o gestire alcune funzionalità di ONTAP, come il monitoraggio anti-ransomware, in modo efficace attraverso Unified Manager.

Questa tabella descrive i problemi o le funzionalità di ONTAP che è possibile gestire direttamente tramite il pulsante **Correggi** o **Correggi tutto** dell'interfaccia utente Web di Unified Manager.

Nome e descrizione dell'evento	Azione di gestione	Operazione di "fix it"
Spazio del volume pieno Il volume è quasi esaurito e ha superato la soglia di capacità massima. Questa soglia viene impostata per impostazione predefinita sul 90% delle dimensioni del volume.	Attiva la crescita automatica del volume	Unified Manager determina che la crescita automatica del volume non è configurata per questo volume, pertanto abilita questa funzione in modo che il volume cresca in capacità quando necessario.
Inode pieno Questo volume ha esaurito gli inode e non può accettare nuovi file.	Aumentare il numero di inode sul volume	Aumenta il numero di inode sul volume del 2%.
Rilevata discrepanza nella policy del livello di storage Il volume contiene molti dati inattivi e il criterio di tiering corrente è impostato su "solo snapshot" o "nessuno".	Abilita il tiering automatico del cloud	Poiché il volume risiede già su un FabricPool, il criterio di tiering viene modificato in "automatico" in modo che i dati inattivi vengano spostati nel livello cloud a costo inferiore.
Rilevata mancata corrispondenza livello di storage Il volume contiene molti dati inattivi, ma non si trova su un livello di storage abilitato al cloud (FabricPool).	Modificare il Tier di storage dei volumi	Sposta il volume sul Tier di storage abilitato al cloud e imposta il criterio di tiering su "auto" per spostare i dati inattivi nel Tier cloud.

Nome e descrizione dell'evento	Azione di gestione	Operazione di "fix it"
Log di audit disattivato Il registro di controllo non è abilitato per la VM di storage	Abilitare la registrazione dell'audit per la VM di storage	Attiva la registrazione dell'audit sulla VM di storage. Tenere presente che la VM di storage deve già avere una posizione del registro di controllo locale o remoto configurata.
Banner di accesso disattivato Il banner di accesso per il cluster deve essere abilitato per aumentare la sicurezza rendendo chiare le restrizioni di accesso.	Impostare il banner di accesso per il cluster	Imposta il banner di accesso del cluster su "accesso limitato agli utenti autorizzati".
Banner di accesso disattivato Il banner di accesso per la VM di storage deve essere abilitato per aumentare la sicurezza rendendo chiare le restrizioni di accesso.	Impostare il banner di accesso per la VM di storage	Imposta il banner di accesso alle macchine virtuali dello storage su "accesso limitato agli utenti autorizzati".
SSH utilizza crittografia non sicura Le cifre con il suffisso "-cbc" sono considerate non sicure.	Rimuovere le crittografia non sicure dal cluster	Rimuove dal cluster le crittografia non sicure, ad esempio aes192-cbc e aes128-cbc.
SSH utilizza crittografia non sicura Le cifre con il suffisso "-cbc" sono considerate non sicure.	Rimuovere le crittografia non sicure dalla VM di storage	Rimuove le crittografia non sicure, ad esempio aes192-cbc e aes128-cbc, dalla VM di storage.
Trasporto HTTPS AutoSupport disattivato Il protocollo di trasporto utilizzato per inviare messaggi AutoSupport al supporto tecnico deve essere crittografato.	Impostare HTTPS come protocollo di trasporto per i messaggi AutoSupport	Imposta HTTPS come protocollo di trasporto per i messaggi AutoSupport sul cluster.
Soglia di squilibrio del carico del cluster violata Indica che il carico non è bilanciato tra i nodi nel cluster. Questo evento viene generato quando la varianza della capacità di performance utilizzata è superiore al 30% tra i nodi.	Bilanciamento dei carichi di lavoro del cluster	Unified Manager identifica il volume migliore da spostare da un nodo all'altro per ridurre lo squilibrio, quindi sposta il volume.

Nome e descrizione dell'evento	Azione di gestione	Operazione di "fix it"
Soglia di squilibrio della capacità del cluster violata Indica che la capacità non è bilanciata tra gli aggregati del cluster. Questo evento viene generato quando la varianza della capacità utilizzata è superiore al 70% tra gli aggregati.	Bilanciare la capacità del cluster	Unified Manager identifica il volume migliore da spostare da un aggregato all'altro per ridurre lo squilibrio, quindi sposta il volume.
Performance Capacity used Threshold violato Indica che il carico sul nodo potrebbe essere utilizzato in eccesso se non si riduce l'utilizzo di uno o più carichi di lavoro altamente attivi. Questo evento viene generato quando il valore della capacità utilizzata per le performance del nodo supera il 100% per più di 12 ore.	Limitare il carico elevato sul nodo	Unified Manager identifica il volume con IOPS più elevati e applica una policy di QoS utilizzando i livelli IOPS storici previsti e di picco per ridurre il carico sul nodo.
Soglia di avviso evento dinamico violata Indica che il nodo sta già operando in uno stato di overload a causa del carico eccessivamente elevato di alcuni carichi di lavoro.	Ridurre il sovraccarico nel nodo	Unified Manager identifica il volume con IOPS più elevati e applica una policy di QoS utilizzando i livelli IOPS storici previsti e di picco per ridurre il carico sul nodo.
Non è possibile effettuare il takeover Il failover è attualmente disattivato, pertanto l'accesso alle risorse del nodo durante un'interruzione o un riavvio andrebbe perso fino a quando il nodo non diventa nuovamente disponibile.	Abilitare il failover del nodo	Unified Manager invia il comando appropriato per abilitare il failover su tutti i nodi del cluster.
L'opzione cf.takeover.on_panic è configurata su OFF L'opzione nodeshell "cf.takeover.on_panic" è impostata su **off**, che potrebbe causare un problema sui sistemi configurati con ha.	Abilitare il Takeover in caso di panico	Unified Manager invia il comando appropriato al cluster per modificare questa impostazione su **on**.

Nome e descrizione dell'evento	Azione di gestione	Operazione di "fix it"
Disattiva l'opzione nodeshell snapmirror.enable La vecchia opzione "snapmirror.enable" è impostata su **on**, che potrebbe causare un problema durante l'avvio dopo l'aggiornamento a ONTAP 9.3 o superiore.	Impostare l'opzione snapmirror.enable su Off	Unified Manager invia il comando appropriato al cluster per modificare questa impostazione su **Off**.
Telnet attivato Indica un potenziale problema di sicurezza perché Telnet non è sicuro e passa i dati in modo non crittografato.	Disattiva Telnet	Unified Manager invia il comando appropriato al cluster per disattivare Telnet.
Configurare l'apprendimento anti-ransomware delle macchine virtuali di storage Verifica periodicamente la presenza di cluster con licenze per il monitoraggio anti-ransomware. Convalida se una VM di storage supporta solo volumi NFS o SMB in un cluster di questo tipo.	Inserire le VM di storage in un `learning` modalità di monitoraggio anti-ransomware	Unified Manager imposta il monitoraggio anti-ransomware su `learning` per le VM di storage attraverso la console di gestione del cluster. Il monitoraggio anti-ransomware su tutti i nuovi volumi creati sulla VM di storage viene automaticamente spostato in una modalità di apprendimento. Grazie a questa abilitazione, ONTAP può apprendere il modello di attività sui volumi e rilevare le anomalie dovute a potenziali attacchi dannosi.
Configurare l'apprendimento anti-ransomware del volume Verifica periodicamente la presenza di cluster con licenze per il monitoraggio anti-ransomware. Convalida se un volume supporta solo servizi NFS o SMB in un cluster di questo tipo.	Inserire i volumi `learning` modalità di monitoraggio anti-ransomware	Unified Manager imposta il monitoraggio anti-ransomware su `learning` stato dei volumi tramite la console di gestione del cluster. Grazie a questa abilitazione, ONTAP può apprendere il modello di attività sui volumi e rilevare le anomalie dovute a potenziali attacchi dannosi.

Nome e descrizione dell'evento	Azione di gestione	Operazione di "fix it"
Abilitare l'anti-ransomware del volume Verifica periodicamente la presenza di cluster con licenze per il monitoraggio anti-ransomware. Rileva se i volumi si trovano in `learning` modalità di monitoraggio anti-ransomware per più di 45 giorni e determina il potenziale cliente di metterli in modalità attiva.	Inserire i volumi `active` modalità di monitoraggio anti-ransomware	Unified Manager imposta il monitoraggio anti-ransomware su `active` sui volumi attraverso la console di gestione del cluster. Grazie a questa abilitazione, ONTAP può apprendere il modello di attività sui volumi e rilevare le anomalie dovute a potenziali attacchi dannosi e creare avvisi per le azioni di protezione dei dati.
Disattiva l'anti-ransomware del volume Verifica periodicamente la presenza di cluster con licenze per il monitoraggio anti-ransomware. Rileva notifiche ripetitive durante il monitoraggio anti-ransomware attivo sui volumi (ad esempio, vengono restituiti più avvisi di potenziali attacchi ransomware nell'arco di 30 giorni).	Disattiva il monitoraggio anti-ransomware sui volumi	Unified Manager disattiva il monitoraggio anti-ransomware sui volumi attraverso la console di gestione del cluster.

Eseguire l'override delle azioni di gestione tramite script

È possibile creare script personalizzati e associarli agli avvisi per eseguire azioni specifiche per eventi specifici, senza optare per le azioni di gestione predefinite disponibili nella pagina delle azioni di gestione o nella dashboard di Unified Manager.

Se si desidera eseguire azioni specifiche per un tipo di evento e scegliere di non correggerle come parte della funzionalità di azione di gestione fornita da Unified Manager, è possibile configurare uno script personalizzato per l'azione specifica. È quindi possibile associare lo script a un avviso per quel tipo di evento e occuparsi di tali eventi singolarmente. In questo caso, le azioni di gestione non vengono generate per quel tipo di evento specifico nella pagina delle azioni di gestione o nella dashboard di Unified Manager.

Gestione dei cluster

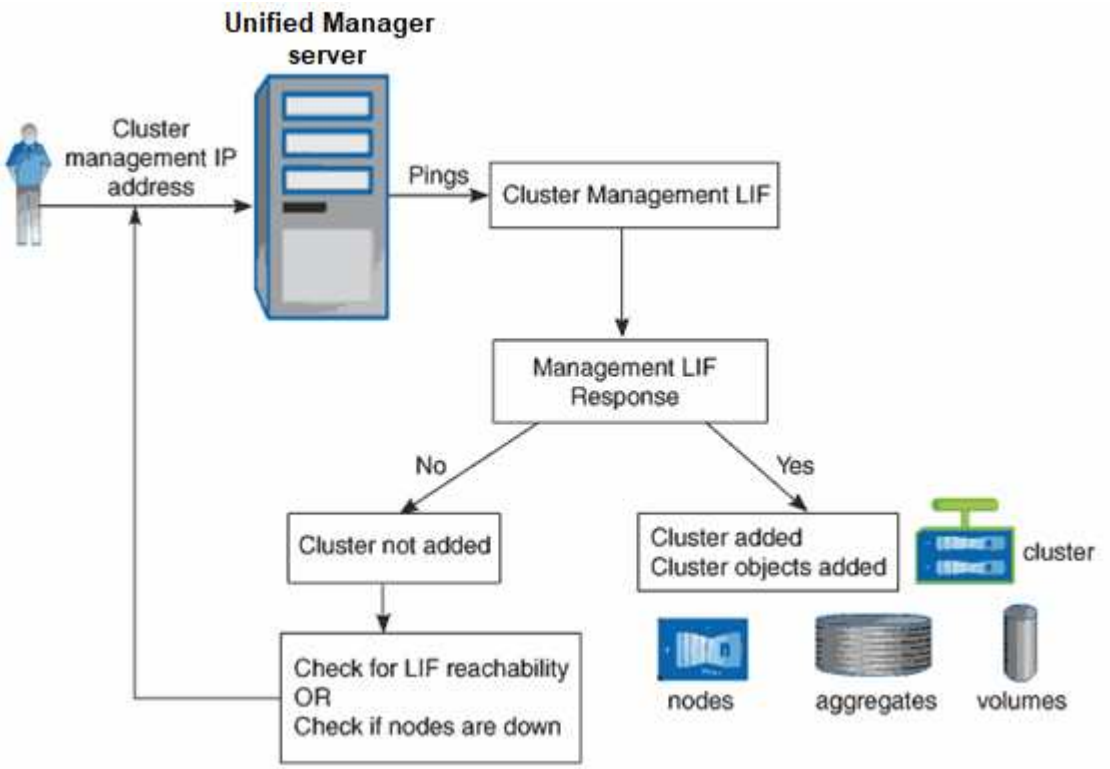
È possibile gestire i cluster ONTAP utilizzando Unified Manager per monitorare, aggiungere, modificare e rimuovere i cluster.

Come funziona il processo di rilevamento del cluster

Dopo aver aggiunto un cluster a Unified Manager, il server rileva gli oggetti del cluster e li aggiunge al database. La comprensione del funzionamento del processo di rilevamento consente di gestire i cluster dell'organizzazione e i relativi oggetti.

L'intervallo di monitoraggio per la raccolta delle informazioni di configurazione del cluster è di 15 minuti. Ad esempio, dopo aver aggiunto un cluster, sono necessari 15 minuti per visualizzare gli oggetti del cluster nell'interfaccia utente di Unified Manager. Questo intervallo di tempo è valido anche quando si apportano modifiche a un cluster. Ad esempio, se si aggiungono due nuovi volumi a una SVM in un cluster, i nuovi oggetti vengono visualizzati nell'interfaccia utente dopo il successivo intervallo di polling, che potrebbe arrivare fino a 15 minuti.

La seguente immagine illustra il processo di rilevamento:



Una volta individuati tutti gli oggetti di un nuovo cluster, Unified Manager inizia a raccogliere dati storici sulle performance per i 15 giorni precedenti. Queste statistiche vengono raccolte utilizzando la funzionalità di raccolta della continuità dei dati. Questa funzionalità fornisce oltre due settimane di informazioni sulle performance per un cluster subito dopo l'aggiunta. Una volta completato il ciclo di raccolta della continuità dei dati, i dati delle performance del cluster in tempo reale vengono raccolti, per impostazione predefinita, ogni cinque minuti.

Dato che la raccolta di 15 giorni di dati sulle performance richiede un uso intensivo della CPU, si consiglia di eseguire l'aggiunta di nuovi cluster in modo che i sondaggi per la raccolta della continuità dei dati non vengano eseguiti su troppi cluster contemporaneamente.

Visualizzazione dell'elenco dei cluster monitorati

È possibile utilizzare la pagina Cluster Setup per visualizzare l'inventario dei cluster. È possibile visualizzare i dettagli dei cluster, ad esempio il nome o l'indirizzo IP e lo stato della comunicazione.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Fase

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Cluster Setup**. + vengono visualizzati tutti i cluster dell'ambiente di storage gestito da Unified Manager. L'elenco dei cluster viene ordinato in base alla colonna del livello di severità dello stato di raccolta. È possibile fare clic sull'intestazione di una colonna per ordinare i cluster in base a colonne diverse.

Aggiunta di cluster

È possibile aggiungere un cluster a Active IQ Unified Manager in modo da poter monitorare il cluster. Ciò include la possibilità di ottenere informazioni sul cluster, come lo stato di salute, la capacità, le performance e la configurazione del cluster, in modo da individuare e risolvere eventuali problemi che potrebbero verificarsi.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario disporre del nome host o dell'indirizzo IP di gestione del cluster (IPv4 o IPv6) per il cluster.

  Quando si utilizza il nome host, deve essere risolto nell'indirizzo IP di gestione del cluster per la LIF di gestione del cluster. Se si utilizza una LIF di gestione dei nodi, l'operazione non riesce.

- Per accedere al cluster, è necessario disporre del nome utente e della password.

  Questo account deve avere il ruolo *admin* con accesso applicazione impostato su *ontapi*, *console* e *http*.

- È necessario conoscere il numero della porta per connettersi al cluster utilizzando il protocollo HTTPS (in genere la porta 443).
- Il cluster deve eseguire il software ONTAP versione 9.1 o superiore.
- È necessario disporre di spazio sufficiente sul server Unified Manager. Non è possibile aggiungere un cluster al server quando oltre il 90% dello spazio è già occupato.
- Si dispone dei certificati richiesti. Unified Manager installa i certificati di sicurezza quando si aggiunge un cluster:

  Certificati server: Questo certificato è di proprietà di Unified Manager. Un certificato SSL (HTTPS) autofirmato predefinito viene generato con una nuova installazione di Unified Manager. NetApp consiglia di eseguire l'upgrade al certificato firmato CA per una maggiore sicurezza. Se il certificato del server scade, è necessario rigenerarlo e riavviare Unified Manager affinché i servizi incorporino il nuovo certificato. Per ulteriori informazioni sulla rigenerazione del certificato SSL, vedere "Generazione di un certificato di protezione HTTPS".

  Certificati per la comunicazione TLS reciproca: Utilizzati durante la comunicazione TLS reciproca tra Unified Manager e ONTAP. L'autenticazione basata su certificato è abilitata per un cluster, in base alla versione di ONTAP. Se il cluster che esegue la versione di ONTAP è inferiore alla 9.5, l'autenticazione basata su certificato non viene attivata.

  L'autenticazione basata su certificato non viene attivata automaticamente per un cluster, se si aggiorna una versione precedente di Unified Manager a Unified Manager 9.12. Tuttavia, è possibile abilitarla modificando e salvando i dettagli del cluster. Se il certificato scade, è necessario rigenerarlo per incorporare il nuovo certificato. Per ulteriori informazioni sulla visualizzazione e la rigenerazione del certificato, vedere "Modifica dei cluster".

- L'autenticazione basata su certificato viene attivata automaticamente se si aggiunge un cluster dall'interfaccia utente Web. Se si aggiunge un cluster dalla console di manutenzione, l'autenticazione basata su certificato non viene attivata.
- Se l'autenticazione basata su certificato è abilitata per un cluster e si esegue il backup di Unified Manager da un server e si esegue il ripristino su un altro server Unified Manager in cui viene modificato il nome host o l'indirizzo IP, il monitoraggio del cluster potrebbe non riuscire. Per evitare il guasto, modificare e salvare i dettagli del cluster. Per ulteriori informazioni sulla modifica dei dettagli del cluster, vedere "Modifica dei cluster".

Certificati client: Utilizzati durante l'autenticazione per i messaggi EMS ricevuti da ONTAP. Questo certificato è di proprietà di ONTAP e viene richiesto quando si aggiunge un cluster ONTAP a Unified Manager. Non è possibile aggiungere un cluster a Unified Manager con un certificato scaduto e, se il certificato client è già scaduto, è necessario rigenerarlo prima di aggiungere il cluster. Tuttavia, se il certificato scade per un cluster già aggiunto e viene utilizzato da Unified Manager, la messaggistica EMS continua a funzionare con il certificato scaduto. Per informazioni sulla generazione dei certificati, consultare l'articolo della Knowledge base (KB) "Come rinnovare un certificato autofirmato ONTAP nell'interfaccia utente di System Manager".

- Una singola istanza di Unified Manager può supportare un numero specifico di nodi. Se è necessario monitorare un ambiente che supera il numero di nodi supportato, è necessario installare un'istanza aggiuntiva di Unified Manager per monitorare alcuni dei cluster. Per visualizzare l'elenco del numero di nodi supportati, vedere "Guida alle Best practice di Unified Manager".

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Cluster Setup**.
2. Nella pagina Cluster Setup, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo Aggiungi cluster, specificare i valori richiesti, quindi fare clic su **Invia**.
4. Nella finestra di dialogo Authorize host (autorizza host), fare clic su **View Certificate** (Visualizza certificato) per visualizzare le informazioni sul certificato del cluster.
5. Fare clic su **Sì**.

   In Unified Manager 9.12, dopo aver salvato i dettagli del cluster, è possibile visualizzare il certificato per la comunicazione TLS reciproca per un cluster.

   Se l'autenticazione basata su certificato non è abilitata, Unified Manager controlla il certificato solo quando il cluster viene aggiunto inizialmente. Unified Manager non controlla il certificato per ogni chiamata API a ONTAP.

Una volta individuati tutti gli oggetti di un nuovo cluster, Unified Manager inizia a raccogliere dati storici sulle performance per i 15 giorni precedenti. Queste statistiche vengono raccolte utilizzando la funzionalità di raccolta della continuità dei dati. Questa funzionalità fornisce oltre due settimane di informazioni sulle performance per un cluster subito dopo l'aggiunta. Una volta completato il ciclo di raccolta della continuità dei dati, i dati delle performance del cluster in tempo reale vengono raccolti, per impostazione predefinita, ogni cinque minuti.

Dato che la raccolta di 15 giorni di dati sulle performance richiede un uso intensivo della CPU, si consiglia di eseguire l'aggiunta di nuovi cluster in modo che i sondaggi per la raccolta della continuità dei dati non vengano eseguiti su troppi cluster contemporaneamente. Inoltre, se si riavvia Unified Manager durante il periodo di raccolta della continuità dei dati, la raccolta viene interrotta e vengono visualizzate lacune nei grafici delle performance per il periodo di tempo mancante.

Se viene visualizzato un messaggio di errore che indica che non è possibile aggiungere il cluster, controllare se si verificano i seguenti problemi:

- Se gli orologi dei due sistemi non sono sincronizzati e la data di inizio del certificato HTTPS di Unified Manager è successiva alla data sul cluster. È necessario assicurarsi che gli orologi siano sincronizzati utilizzando NTP o un servizio simile.
- Se il cluster ha raggiunto il numero massimo di destinazioni di notifica EMS, l'indirizzo di Unified Manager non può essere aggiunto. Per impostazione predefinita, nel cluster è possibile definire solo 20 destinazioni di notifica EMS.

Informazioni correlate

"Aggiunta di utenti"

"Visualizzazione dell'elenco e dei dettagli del cluster"

"Installazione di un certificato HTTPS firmato e restituito dalla CA"

Modifica dei cluster

È possibile modificare le impostazioni di un cluster esistente, ad esempio il nome host o l'indirizzo IP, il nome utente, la password e la porta, utilizzando la finestra di dialogo Edit Cluster (Modifica cluster).

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

A partire da Unified Manager 9.7, i cluster possono essere aggiunti solo utilizzando HTTPS.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Cluster Setup**.
2. Nella pagina **Cluster Setup**, selezionare il cluster che si desidera modificare, quindi fare clic su **Edit** (Modifica).
3. Nella finestra di dialogo **Edit Cluster** (Modifica cluster), modificare i valori secondo necessità. + se sono stati modificati i dettagli di un cluster aggiunto a Unified Manager 9.12, è possibile visualizzare i dettagli del certificato per la comunicazione TLS reciproca, in base alla versione di ONTAP. Per ulteriori informazioni sulla versione di ONTAP, vedere "Certificati per comunicazioni TLS reciproche". + per visualizzare i dettagli del certificato, fare clic su **Dettagli certificato**. Se il certificato è scaduto, fare clic sul pulsante **rigenera** per incorporare il nuovo certificato.
4. Fare clic su **Invia**.
5. Nella finestra di dialogo Authorize host (autorizza host), fare clic su **View Certificate** (Visualizza certificato) per visualizzare le informazioni sul certificato del cluster.
6. Fare clic su **Sì**.

Informazioni correlate

"Aggiunta di utenti"

"Visualizzazione dell'elenco e dei dettagli del cluster"

Rimozione dei cluster

È possibile rimuovere un cluster da Unified Manager utilizzando la pagina Cluster Setup. Ad esempio, è possibile rimuovere un cluster se il rilevamento del cluster non riesce o quando si desidera decommissionare un sistema storage.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Questa attività rimuove il cluster selezionato da Unified Manager. Una volta rimosso, il cluster non viene più monitorato. Anche l'istanza di Unified Manager registrata con il cluster rimosso non viene registrata dal cluster.

La rimozione di un cluster elimina anche tutti gli oggetti di storage, i dati storici, i servizi di storage e tutti gli eventi associati da Unified Manager. Queste modifiche si riflettono sulle pagine di inventario e sui dettagli dopo il successivo ciclo di raccolta dei dati.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Cluster Setup**.
2. Nella pagina Cluster Setup, selezionare il cluster che si desidera rimuovere e fare clic su **Remove** (Rimuovi).
3. Nella finestra di dialogo del messaggio **Remove Data Source** (Rimuovi origine dati), fare clic su **Remove** (Rimuovi) per confermare la richiesta di rimozione.

Informazioni correlate

"Aggiunta di utenti"

"Visualizzazione dell'elenco e dei dettagli del cluster"

Riscoprendo i cluster

È possibile riscoprire manualmente un cluster dalla pagina Cluster Setup per ottenere le informazioni più recenti sullo stato di salute, sullo stato di monitoraggio e sullo stato delle performance del cluster.

È possibile riscoprire manualmente un cluster quando si desidera aggiornare il cluster, ad esempio aumentando le dimensioni di un aggregato quando lo spazio è insufficiente, e si desidera che Unified Manager rilevi le modifiche apportate.

Quando Unified Manager viene associato a OnCommand Workflow Automation (WFA), l'associazione attiva la riacquisizione dei dati memorizzati nella cache da WFA.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Cluster Setup**.
2. Nella pagina **Cluster Setup**, fare clic su **riscopri**.

   Unified Manager rileva nuovamente il cluster selezionato e visualizza lo stato di salute e delle performance più recenti.

Informazioni correlate

"Visualizzazione dell'elenco e dei dettagli del cluster"

Monitoraggio dell'infrastruttura virtuale VMware

Active IQ Unified Manager offre visibilità sulle macchine virtuali (VM) dell'infrastruttura virtuale e consente il monitoraggio e la risoluzione dei problemi relativi a storage e performance nell'ambiente virtuale. È possibile utilizzare questa funzione per determinare eventuali problemi di latenza nell'ambiente di storage o quando si verifica un evento di performance segnalato su vCenter Server.

Una tipica implementazione di un'infrastruttura virtuale su ONTAP include diversi componenti distribuiti tra livelli di calcolo, rete e storage. Eventuali ritardi nelle performance in un'applicazione VM potrebbero verificarsi a causa di una combinazione di latenze affrontate dai vari componenti nei rispettivi layer. Questa funzionalità è utile per gli amministratori di storage e vCenter Server e PER I generalisti IT che devono analizzare un problema di performance in un ambiente virtuale e comprendere in quale componente si è verificato il problema.

È ora possibile accedere a vCenter Server dal menu vCenter della sezione VMware. La vista peek di ciascuna macchina virtuale elencata presenta il collegamento **VCENTER SERVER** nella VISTA DELLA TOPOLOGIA che avvia vCenter Server in un nuovo browser. È inoltre possibile utilizzare il pulsante **Espandi topologia** per avviare vCenter Server e fare clic sul pulsante **Visualizza in vCenter** per visualizzare gli archivi dati in vCenter Server.

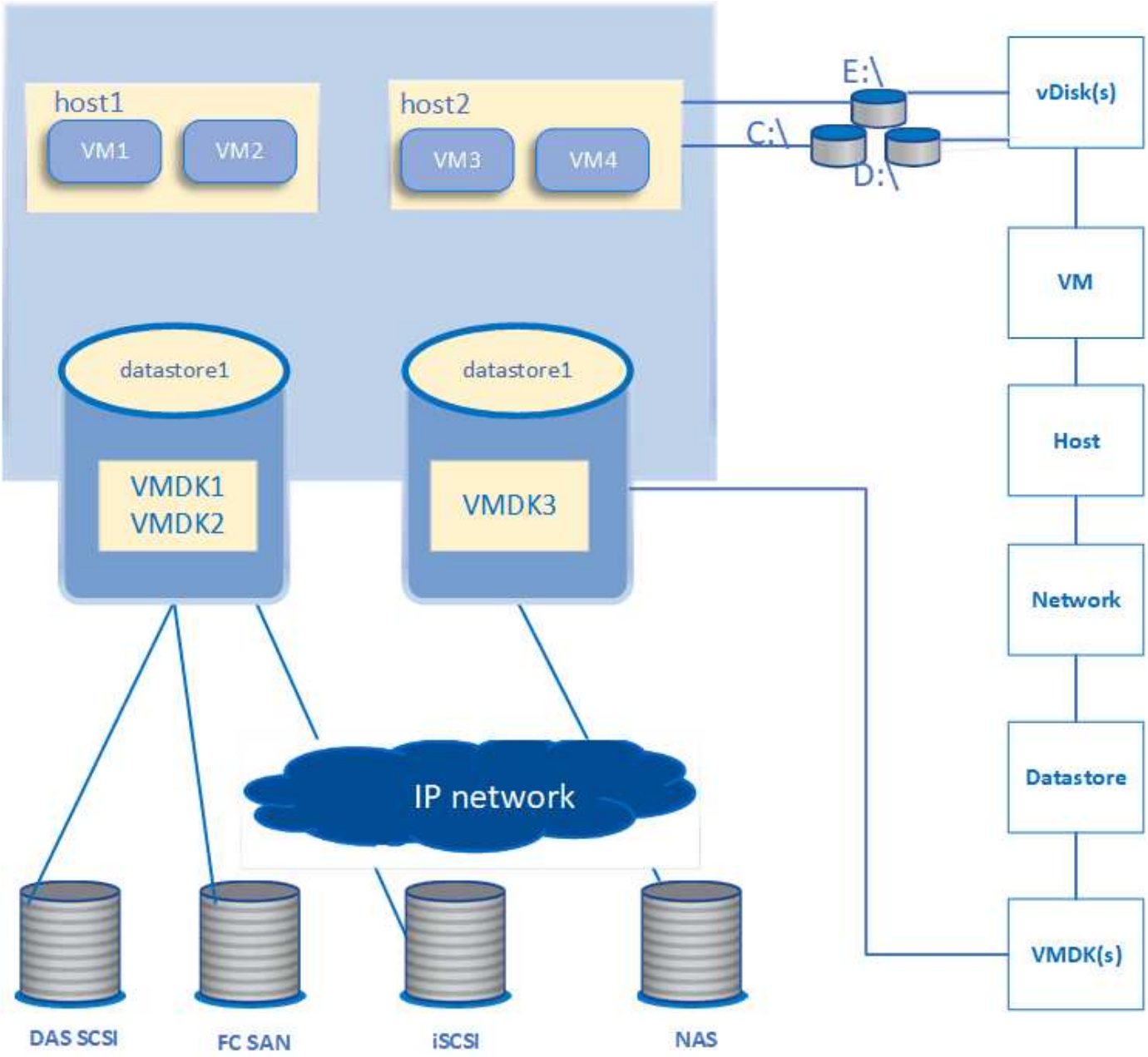
Unified Manager presenta il sottosistema sottostante di un ambiente virtuale in una vista topologica per determinare se si è verificato un problema di latenza nel nodo di calcolo, nella rete o nello storage. La vista evidenzia anche l'oggetto specifico che causa il ritardo delle performance per l'adozione di misure correttive e la risoluzione del problema sottostante.

Un'infrastruttura virtuale implementata sullo storage ONTAP include i seguenti oggetti:

- VCenter Server: Un piano di controllo centralizzato per la gestione delle macchine virtuali VMware, degli host ESXi e di tutti i componenti correlati in un ambiente virtuale. Per ulteriori informazioni su vCenter Server, consultare la documentazione VMware.
- Host: Un sistema fisico o virtuale che esegue ESXi, il software di virtualizzazione di VMware, e ospita la macchina virtuale.
- Datastore: I datastore sono oggetti di storage virtuale connessi agli host ESXi. Gli archivi di dati sono entità di storage gestibili di ONTAP, come LUN o volumi, utilizzate come repository per i file delle macchine virtuali, come file di log, script, file di configurazione e dischi virtuali. Sono connessi agli host dell'ambiente tramite UNA connessione DI rete SAN o IP. Gli archivi dati esterni a ONTAP mappati a vCenter Server non sono supportati o visualizzati in Unified Manager.
- VM: Una macchina virtuale VMware.
- Dischi virtuali: I dischi virtuali negli archivi dati appartenenti alle macchine virtuali che hanno un'estensione come VMDK. I dati provenienti da un disco virtuale vengono memorizzati sul VMDK corrispondente.
- VMDK: Disco di una macchina virtuale nel datastore che fornisce spazio di storage per i dischi virtuali. Per ciascun disco virtuale, è disponibile un VMDK corrispondente.

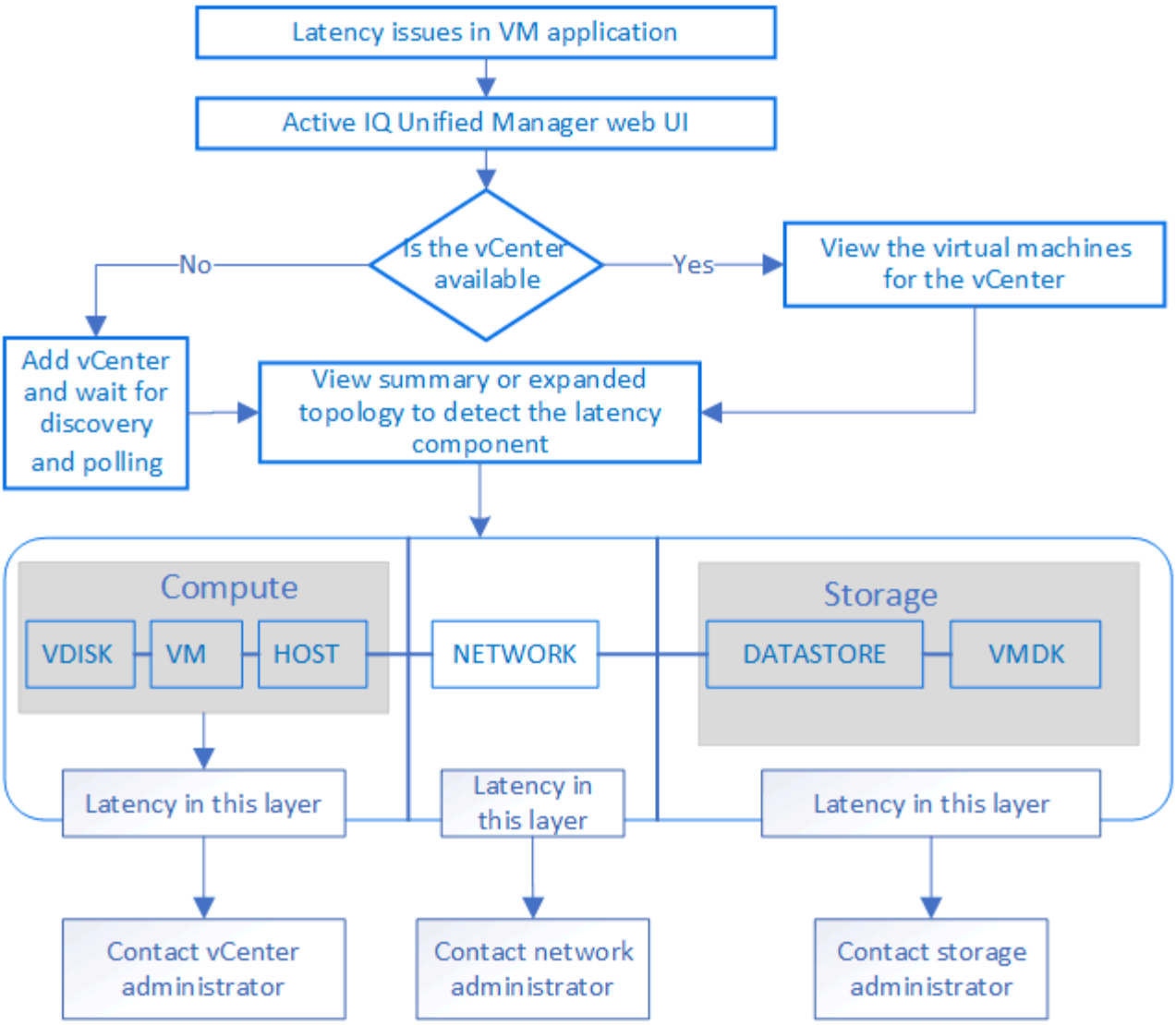
Questi oggetti sono rappresentati in una vista della topologia della macchina virtuale.

Virtualizzazione VMware su ONTAP



Workflow utente

Il seguente diagramma mostra un tipico caso di utilizzo della vista della topologia della macchina virtuale:



Cosa non è supportato

- Gli archivi dati esterni a ONTAP e mappati alle istanze di vCenter Server non sono supportati da Unified Manager. Non sono supportate anche le macchine virtuali con dischi virtuali su tali datastore.
- Un datastore che si estende su più LUN non è supportato.
- Gli archivi di dati che utilizzano NAT (Network Address Translation) per la mappatura dei dati LIF (access endpoint) non sono supportati.
- L'esportazione di volumi o LUN come datastore su cluster diversi con gli stessi indirizzi IP in una configurazione a più LIF non è supportata in quanto Unified Manager non è in grado di identificare quale datastore appartiene a quale cluster.

  Esempio: Supponiamo che il cluster A abbia un datastore A. Il datastore A viene esportato tramite dati LIF con lo stesso indirizzo IP x.x.x.x e viene creata una VM A su questo datastore. Analogamente, il cluster B dispone di datastore B. Il datastore B viene esportato tramite dati LIF con lo stesso indirizzo IP x.x.x.x e VM B viene creato nel datastore B. UM non sarà in grado di mappare il datastore A per la topologia della VM A al volume/LUN ONTAP corrispondente né di mappare la VM B.

- Solo i volumi NAS e SAN (iSCSI e FCP per VMFS) sono supportati come datastore, mentre i volumi virtuali (vVol) non sono supportati.

- Sono supportati solo i dischi virtuali iSCSI. I dischi virtuali di tipo NVMe e SATA non sono supportati.
- Le viste non consentono di generare report per l'analisi delle prestazioni dei vari componenti.
- Per la configurazione del disaster recovery (DR) della macchina virtuale di storage (VM di storage) supportata solo per l'infrastruttura virtuale su Unified Manager, la configurazione deve essere modificata manualmente in vCenter Server per puntare ai LUN attivi negli scenari di switchover e switchback. Senza un intervento manuale, i loro datastore diventano inaccessibili.

Visualizzazione e aggiunta di vCenter Server

Per visualizzare e risolvere i problemi relativi alle prestazioni delle macchine virtuali (VM), è necessario aggiungere i server vCenter associati all'istanza di Active IQ Unified Manager.

Cosa ti serve

Prima di aggiungere o visualizzare i server vCenter, verificare quanto segue:

- Si conoscono i nomi di vCenter Server.
- Si conosce l'indirizzo IP di vCenter Server e si dispone delle credenziali richieste. Le credenziali devono essere di un amministratore di vCenter Server o di un utente root con accesso in sola lettura a vCenter Server.
- Il vCenter Server che si desidera aggiungere esegue vSphere 6.5 o versione successiva.
- L'impostazione di raccolta dati in vCenter Server è impostata sul livello di statistiche di `Level 3`, garantendo il livello richiesto di raccolta delle metriche per tutti gli oggetti monitorati. La durata dell'intervallo deve essere di `5 minutes`, e il periodo di salvataggio dovrebbe essere `1 day`.

  Per ulteriori informazioni, consulta la sezione "DATA Collection Levels" della *vSphere Monitoring and Performance Guide* nella documentazione VMware.

- I valori di latenza in vCenter Server sono configurati in millisecondi, e non in microsecondi, per il corretto calcolo dei valori di latenza.
- Durante l'aggiunta del datastore a vCenter Server, è possibile utilizzare sia l'indirizzo IP dell'host che il nome di dominio completo (FQDN). Se si aggiunge FQDN, assicurarsi che il nome di dominio possa essere risolto dal server Unified Manager. Ad esempio, per un'installazione Linux, assicurarsi che il nome di dominio sia aggiunto in `/etc/resolv.conf` file.
- L'ora corrente di vCenter Server è sincronizzata con il fuso orario di vCenter Server.
- VCenter Server è raggiungibile per un rilevamento corretto.
- Quando si aggiunge vCenter Server a Unified Manager, si dispone dell'accesso in lettura a VMware SDK. Questo è necessario per il polling della configurazione.

Per ogni server vCenter aggiunto e rilevato, Unified Manager raccoglie i dati di configurazione, come i dettagli del server vCenter e ESXi, il mapping ONTAP, i dettagli del datastore e il numero di macchine virtuali ospitate. Raccoglie ulteriormente le metriche delle performance dei componenti.

Fasi

1. Accedere a **VMWARE** > **vCenter** e verificare che vCenter Server sia disponibile nell'elenco.

   Se vCenter Server non è disponibile, è necessario aggiungere vCenter Server.

a. Fare clic su **Aggiungi**.
b. Aggiungere l'indirizzo IP corretto per vCenter Server e assicurarsi che la periferica sia raggiungibile.
c. Aggiungere il nome utente e la password dell'amministratore o dell'utente root con accesso in sola lettura a vCenter Server.
d. Aggiungere il numero di porta personalizzato se si utilizza una porta diversa da quella predefinita 443.
e. Fare clic su **Save** (Salva).

   Una volta completato il rilevamento, viene visualizzato un certificato del server da accettare.

Quando si accetta il certificato, vCenter Server viene aggiunto all'elenco dei vCenter Server disponibili. L'aggiunta del dispositivo non comporta la raccolta di dati per le macchine virtuali associate e la raccolta avviene a intervalli pianificati.

2. Se vCenter Server è disponibile nella pagina **vCenters**, controllare lo stato del server passando il mouse sul campo **Status** per visualizzare se le prestazioni del server vCenter sono quelle previste o se sono presenti avvisi o errori.

   L'aggiunta di vCenter Server consente di visualizzare i seguenti stati. Tuttavia, i dati relativi a performance e latenza delle macchine virtuali corrispondenti potrebbero richiedere fino a un'ora dopo l'aggiunta di vCenter Server per essere riflessi con precisione.

   - Verde: "Normale", che indica che vCenter Server è stato rilevato e che le metriche delle performance sono state raccolte correttamente
   - Giallo: "Avviso" (ad esempio, quando il livello delle statistiche per vCenter Server non è stato impostato su 3 o superiore per ottenere statistiche per ciascun oggetto)
   - Arancione: "Error" (indica eventuali errori interni, ad esempio eccezioni, errori nella raccolta dati di configurazione o irraggiungibile di vCenter Server). Fare clic sull'icona di visualizzazione della colonna (**Show/Hide**) per visualizzare il messaggio di stato relativo allo stato di vCenter Server e risolvere il problema.
3. Nel caso in cui vCenter Server non sia raggiungibile o le credenziali siano cambiate, modificare i dettagli di vCenter Server selezionando **vCenter** > **Edit**.
4. Apportare le modifiche necessarie nella pagina **Modifica VMware vCenter Server**.
5. Fare clic su **Save** (Salva).

Inizia la raccolta dati di vCenter Server

VCenter Server raccoglie in tempo reale campioni di dati relativi alle performance di 20 secondi e li presenta fino a 5 minuti di campioni. La pianificazione per la raccolta dei dati sulle performance di Unified Manager si basa sulle impostazioni predefinite di vCenter Server. Unified Manager elabora i campioni di 5 minuti ottenuti da vCenter Server e calcola una media oraria degli IOPS e della latenza per i dischi virtuali, le macchine virtuali e gli host. Per gli archivi di dati, Unified Manager calcola una media oraria degli IOPS e della latenza dai campioni ottenuti da ONTAP. Questi valori sono disponibili all'inizio dell'ora. Le metriche delle performance non sono disponibili immediatamente dopo l'aggiunta di vCenter Server ed è disponibile solo all'inizio dell'ora successiva. Il polling dei dati sulle performance inizia al completamento di un ciclo di raccolta dei dati di configurazione.

Per il polling dei dati di configurazione di vCenter Server, Unified Manager segue la stessa pianificazione utilizzata per la raccolta dei dati di configurazione del cluster. Per informazioni sulla configurazione di vCenter Server e sulla pianificazione della raccolta dei dati sulle performance, vedere "attività di raccolta dei dati sulle performance e sulla configurazione del cluster".

Informazioni correlate

"Attività di raccolta dei dati relativi alla configurazione e alle performance del cluster"

Monitoraggio delle macchine virtuali

In caso di problemi di latenza nelle applicazioni delle macchine virtuali (VM), potrebbe essere necessario monitorare le macchine virtuali per analizzare e risolvere i problemi della causa. Le macchine virtuali sono disponibili quando il server vCenter e i cluster ONTAP che ospitano lo storage delle macchine virtuali vengono aggiunti a Unified Manager.

I dettagli delle macchine virtuali sono disponibili nella pagina **VMWARE** > > **macchine virtuali**. Vengono visualizzate informazioni quali disponibilità, stato, capacità utilizzata e allocata, latenza di rete, IOPS e latenza di VM, datastore e host. Per una macchina virtuale che supporta più datastore, la griglia mostra le metriche del datastore con la latenza peggiore, con un asterisco (*) che indica ulteriori datastore. Facendo clic sull'icona, vengono visualizzate le metriche dell'archivio dati aggiuntivo. Alcune di queste colonne non sono disponibili per l'ordinamento e il filtraggio.

Per visualizzare una macchina virtuale e i relativi dettagli, è necessario completare il rilevamento (polling o raccolta di metriche) del cluster ONTAP. Se il cluster viene rimosso da Unified Manager, la macchina virtuale non è più disponibile, dopo il successivo ciclo di ricerca.

Da questa pagina è inoltre possibile visualizzare la topologia dettagliata di una macchina virtuale, visualizzando i componenti a cui è collegata la macchina virtuale, ad esempio l'host, il disco virtuale e il datastore ad essa collegato. La vista della topologia visualizza i componenti sottostanti nei rispettivi layer specifici, nel seguente ordine: **Virtual Disk** > **VM** > **host** > **Network** > **Datastore** > **VMDK**.

È possibile determinare il percorso di i/o e le latenze a livello di componente da un aspetto topologico e identificare se lo storage è la causa del problema di performance. La vista riepilogativa della topologia visualizza il percorso di i/o ed evidenzia il componente che presenta problemi di IOPS e latenza per decidere le fasi di risoluzione dei problemi. È inoltre possibile avere una vista estesa della topologia che raffigura ciascun componente separatamente insieme alla latenza di tale componente. È possibile selezionare un componente per determinare il percorso di i/o evidenziato attraverso i livelli.

Visualizzazione della topologia di riepilogo

Per determinare i problemi di performance visualizzando le VM in una topologia riepilogativa:

1. Accedere a **VMWARE** > **Virtual Machines**.
2. Cercare la macchina virtuale digitandone il nome nella casella di ricerca. Puoi anche filtrare i risultati della ricerca in base a criteri specifici facendo clic sul pulsante **Filter**. Tuttavia, se non si riesce a trovare la macchina virtuale, assicurarsi che il server vCenter corrispondente sia stato aggiunto e rilevato.

I server vCenter consentono l'utilizzo di caratteri speciali (ad esempio %, &, *, €, n., @, !, /, :, *, ?, "`, <, >, |, ;, ') nei nomi delle entità vSphere, ad esempio VM, cluster, datastore, cartella, o file. VMware vCenter Server e ESX/ESXi Server non escapano i caratteri speciali utilizzati nei nomi visualizzati. Tuttavia, quando il nome viene elaborato in Unified Manager, viene visualizzato in modo diverso. Ad esempio, una macchina virtuale denominata con il nome `%$VC_AIQUM_clone_191124%` In vCenter Server viene visualizzato come `%25$VC_AIQUM_clone_191124%25` In Unified Manager. È necessario tenere nota di questo problema quando si esegue una query su una macchina virtuale con un nome contenente caratteri speciali.

3. Controllare lo stato della macchina virtuale. Gli stati delle macchine virtuali vengono recuperati da vCenter Server. Sono disponibili i seguenti stati. Per ulteriori informazioni su questi stati, consultare la documentazione VMware.
   - Normale
   - Attenzione
   - Avviso
   - Non monitorato
   - Sconosciuto
4. Fare clic sulla freccia verso il basso accanto alla macchina virtuale per visualizzare la vista riepilogativa della topologia dei componenti nei livelli di calcolo, rete e storage. Viene evidenziato il nodo che presenta problemi di latenza. La vista di riepilogo mostra la latenza peggiore dei componenti. Ad esempio, se una macchina virtuale ha più di un disco virtuale, questa vista mostra il disco virtuale che ha la latenza peggiore tra tutti i dischi virtuali.
5. Per analizzare la latenza e il throughput del datastore in un determinato periodo di tempo, fare clic sul pulsante **workload Analyzer** nella parte superiore dell'icona dell'oggetto datastore. Si accede alla pagina workload Analysis (analisi del carico di lavoro), in cui è possibile selezionare un intervallo di tempo e visualizzare i grafici delle performance del datastore. Per ulteriori informazioni sull'analizzatore del carico di lavoro, consulta la sezione *risoluzione dei problemi relativi ai carichi di lavoro mediante l'analizzatore del carico di lavoro*.

Visualizzazione della topologia estesa

È possibile eseguire il drill-down di ciascun componente separatamente visualizzando la topologia estesa della macchina virtuale.

Fasi

1. Dalla vista di riepilogo della topologia, fare clic su **Espandi topologia**. È possibile visualizzare la topologia dettagliata di ciascun componente separatamente con i numeri di latenza per ciascun oggetto. Se in una categoria sono presenti più nodi, ad esempio più nodi nel datastore o VMDK, il nodo con latenza peggiore viene evidenziato in rosso.
2. Per controllare il percorso io di un oggetto specifico, fare clic su tale oggetto per visualizzare il percorso io e la mappatura corrispondente. Ad esempio, per visualizzare la mappatura di un disco virtuale, fare clic sul disco virtuale per visualizzarne la mappatura evidenziata sul relativo VMDK. In caso di ritardo delle prestazioni di questi componenti, è possibile raccogliere più dati da ONTAP e risolvere il problema.

Le metriche non vengono riportate per i VMDK. Nella topologia, vengono visualizzati solo i nomi VMDK e non le metriche.

Informazioni correlate

"Risoluzione dei problemi relativi ai carichi di lavoro con workload Analyzer"

Visualizzazione dell'infrastruttura virtuale in una configurazione di disaster recovery

È possibile visualizzare la configurazione e le metriche delle performance degli archivi dati ospitati in una configurazione MetroCluster o in una configurazione di disaster recovery (DR SVM) di una macchina virtuale di storage (VM di storage).

In Unified Manager, è possibile visualizzare i volumi NAS o le LUN in una configurazione MetroCluster che sono collegate come datastore in vCenter Server. Gli archivi dati ospitati in una configurazione MetroCluster sono rappresentati nella stessa vista topologica di un datastore in un ambiente standard.

È inoltre possibile visualizzare i volumi NAS o i LUN in una configurazione di disaster recovery delle macchine virtuali dello storage mappata agli archivi dati in vCenter Server.

Visualizzazione degli archivi dati nella configurazione MetroCluster

Prima di visualizzare gli archivi dati in una configurazione MetroCluster, tenere presente i seguenti prerequisiti:

- In caso di switchover e switchback, il rilevamento dei cluster primari e secondari della coppia ha e dei server vCenter deve essere completato.
- I cluster primari e secondari della coppia ha e i server vCenter devono essere gestiti da Unified Manager.
- La configurazione richiesta deve essere completata su ONTAP e vCenter Server. Per informazioni, consultare la documentazione di ONTAP e vCenter.

  "Centro documentazione di ONTAP 9"

Per visualizzare i datastore, attenersi alla seguente procedura:

1. Nella pagina **VMWARE** > **Virtual Machines**, fare clic sulla VM che ospita il datastore. Fare clic sul collegamento **workload Analyzer** o sull'oggetto datastore. Nello scenario standard in cui il sito primario che ospita il volume o il LUN funziona come previsto, è possibile visualizzare i dettagli del cluster VServer del sito primario.
2. In caso di disastro e di switchover consecutivo al sito secondario, il collegamento del datastore punta alle metriche di performance del volume o del LUN nel cluster secondario. Ciò si riflette dopo il successivo ciclo di cluster e il completamento del rilevamento (acquisizione) di VServer.
3. Dopo un switchback riuscito, il collegamento del datastore riflette nuovamente le metriche delle performance del volume o del LUN nel cluster primario. Ciò si riflette al termine del ciclo successivo di rilevamento dei cluster e di VServer.

Visualizzazione dei datastore nella configurazione del disaster recovery delle macchine virtuali di storage

Prima di visualizzare gli archivi dati in una configurazione di disaster recovery per le macchine virtuali di storage, tenere presente i seguenti prerequisiti:

- In caso di switchover e switchback, il rilevamento dei cluster primari e secondari della coppia ha e dei server vCenter deve essere completato.
- Unified Manager deve gestire sia il cluster di origine che quello di destinazione e le macchine virtuali di storage.

- La configurazione richiesta deve essere completata su ONTAP e vCenter Server.
  - Per gli archivi dati NAS (NFS e VMFS), in caso di disastro, i passaggi includono l'attivazione della VM di storage secondaria, la verifica dei percorsi e delle LIF dei dati, la creazione di connessioni perse su vCenter Server e l'avvio delle VM.

    Per uno switchback al sito primario, i dati tra i volumi devono essere sincronizzati prima che il sito primario inizi a servire i dati.
  - Per gli archivi di dati SAN (iSCSI e FC per VMFS), vCenter Server formatta il LUN montato in un formato VMFS. In caso di disastro, i passaggi includono l'avvio della macchina virtuale dello storage secondario, la verifica dei percorsi e delle LIF dei dati. Se gli IP di destinazione iSCSI sono diversi dai LIF primari, è necessario aggiungerli manualmente. I nuovi LUN devono essere disponibili come dispositivi sotto l'adattatore iSCSI dell'adattatore storage dell'host. In seguito, è necessario creare nuovi datastore VMFS con le nuove LUN e registrare le vecchie macchine virtuali con nuovi nomi. Le VM devono essere attive e in esecuzione.

    In caso di ripristino, i dati tra i volumi devono essere sincronizzati. È necessario creare nuovamente nuovi datastore VMFS utilizzando le LUN e le vecchie macchine virtuali registrate con nuovi nomi.

    Per informazioni sull'installazione, consultare la documentazione di ONTAP e vCenter Server.

  "Centro documentazione di ONTAP 9"

Per visualizzare i datastore, attenersi alla seguente procedura:

1. Nella pagina **VMWARE** > **macchine virtuali**, fare clic sull'inventario delle macchine virtuali che ospita il datastore. Fare clic sul collegamento oggetto datastore. Nello scenario standard, è possibile visualizzare i dati delle performance dei volumi e delle LUN nella VM dello storage primario.
2. In caso di disastro e di switchover consecutivo alla VM dello storage secondario, il link del datastore punta alle metriche di performance del volume o del LUN nella VM dello storage secondario. Ciò si riflette dopo il successivo ciclo di cluster e il completamento del rilevamento (acquisizione) di VServer.
3. Dopo un switchback riuscito, il collegamento del datastore riflette nuovamente le metriche delle performance del volume o del LUN nella VM dello storage primario. Ciò si riflette al termine del ciclo successivo di rilevamento dei cluster e di VServer.

Scenari non supportati

- Per una configurazione MetroCluster, tenere presente le seguenti limitazioni:
  - Cluster solo in `NORMAL` e. `SWITCHOVER` gli stati vengono presi in considerazione. Altri stati, ad esempio `PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK`, e. `NOT_REACHABLE` non sono supportati.
  - A meno che non sia attivato lo switch over automatico (ASO), se il cluster primario non funziona, il cluster secondario non può essere rilevato e la topologia continua a puntare al volume o al LUN nel cluster primario.
- Per una configurazione di disaster recovery per le macchine virtuali dello storage, tenere presente i seguenti limiti:
  - Una configurazione con Site Recovery Manager (SRM) o Storage Replication Adapter (SRA) abilitati per un ambiente di storage SAN non è supportata.

Provisioning e gestione dei carichi di lavoro

La funzionalità di gestione attiva di Active IQ Unified Manager offre livelli di servizio delle performance, policy di efficienza dello storage e API dei provider di storage per il provisioning, il monitoraggio e la gestione dei carichi di lavoro dello storage in un data center.

Unified Manager fornisce questa funzionalità per impostazione predefinita. È possibile disattivarla da **Storage Management** > **Feature Settings** se non si intende utilizzare questa funzionalità.

Una volta attivata, è possibile eseguire il provisioning dei carichi di lavoro sui cluster ONTAP gestiti dalla propria istanza di Unified Manager. Puoi anche assegnare policy, come Performance Service Levels e Storage Efficiency Policies sui carichi di lavoro e gestire il tuo ambiente di storage in base a tali policy.

Questa funzione attiva le seguenti funzioni:

- Rilevamento automatico dei carichi di lavoro dello storage sui cluster aggiunti per una facile valutazione e implementazione dei carichi di lavoro dello storage
- Provisioning di carichi di lavoro NAS che supportano i protocolli NFS e CIFS
- Provisioning dei carichi di lavoro SAN che supportano i protocolli iSCSI e FCP
- Supporto per protocolli NFS e CIFS sulla stessa condivisione file
- Gestione dei livelli di servizio delle performance e delle policy di efficienza dello storage
- Assegnazione dei livelli di servizio delle performance e delle policy di efficienza dello storage ai carichi di lavoro dello storage

Le opzioni **Provisioning**, **Storage** > **workload** e **Policies** nel riquadro sinistro dell'interfaccia utente consentono di modificare diverse configurazioni.

È possibile eseguire le seguenti funzioni utilizzando le seguenti opzioni:

- Visualizza i carichi di lavoro dello storage nella pagina **Storage** > **workload**
- Crea workload di storage dalla pagina Provision workload
- Creare e gestire i livelli di Performance Service dalle policy
- Crea e gestisci le policy di efficienza dello storage dalle policy
- Assegnare le policy ai carichi di lavoro dello storage dalla pagina dei carichi di lavoro

Informazioni correlate

"Gestione dello storage basata su policy"

Panoramica sui carichi di lavoro

Un carico di lavoro rappresenta le operazioni di input/output (i/o) di un oggetto storage, ad esempio un volume o un LUN. Il provisioning dello storage si basa sui requisiti di carico di lavoro previsti. Le statistiche dei carichi di lavoro vengono monitorate da Active IQ Unified Manager solo dopo la presenza di traffico da e verso l'oggetto storage. Ad

esempio, i valori di IOPS e latenza del carico di lavoro sono disponibili dopo che gli utenti iniziano a utilizzare un database o un'applicazione e-mail.

La pagina workload visualizza un riepilogo dei carichi di lavoro dello storage dei cluster ONTAP gestiti da Unified Manager. Fornisce informazioni cumulative a colpo d'occhio sui carichi di lavoro dello storage conformi al Performance Service Level e sui carichi di lavoro dello storage non conformi. Consente inoltre di valutare la capacità e le performance (IOPS) totali, disponibili e utilizzate dei cluster nel data center.

Si consiglia di valutare il numero di carichi di lavoro dello storage non conformi, non disponibili o non gestiti da un livello di servizio delle performance e di intraprendere le azioni necessarie per garantirne la conformità, l'utilizzo della capacità e gli IOPS.

La pagina relativa ai carichi di lavoro contiene le seguenti due sezioni:

- Panoramica sui workload: Fornisce una panoramica del numero di workload di storage sui cluster ONTAP gestiti da Unified Manager.
- Panoramica del data center: Fornisce una panoramica della capacità e degli IOPS dei carichi di lavoro dello storage nel data center. I dati rilevanti vengono visualizzati a livello di data center e per i singoli .

Sezione panoramica sui carichi di lavoro

La sezione panoramica sui workload fornisce informazioni cumulative a colpo d'occhio sui workload dello storage. Lo stato dei carichi di lavoro dello storage viene visualizzato in base ai livelli di Performance Service assegnati e non assegnati.

- **Assigned**: Vengono riportati i seguenti stati per i carichi di lavoro dello storage a cui sono stati assegnati i livelli di Performance Service:
  - **Conforme**: Le performance dei carichi di lavoro dello storage si basano sui livelli di Performance Service assegnati. Se i carichi di lavoro dello storage rientrano nella latenza di soglia definita nei livelli di Performance Service associati, vengono contrassegnati come "conformi". I carichi di lavoro conformi sono contrassegnati in blu.
  - **Non conforme**: Durante il monitoraggio delle performance, i carichi di lavoro dello storage sono contrassegnati come "non conforme" se la latenza dei carichi di lavoro dello storage supera la latenza di soglia definita nel livello di servizio delle performance associato. I carichi di lavoro non conformi sono contrassegnati in arancione.
  - **Non disponibile**: I carichi di lavoro dello storage sono contrassegnati come "non disponibile" se non sono in linea o se il cluster corrispondente non è raggiungibile. I carichi di lavoro non disponibili sono contrassegnati in rosso.
- **Non assegnato**: I carichi di lavoro dello storage a cui non è stato assegnato un livello di servizio delle performance vengono riportati come "non assegnato". Il numero viene trasmesso dall'icona delle informazioni.

Il numero totale di workload corrisponde alla somma totale dei workload assegnati e non assegnati.

È possibile fare clic sul numero totale di workload visualizzati in questa sezione e visualizzarli nella pagina workload.

La sottosezione conformità per livelli di servizio delle performance visualizza il numero totale di carichi di lavoro dello storage disponibili:

- Conforme a ciascun tipo di Performance Service Level

- Per i quali esiste una discrepanza tra i livelli di servizio delle prestazioni assegnati e quelli consigliati

Sezione panoramica del data center

La sezione panoramica del data center rappresenta graficamente la capacità disponibile e utilizzata e gli IOPS per tutti i cluster del data center. Utilizzando questi dati, è necessario gestire la capacità e gli IOPS dei carichi di lavoro dello storage. La sezione visualizza inoltre le seguenti informazioni per i carichi di lavoro dello storage in tutti i cluster:

- La capacità totale, disponibile e utilizzata per tutti i cluster del data center
- Gli IOPS totali, disponibili e utilizzati per tutti i cluster del data center
- La capacità disponibile e utilizzata in base a ciascun livello di servizio Performance
- Gli IOPS disponibili e utilizzati in base a ciascun livello di servizio delle performance
- Lo spazio totale e gli IOPS utilizzati dai carichi di lavoro che non hanno un livello di servizio delle performance assegnato

Come vengono calcolate la capacità e le performance del data center in base ai livelli di Performance Service

La capacità e gli IOPS utilizzati vengono recuperati in termini di capacità e performance totali utilizzate di tutti i carichi di lavoro dello storage nei cluster.

Gli IOPS disponibili vengono calcolati in base alla latenza prevista e ai livelli consigliati di Performance Service sui nodi. Include gli IOPS disponibili per tutti i livelli di Performance Service la cui latenza prevista è inferiore o uguale alla latenza prevista.

La capacità disponibile viene calcolata in base alla latenza prevista e ai livelli consigliati di Performance Service sugli aggregati. Include la capacità disponibile per tutti i livelli di Performance Service la cui latenza prevista è inferiore o uguale alla latenza prevista.

Visualizzazione dei carichi di lavoro

Quando si aggiungono cluster a Unified Manager, i carichi di lavoro dello storage su ciascun cluster vengono rilevati e visualizzati automaticamente nella pagina dei carichi di lavoro.

Unified Manager inizia ad analizzare i carichi di lavoro per ottenere consigli (PSL consigliati) solo dopo l'avvio delle operazioni di i/o sui carichi di lavoro dello storage.

Sono esclusi i volumi FlexGroup e i relativi componenti.

Panoramica sui carichi di lavoro

La pagina Panoramica sui workload visualizza una panoramica dei workload nel data center e una panoramica dello spazio e delle performance del data center.

- Pannello **workload Overview**: Visualizza il numero totale di workload e il numero di workload con o senza PSL assegnati. Viene visualizzata anche la srazione del conteggio dei carichi di lavoro per ogni PSL. Facendo clic sui conteggi si passa alla vista **tutti i carichi di lavoro** con i carichi di lavoro filtrati. È inoltre possibile visualizzare il numero di carichi di lavoro non conformi alle raccomandazioni di sistema e assegnarli facendo clic sul pulsante **Assign System-Recommended PSL** (Assegna PSL raccomandati dal sistema).

- Pannello **Data Center Overview** (Panoramica data center): Visualizza lo spazio disponibile e utilizzato (TIB) e le performance (IOPS) del data center. Viene inoltre visualizzata una srazione dello spazio disponibile e utilizzato (TIB) e delle performance (IOPS) di tutti i carichi di lavoro sotto ogni PSL.

Vista tutti i carichi di lavoro

La pagina **Storage > workload > All workload** elenca i workload di storage associati ai cluster ONTAP gestiti da Unified Manager.

Per i carichi di lavoro dello storage appena scoperti in cui non sono state eseguite operazioni di i/o, lo stato è "Waiting for i/o" (in attesa di i/o). Una volta iniziate le operazioni di i/o sui carichi di lavoro dello storage, Unified Manager avvia l'analisi e lo stato del carico di lavoro cambia in "Learning…". Al termine dell'analisi (entro 24 ore dall'inizio delle operazioni di i/o), vengono visualizzati gli PSL consigliati per i carichi di lavoro dello storage.

La pagina consente inoltre di assegnare le policy di efficienza dello storage (SEPS) e i livelli di servizio delle performance (PSL) ai carichi di lavoro dello storage. È possibile eseguire più attività:

- Aggiungere o eseguire il provisioning dei carichi di lavoro dello storage
- Visualizzare e filtrare l'elenco dei workload
- Assegnare gli PSL ai carichi di lavoro dello storage
- Valutare gli PSL raccomandati dal sistema e assegnarli ai carichi di lavoro
- Assegnare SEPS ai carichi di lavoro dello storage

Aggiunta o provisioning dei carichi di lavoro dello storage

È possibile aggiungere o eseguire il provisioning dei carichi di lavoro dello storage a LUN supportati (che supportano protocolli iSCSI e FCP), condivisioni di file NFS e condivisioni SMB.

Fasi

1. Fare clic su **Storage > workload > All workload > Create** (Storage > workload > tutti i workload > Crea).
2. Creare carichi di lavoro. Per ulteriori informazioni, vedere "Provisioning e gestione dei carichi di lavoro".

Visualizzazione e filtraggio dei carichi di lavoro

Nella schermata All workload (tutti i carichi di lavoro), è possibile visualizzare tutti i carichi di lavoro del data center o cercare carichi di lavoro storage specifici in base alle PSL o ai nomi. È possibile utilizzare l'icona del filtro per inserire condizioni specifiche per la ricerca. È possibile eseguire la ricerca in base a diverse condizioni di filtro, ad esempio in base al cluster host o alla VM di storage. L'opzione **Capacity Total** consente di filtrare in base alla capacità totale dei carichi di lavoro (in MB). Tuttavia, in questo caso, il numero di workload restituiti potrebbe variare, in quanto la capacità totale viene confrontata a livello di byte.

Per ogni carico di lavoro, vengono visualizzate informazioni, come il cluster host e la VM di storage, insieme al PSL e AL SEP assegnati.

La pagina consente inoltre di visualizzare i dettagli delle performance di un workload. È possibile visualizzare informazioni dettagliate sugli IOPS, la capacità e la latenza del carico di lavoro facendo clic sul pulsante **Choose / Order Columns** (Scegli / Ordina colonne) e selezionando le colonne specifiche da visualizzare. La colonna Performance View (visualizzazione prestazioni) visualizza gli IOPS medi e massimi per un carico di lavoro, quindi fare clic sull'icona dell'analizzatore del carico di lavoro per visualizzare l'analisi IOPS dettagliata.

Analisi dei criteri di performance e capacità per un carico di lavoro

Il pulsante **Analyze workload** (analizza carico di lavoro) nella finestra a comparsa **IOPS Analysis** (analisi IOPS) consente di accedere alla pagina workload Analysis (analisi del carico di lavoro), in cui è possibile selezionare un intervallo di tempo e visualizzare i trend di latenza, throughput e capacità per il carico di lavoro selezionato. Per ulteriori informazioni sull'analizzatore del carico di lavoro, vedere "Risoluzione dei problemi dei carichi di lavoro utilizzando l'analizzatore dei carichi di lavoro".

È possibile visualizzare le informazioni sulle performance relative a un carico di lavoro per agevolare la risoluzione dei problemi facendo clic sull'icona del grafico a barre nella colonna **visualizzazione delle performance**. Per visualizzare i grafici delle performance e della capacità nella pagina workload Analysis (analisi del carico di lavoro) per analizzare l'oggetto, fare clic sul pulsante **Analyze workload** (analizza carico di lavoro).

Per ulteriori informazioni, vedere "Quali dati vengono visualizzati dall'analizzatore del carico di lavoro".

Assegnazione di policy ai carichi di lavoro

Puoi assegnare le policy di efficienza dello storage (SEPS) e i livelli di servizio delle performance (PSL) ai carichi di lavoro dello storage dalla pagina tutti i carichi di lavoro utilizzando le diverse opzioni di navigazione.

Assegnazione di policy a un singolo carico di lavoro

È possibile assegnare un PSL o UN SET o entrambi a un singolo carico di lavoro. Attenersi alla seguente procedura:

1. Selezionare il carico di lavoro.
2. Fare clic sull'icona di modifica accanto alla riga, quindi fare clic su **Modifica**.

   I campi **Assigned Performance Service Level** e **Storage Efficiency Policy** sono abilitati.

3. Selezionare il PSL o SEP o entrambi.
4. Fare clic sull'icona del segno di spunta per applicare le modifiche.

> È inoltre possibile selezionare un carico di lavoro e fare clic su **altre azioni** per assegnare i criteri.

Assegnazione di policy a più carichi di lavoro dello storage

È possibile assegnare un PSL o UN SET a più carichi di lavoro dello storage insieme. Attenersi alla seguente procedura:

1. Selezionare le caselle di controllo per i carichi di lavoro a cui si desidera assegnare la policy oppure selezionare tutti i carichi di lavoro nel data center.
2. Fare clic su **altre azioni**.
3. Per assegnare un PSL, selezionare **Assegna livello di servizio delle prestazioni**. Per assegnare UN SET, selezionare **Assign Storage Efficiency Policy**. Viene visualizzata una finestra a comparsa per la selezione del criterio.
4. Selezionare la policy appropriata e fare clic su **Apply** (Applica). Viene visualizzato il numero di workload su cui vengono assegnati i criteri. Vengono elencati anche i carichi di lavoro per i quali non vengono assegnati i criteri, con la causa.

L'applicazione di policy sui carichi di lavoro in blocco potrebbe richiedere del tempo a seconda del numero di carichi di lavoro selezionati. È possibile fare clic sul pulsante **Esegui in background** e continuare con altre attività mentre l'operazione viene eseguita in background. Una volta completata l'assegnazione in blocco, è possibile visualizzare lo stato di completamento. Se si applica una PSL su più carichi di lavoro, non è possibile attivare un'altra richiesta quando è in esecuzione il precedente processo di assegnazione in blocco.

Assegnazione di PSL consigliati dal sistema ai carichi di lavoro

È possibile assegnare gli PSL consigliati dal sistema ai carichi di lavoro dello storage in un data center che non hanno PSL assegnati oppure gli PSL assegnati non corrispondono alle raccomandazioni del sistema. Per utilizzare questa funzionalità, fare clic sul pulsante **Assign System Recommended PSL** (Assegna PSL raccomandati dal sistema). Non è necessario selezionare carichi di lavoro specifici.

Il suggerimento è determinato internamente dall'analisi del sistema e viene ignorato per quei carichi di lavoro i cui IOPS e altri parametri non coincidono con le definizioni di qualsiasi PSL disponibile. Carichi di lavoro dello storage con `Waiting for I/O` Sono esclusi anche gli stati e Learning.

Nel nome del carico di lavoro, Unified Manager cerca parole chiave speciali per eseguire l'override delle analisi di sistema e consigliare un PSL diverso per il carico di lavoro. Quando il carico di lavoro ha le lettere "ora" nel nome, si consiglia di utilizzare il profilo **Extreme Performance**PSL. E quando il carico di lavoro ha le lettere "vm" nel nome, si consiglia di utilizzare il profilo **Performance**PSL.

Consultare anche l'articolo della Knowledge base (KB) "ActiveIQ Unified Manager "Assign System Recommended Performance Service Level" non è adattabile a un carico di lavoro altamente variabile"

Provisioning dei volumi di condivisione dei file

È possibile creare volumi di file share che supportano i protocolli CIFS/SMB e NFS su un cluster esistente e su una Storage Virtual Machine (Storage VM) dalla pagina Provision workload (carico di lavoro di provisioning).

Cosa ti serve

- La VM di storage deve disporre di spazio per il provisioning del volume di condivisione file.
- Entrambi i servizi SMB e NFS devono essere attivati sulla vostra macchina virtuale di storage.
- Per selezionare e assegnare il livello di servizio delle performance (PSL) e la policy di efficienza dello storage (SEP) sul carico di lavoro, le policy devono essere state create prima di iniziare a creare il carico di lavoro.

Fasi

1. Nella pagina **carico di lavoro di provisioning**, aggiungere il nome del carico di lavoro che si desidera creare, quindi selezionare il cluster dall'elenco Available (disponibile).
2. In base al cluster selezionato, il campo **STORAGE VM** filtra le VM di storage disponibili per quel cluster. Selezionare dall'elenco la VM di storage richiesta.

   In base ai servizi SMB e NFS supportati dalla VM di storage, l'opzione NAS viene attivata nella sezione host Information (informazioni host).

3. Nella sezione Storage and Optimization (Storage e ottimizzazione), assegnare la capacità di storage e il

PSL e, facoltativamente, un SEP per il carico di lavoro.

Le specifiche di SEP vengono assegnate al LUN e le definizioni per il PSL vengono applicate al carico di lavoro al momento della creazione.

4. Selezionare la casella di controllo **Imponi limiti di performance** se si desidera applicare il PSL assegnato al carico di lavoro.

   L'assegnazione di una PSL a un workload garantisce che l'aggregato su cui viene creato il workload possa supportare gli obiettivi di performance e capacità definiti nelle rispettive policy. Ad esempio, se a un carico di lavoro viene assegnato il livello "PSL per prestazioni estreme", l'aggregato su cui deve essere eseguito il provisioning del carico di lavoro deve essere in grado di supportare gli obiettivi di performance e capacità della policy "Extreme Performance", come lo storage SSD.

   > A meno che non si selezioni questa casella di controllo, il PSL non viene applicato al carico di lavoro e lo stato del carico di lavoro sulla dashboard viene visualizzato come non assegnato.

5. Selezionare l'opzione **NAS**.

   Se non si riesce a visualizzare l'opzione **NAS** attivata, verificare se la VM di storage selezionata supporta SMB, NFS o entrambi.

   > Se la vostra VM di storage è abilitata per servizi SMB e NFS, potete selezionare le caselle di controllo **Share by NFS** e **Share by SMB** e creare una condivisione file che supporti sia i protocolli NFS che SMB. Se si desidera creare una condivisione SMB o CIFS, selezionare solo la rispettiva casella di controllo.

6. Per i volumi di condivisione file NFS, specificare l'indirizzo IP dell'host o della rete per accedere al volume di condivisione file. È possibile immettere valori separati da virgole per più host.

   Quando si aggiunge l'indirizzo IP dell'host, viene eseguita una verifica interna per verificare la corrispondenza dei dettagli dell'host con la VM di storage e la policy di esportazione per tale host, oppure, nel caso in cui esista una policy esistente, questa viene riutilizzata. Se sono state create diverse condivisioni NFS per lo stesso host, viene riutilizzata una policy di esportazione disponibile per lo stesso host con regole corrispondenti per tutte le condivisioni file. La funzione di specificare le regole dei singoli criteri o di riutilizzare i criteri fornendo chiavi di policy specifiche è disponibile quando si effettua il provisioning della condivisione NFS utilizzando le API.

7. Per una condivisione SMB, specificare quali utenti o gruppi di utenti possono accedere alla condivisione SMB e assegnare le autorizzazioni richieste. Per ciascun gruppo di utenti, viene generato un nuovo elenco di controllo degli accessi (ACL) durante la creazione della condivisione file.
8. Fare clic su **Save** (Salva).

   Il carico di lavoro viene aggiunto all'elenco dei carichi di lavoro dello storage.

Provisioning dei LUN

È possibile creare LUN che supportano i protocolli CIFS/SMB e NFS su un cluster e una Storage Virtual Machine (Storage VM) esistenti dalla pagina Provision workload (carico di lavoro provisioning).

Cosa ti serve

- La VM di storage deve disporre di spazio per il provisioning del LUN.
- Sia iSCSI che FCP devono essere attivati sulla VM di storage su cui si crea il LUN.
- Per selezionare e assegnare il livello di servizio delle performance (PSL) e la policy di efficienza dello storage (SEP) sul carico di lavoro, le policy devono essere state create prima di iniziare a creare il carico di lavoro.

Fasi

1. Nella pagina **carico di lavoro di provisioning**, aggiungere il nome del carico di lavoro che si desidera creare, quindi selezionare il cluster dall'elenco Available (disponibile).

   In base al cluster selezionato, il campo **STORAGE VM** filtra le VM di storage disponibili per quel cluster.

2. Selezionare la VM di storage dall'elenco che supporta i servizi iSCSI e FCP.

   In base alla selezione effettuata, l'opzione SAN viene attivata nella sezione host Information (informazioni host).

3. Nella sezione **Storage and Optimization** (Storage e ottimizzazione), assegnare la capacità di storage e il PSL e, facoltativamente, IL SET per il carico di lavoro.

   Le specifiche di SEP vengono assegnate al LUN e le definizioni per il PSL vengono applicate al carico di lavoro al momento della creazione.

4. Selezionare la casella di controllo **Imponi limiti di performance** se si desidera applicare il PSL assegnato al carico di lavoro.

   L'assegnazione di una PSL a un workload garantisce che l'aggregato su cui viene creato il workload possa supportare gli obiettivi di performance e capacità definiti nelle rispettive policy. Ad esempio, se a un carico di lavoro viene assegnato il PSL "Extreme Performance", l'aggregato su cui deve essere eseguito il provisioning del carico di lavoro dovrebbe essere in grado di supportare gli obiettivi di performance e capacità della policy "Extreme Performance", come lo storage SSD.

   > A meno che non si selezioni questa casella di controllo, il PSL non viene applicato al carico di lavoro e lo stato del carico di lavoro sulla dashboard viene visualizzato come `unassigned`.

5. Selezionare l'opzione **SAN**. Se l'opzione **SAN** non è attivata, verificare se la VM di storage selezionata supporta iSCSI e FCP.
6. Selezionare il sistema operativo host.
7. Specificare il mapping dell'host per controllare l'accesso degli iniziatori al LUN. È possibile assegnare gruppi iniziatori esistenti (igroups) oppure definire e mappare nuovi igroups.

   > Se si crea un nuovo igroup durante il provisioning del LUN, è necessario attendere il successivo ciclo di rilevamento (fino a 15 minuti) per utilizzarlo. Si consiglia pertanto di utilizzare un igroup esistente dall'elenco di igroups disponibili.

   Se si desidera creare un nuovo igroup, selezionare il pulsante **Create a new initiator group** (Crea un nuovo gruppo di iniziatori) e immettere le informazioni per l'igroup.

8. Fare clic su **Save** (Salva).

Il LUN viene aggiunto all'elenco dei carichi di lavoro dello storage.

Performance livelli di servizio

Un Performance Service Level (PSL) consente di definire gli obiettivi di performance e storage per un carico di lavoro. È possibile assegnare un PSL a un workload durante la creazione iniziale del workload o successivamente modificando il workload.

La gestione e il monitoraggio delle risorse storage si basano sugli obiettivi del livello di servizio (SLO). Gli SLO sono definiti da contratti di livello di servizio basati sulle prestazioni e sulla capacità richieste. In Unified Manager, gli SLO si riferiscono alle definizioni PSL delle applicazioni in esecuzione sullo storage NetApp. I servizi di storage si differenziano in base alle performance e all'utilizzo delle risorse sottostanti. Un PSL è una descrizione degli obiettivi del servizio di storage. Un PSL consente al provider di storage di specificare gli obiettivi di performance e capacità per il carico di lavoro. Quando si assegna un PSL a un carico di lavoro, il carico di lavoro corrispondente su ONTAP viene gestito in base ai suoi obiettivi di performance e capacità. Ogni PSL è regolato da IOPS minimi massimi, previsti e assoluti e latenza prevista.

Unified Manager dispone dei seguenti tipi di PSL:

- **Definito dal sistema**: Unified Manager fornisce alcune policy predefinite che non possono essere modificate. Questi PSL predefiniti sono:
  - Performance elevate
  - Performance
  - Valore

    Le PSL Extreme Performance, Performance e Value sono applicabili alla maggior parte dei carichi di lavoro storage comuni in un data center.

  Unified Manager offre anche tre livelli di Performance Service per le applicazioni di database. Si tratta di PSL dalle performance estremamente elevate che supportano IOPS bursty e sono adatti per applicazioni di database con la più elevata domanda di throughput.
  - Extreme per i registri del database
  - Extreme per i dati condivisi del database
  - Extreme per i dati del database
- **Definito dall'utente**: Se i livelli di Performance Service predefiniti non soddisfano i requisiti, è possibile creare nuovi PSL per soddisfare le proprie esigenze. Per ulteriori informazioni, vedere "Creazione e modifica dei livelli di Performance Service".
- **Beyond Extreme**: Le PSL Beyond Extreme sono le PSL consigliate dal sistema per i carichi di lavoro che richiedono IOPS superiori a Extreme. I carichi di lavoro vengono analizzati internamente in base ai relativi IOPS, capacità e latenza, mentre per ciascuno di questi carichi di lavoro si consiglia un livello di protezione superiore a quello estremo nella schermata **Storage > workload > All workload** (Storage > carichi di lavoro > tutti i carichi di lavoro). È possibile applicare gli PSL ai carichi di lavoro per garantire performance ottimali.

  I parametri IOPS per i carichi di lavoro vengono generati dinamicamente, a seconda del comportamento del carico di lavoro, e aggiunti al nome del Beyond Extreme PSL nel formato `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`. Ad esempio, se il sistema determina un carico di lavoro in modo da avere gli IOPS di picco e quelli previsti come `106345` e. `37929` Rispettivamente, il valore Beyond Extreme PSL generato per il carico di lavoro viene denominato come

`Beyond Extreme 106345 37929`. Sebbene queste PSL siano raccomandate dal sistema, quando le si assegnano ai carichi di lavoro, queste PSL sono etichettate come `User-defined` nel tipo.

Gestione dei carichi di lavoro mediante l'assegnazione di PSL

È possibile accedere alle PSL dalla pagina **Policy** > **Performance Service Levels** e utilizzando le API del provider di storage. La gestione dei carichi di lavoro dello storage mediante l'assegnazione di PSL è conveniente in quanto non è necessario gestire singolarmente i carichi di lavoro dello storage. Qualsiasi modifica può essere gestita anche riassegnando un altro PSL invece di gestirlo singolarmente. Unified Manager consente di assegnare PSL ai carichi di lavoro in base a valutazioni e raccomandazioni interne.

Per informazioni sull'assegnazione di PSL consigliati dal sistema ai carichi di lavoro, vedere "Assegnazione di PSL consigliati dal sistema ai carichi di lavoro"

La pagina Performance Service Levels elenca i criteri PSL disponibili e consente di aggiungerli, modificarli ed eliminarli.

Non è possibile modificare un PSL definito dal sistema o attualmente assegnato a un carico di lavoro. Non è possibile eliminare un PSL assegnato a un carico di lavoro o se è l'unico PSL disponibile.

In questa pagina vengono visualizzate le seguenti informazioni:

Campo	Descrizione
Nome	Nome del PSL.
Tipo	Se il criterio è definito dal sistema o dall'utente.
IOPS/TB previsti	Numero minimo di IOPS che un'applicazione deve eseguire su una LUN o una condivisione file. Gli IOPS previsti specificano gli IOPS minimi previsti allocati, in base alla dimensione allocata dell'oggetto di storage.

Campo	Descrizione
IOPS/TB di picco	Numero massimo di IOPS che un'applicazione può eseguire su una LUN o una condivisione file. Peak IOPS specifica il massimo IOPS possibile allocato, in base alla dimensione allocata dell'oggetto di storage o alla dimensione utilizzata dell'oggetto di storage. Gli IOPS di picco si basano su una policy di allocazione. La policy di allocazione è lo spazio allocato o lo spazio utilizzato. Quando la policy di allocazione è impostata su allocated-space, gli IOPS di picco vengono calcolati in base alle dimensioni dell'oggetto di storage. Quando la policy di allocazione è impostata su used-space, gli IOPS di picco vengono calcolati in base alla quantità di dati memorizzati nell'oggetto storage, tenendo conto dell'efficienza dello storage. Per impostazione predefinita, il criterio di allocazione è impostato su spazio utilizzato.
IOPS minimi assoluti	L'IOPS minimo assoluto viene utilizzato come override, quando l'IOPS previsto è inferiore a questo valore. I valori predefiniti degli PSL definiti dal sistema sono i seguenti: • Performance estreme: Se IOPS previsti >= 6144/TB, allora IOPS minimi assoluti = 1000 • Performance (prestazioni): Se IOPS previsti >= 2048/TB e < 6144/TB, allora IOPS minimi assoluti = 500 • Valore: Se IOPS previsti >= 128/TB e < 2048/TB, allora IOPS minimi assoluti = 75 I valori predefiniti degli PSL del database definiti dal sistema sono i seguenti: • Extreme per i registri del database: Se IOPS previsti >= 22528, allora IOPS minimi assoluti = 4000 • Extreme per i dati condivisi del database: Se IOPS previsti >= 16384, allora IOPS minimi assoluti = 2000 • Extreme per i dati del database: Se IOPS previsti >= 12288, allora IOPS minimi assoluti = 2000 Il valore più elevato degli IOPS minimi assoluti per gli PSL personalizzati può essere un massimo di 75000. Il valore inferiore viene calcolato come segue: 1000/latenza prevista

Campo	Descrizione
Latenza prevista	Latenza prevista per gli IOPS dello storage in millisecondi per operazione (ms/op).
Capacità	Capacità totale disponibile e utilizzata nei cluster.
Carichi di lavoro	Numero di carichi di lavoro dello storage a cui è stato assegnato il PSL.

Per informazioni su come i picchi di IOPS e gli IOPS previsti aiutano a ottenere performance differenziate coerenti sui cluster ONTAP, consulta il seguente articolo della Knowledge base:https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["Cos'è il budget per le performance?"]

Eventi generati per i carichi di lavoro che violano la soglia definita dagli PSL

Si noti che se i carichi di lavoro superano il valore di latenza previsto per il 30% del tempo durante l'ora precedente, Unified Manager genera uno dei seguenti eventi per notificare un potenziale problema di performance:

- Soglia di latenza del volume del carico di lavoro violata come definito dalla Performance Service Level Policy
- Soglia di latenza LUN del carico di lavoro violata come definito dalla Performance Service Level Policy.

Si consiglia di analizzare il carico di lavoro per vedere cosa potrebbe causare valori di latenza più elevati.

Per ulteriori informazioni, consultare i seguenti collegamenti:

- "Eventi di volume"
- "Cosa accade quando una policy di soglia delle performance viene violata"
- "Come Unified Manager utilizza la latenza dei workload per identificare i problemi di performance"
- "Quali sono gli eventi relativi alle performance"

PSL definiti dal sistema

La seguente tabella fornisce informazioni sugli PSL definiti dal sistema:

Performance Service Level	Descrizione e caso d'utilizzo	Latenza prevista (ms/op)	IOPS di picco	IOPS previsti	IOPS minimi assoluti
Performance elevate	Offre un throughput estremamente elevato a una latenza molto bassa Ideale per applicazioni sensibili alla latenza	1	12288	6144	1000
Performance	Offre un throughput elevato a bassa latenza Ideale per database e applicazioni virtualizzate	2	4096	2048	500
Valore	Offre un'elevata capacità di storage e una latenza moderata Ideale per applicazioni ad alta capacità come e-mail, contenuti Web, condivisioni di file e destinazioni di backup	17	512	128	75

Performance Service Level	Descrizione e caso d'utilizzo	Latenza prevista (ms/op)	IOPS di picco	IOPS previsti	IOPS minimi assoluti
Extreme per i registri del database	Offre il massimo throughput con la latenza più bassa. Ideale per applicazioni di database che supportano i log di database. Questo PSL offre il throughput più elevato perché i log del database sono estremamente bursty e la registrazione è costantemente richiesta.	1	45056	22528	4000
Extreme per i dati condivisi del database	Offre un throughput molto elevato con la latenza più bassa. Ideale per i dati delle applicazioni di database memorizzati in un archivio dati comune, ma condivisi tra database.	1	32768	16384	2000

Performance Service Level	Descrizione e caso d'utilizzo	Latenza prevista (ms/op)	IOPS di picco	IOPS previsti	IOPS minimi assoluti
Extreme per i dati del database	Offre un throughput elevato con la latenza più bassa. Ideale per i dati delle applicazioni di database, come le informazioni sulle tabelle di database e i metadati.	1	24576	12288	2000

Creazione e modifica dei livelli di Performance Service

Quando i livelli di Performance Service definiti dal sistema non corrispondono ai requisiti del carico di lavoro, puoi creare i tuoi livelli di Performance Service ottimizzati per i carichi di lavoro.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione.
- Il nome del livello di servizio Performance deve essere univoco e non è possibile utilizzare le seguenti parole chiave riservate:

  `Prime`, `Extreme`, `Performance`, `Value`, `Unassigned`, `Learning`, `Idle`, `Default`, e. `None`.

È possibile creare e modificare i livelli di Performance Service personalizzati dalla pagina Performance Service Levels definendo gli obiettivi del livello di servizio richiesti per le applicazioni che accederanno allo storage.

Non è possibile modificare un livello di servizio delle prestazioni se è attualmente assegnato a un carico di lavoro.

Fasi

1. Nel riquadro di navigazione a sinistra sotto **Impostazioni**, selezionare **Criteri** > **livelli di servizio delle prestazioni**.
2. Nella pagina **Performance Service Level**, fare clic sul pulsante appropriato a seconda che si desideri creare un nuovo Performance Service Level o modificare un Performance Service Level esistente.

Per…	Attenersi alla procedura descritta di seguito…
Creare un nuovo livello di servizio per le performance	Fare clic su **Aggiungi**.

Per…	Attenersi alla procedura descritta di seguito…
Modificare un livello di servizio delle performance esistente	Selezionare un Performance Service Level esistente, quindi fare clic su **Edit** (Modifica).

Viene visualizzata la pagina per aggiungere o modificare un livello di servizio delle prestazioni.

3. Personalizzare il Performance Service Level specificando gli obiettivi di performance, quindi fare clic su **Submit** per salvare il Performance Service Level.

È possibile applicare il nuovo o modificato livello di servizio delle performance ai carichi di lavoro (LUN, condivisioni file NFS, condivisioni CIFS) dalla pagina dei carichi di lavoro o durante il provisioning di un nuovo carico di lavoro.

Gestione delle policy di efficienza dello storage

Una Storage Efficiency Policy (SEP) consente di definire le caratteristiche di efficienza dello storage di un workload. È possibile assegnare UN SET a un workload durante la creazione iniziale del workload o successivamente modificando il workload.

L'efficienza dello storage include l'utilizzo di tecnologie come thin provisioning, deduplica e compressione dei dati che aumentano l'utilizzo dello storage e riducono i costi dello storage. Durante la creazione di SEPS, è possibile utilizzare queste tecnologie di risparmio dello spazio singolarmente o insieme per ottenere la massima efficienza dello storage. Quando si associano le policy ai carichi di lavoro dello storage, vengono assegnate loro le impostazioni di policy specificate. Unified Manager consente di assegnare SEPS definiti dal sistema e dall'utente per ottimizzare le risorse di storage nel data center.

Unified Manager offre due SEPS definiti dal sistema: Alto e basso. Questi SEPS sono applicabili alla maggior parte dei carichi di lavoro dello storage in un data center; tuttavia, è possibile creare policy personalizzate se i SEPS definiti dal sistema non soddisfano i requisiti.

Non è possibile modificare UN SEP definito dal sistema o attualmente assegnato a un workload. Non è possibile eliminare UN SEP assegnato a un workload o se è l'unico SEP disponibile.

La pagina Storage Efficiency Policies elenca i SEPS disponibili e consente di aggiungere, modificare ed eliminare SEPS personalizzati. In questa pagina vengono visualizzate le seguenti informazioni:

Campo	Descrizione
Nome	Nome DEL SET.
Tipo	Se il criterio è definito dal sistema o dall'utente.
Riserva di spazio	Se il volume è dotato di thin provisioning o thick provisioning.

Campo	Descrizione
Deduplica	Se la deduplica è abilitata sul carico di lavoro: • Inline: La deduplica si verifica durante la scrittura sul carico di lavoro • Background: La deduplica si verifica nel carico di lavoro • Disable (Disattiva): La deduplica è disattivata sul carico di lavoro
Compressione	Se la compressione dei dati è attivata sul carico di lavoro: • Inline: La compressione dei dati si verifica durante la scrittura sul carico di lavoro • Background: La compressione dei dati si verifica nel carico di lavoro • Disable (Disattiva): La compressione dei dati è disattivata sul carico di lavoro
Carichi di lavoro	Numero di carichi di lavoro dello storage a cui è stato assegnato IL SET

Linee guida per la creazione di una policy di efficienza dello storage personalizzata

Se i SEPS esistenti non soddisfano i requisiti delle policy per i carichi di lavoro dello storage, è possibile creare UN SET personalizzato. Tuttavia, si consiglia di tentare di utilizzare il SEPS definito dal sistema per i carichi di lavoro dello storage e di creare solo SEPS personalizzati, se necessario.

È possibile visualizzare IL SET assegnato ai carichi di lavoro nella pagina All workload (tutti i carichi di lavoro) e nella pagina Volume / Health Details (Dettagli volume/salute). È possibile visualizzare il rapporto di riduzione dei dati a livello di cluster in base a queste efficienze dello storage nel pannello Capacity (capacità) del dashboard e nella vista Capacity: All Clusters (capacità: Tutti i cluster).

Creazione e modifica delle policy di efficienza dello storage

Quando le policy di efficienza dello storage definite dal sistema non corrispondono ai requisiti dei carichi di lavoro, è possibile creare policy di efficienza dello storage personalizzate e ottimizzate per i carichi di lavoro.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione.
- Il nome della Storage Efficiency Policy deve essere univoco e non è possibile utilizzare le seguenti parole chiave riservate:

  `High`, `Low`, `Unassigned`, `Learning`, `Idle`, `Default`, e. `None`.

È possibile creare e modificare policy di efficienza dello storage personalizzate dalla pagina Storage Efficiency Policies (Criteri di efficienza dello storage) definendo le caratteristiche di efficienza dello storage necessarie per le applicazioni che accederanno allo storage.

Non è possibile modificare una policy di efficienza dello storage se è attualmente assegnata a un carico di lavoro.

Fasi

1. Nel riquadro di navigazione a sinistra sotto **Impostazioni**, selezionare **Criteri** > **efficienza dello storage**.
2. Nella pagina **Storage Efficiency Policies**, fare clic sul pulsante appropriato a seconda che si desideri creare una nuova Storage Efficiency Policy o modificare una Storage Efficiency Policy esistente.

Per…	Attenersi alla procedura descritta di seguito…
Creare una nuova policy di efficienza dello storage	Fare clic su **Aggiungi**
Modificare una policy di efficienza dello storage esistente	Selezionare una policy di efficienza dello storage esistente e fare clic su **Edit** (Modifica)

   Viene visualizzata la pagina per aggiungere o modificare una policy di efficienza dello storage.

3. Personalizzare la Storage Efficiency Policy specificando le caratteristiche di efficienza dello storage, quindi fare clic su **Submit** per salvare la Storage Efficiency Policy.

È possibile applicare la nuova policy sull'efficienza dello storage o modificarla ai workload (LUN, condivisioni file NFS, condivisioni CIFS) dalla pagina workload o durante il provisioning di un nuovo workload.

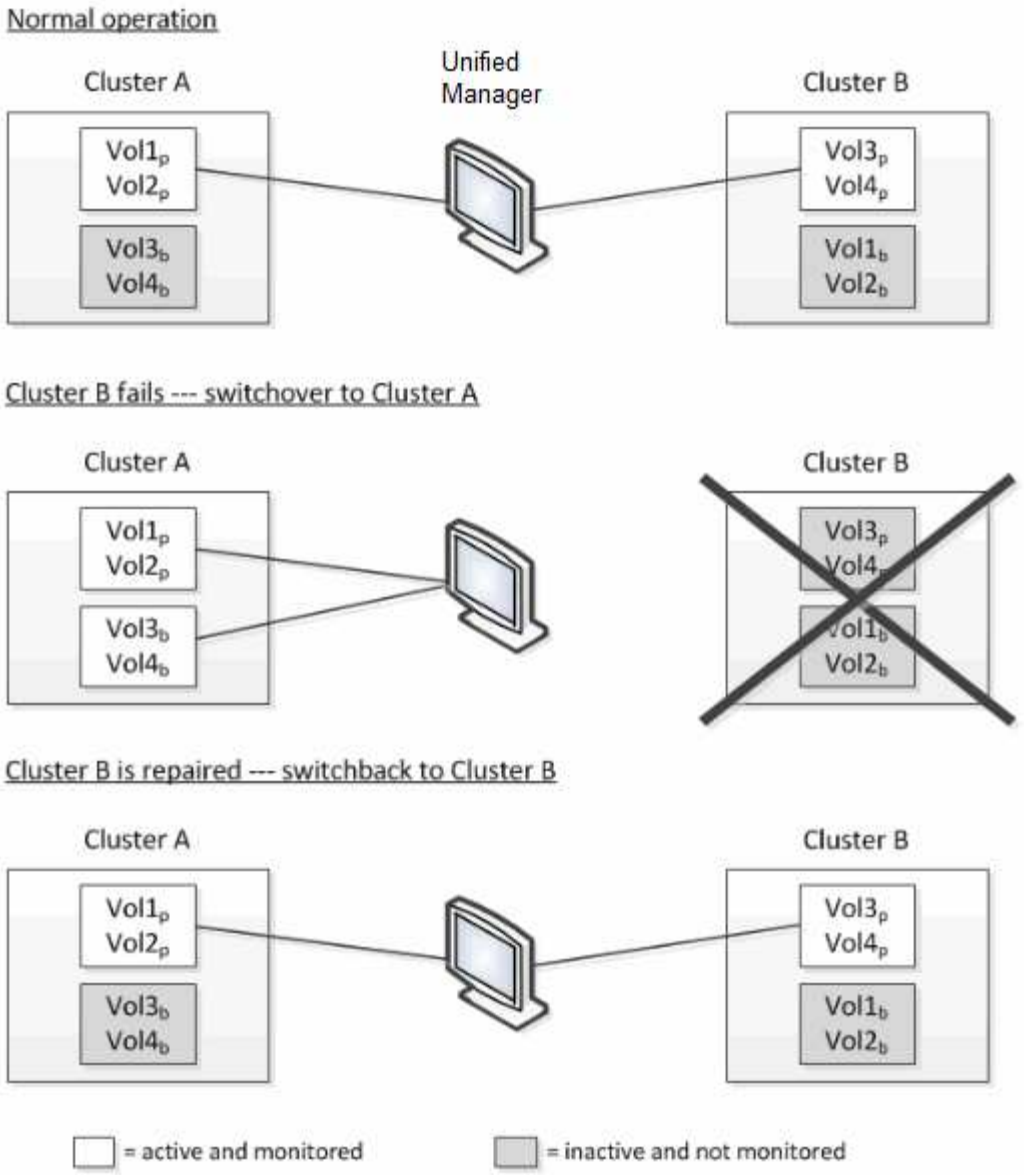
Gestione e monitoraggio delle configurazioni MetroCluster

Il supporto per il monitoraggio delle configurazioni MetroCluster nell'interfaccia utente Web di Unified Manager consente di verificare la presenza di eventuali problemi di connettività nelle configurazioni MetroCluster su FC e IP. Il rilevamento anticipato di un problema di connettività consente di gestire in modo efficace le configurazioni MetroCluster.

Comportamento del volume durante lo switchover e lo switchback

Gli eventi che attivano uno switchover o uno switchback causano lo spostamento dei volumi attivi da un cluster all'altro nel gruppo di disaster recovery. I volumi sul cluster attivi e che forniscono dati ai client vengono arrestati e i volumi sull'altro cluster vengono attivati e iniziano a servire i dati. Unified Manager monitora solo i volumi attivi e in esecuzione.

Poiché i volumi vengono spostati da un cluster all'altro, si consiglia di monitorare entrambi i cluster. Una singola istanza di Unified Manager può monitorare entrambi i cluster in una configurazione MetroCluster, ma a volte la distanza tra le due posizioni richiede l'utilizzo di due istanze di Unified Manager per monitorare entrambi i cluster. La figura seguente mostra una singola istanza di Unified Manager:



I volumi con p nei loro nomi indicano i volumi primari e i volumi con b nei loro nomi sono volumi di backup mirrorati creati da SnapMirror.

Durante il normale funzionamento:

- Il cluster A ha due volumi attivi: Vol1p e Vol2p.
- Il cluster B ha due volumi attivi: Vol3p e Vol4p.
- Il cluster A ha due volumi inattivi: Vol3b e Vol4b.
- Il cluster B ha due volumi inattivi: Vol1b e Vol2b.

Unified Manager raccoglie le informazioni relative a ciascuno dei volumi attivi (statistiche, eventi e così via). Le statistiche Vol1p e Vol2p vengono raccolte dal cluster A e le statistiche Vol3p e Vol4p vengono raccolte dal cluster B.

Dopo un guasto catastrofico che causa lo switchover dei volumi attivi dal cluster B al cluster A:

- Il cluster A ha quattro volumi attivi: Vol1p, Vol2p, Vol3b e Vol4b.

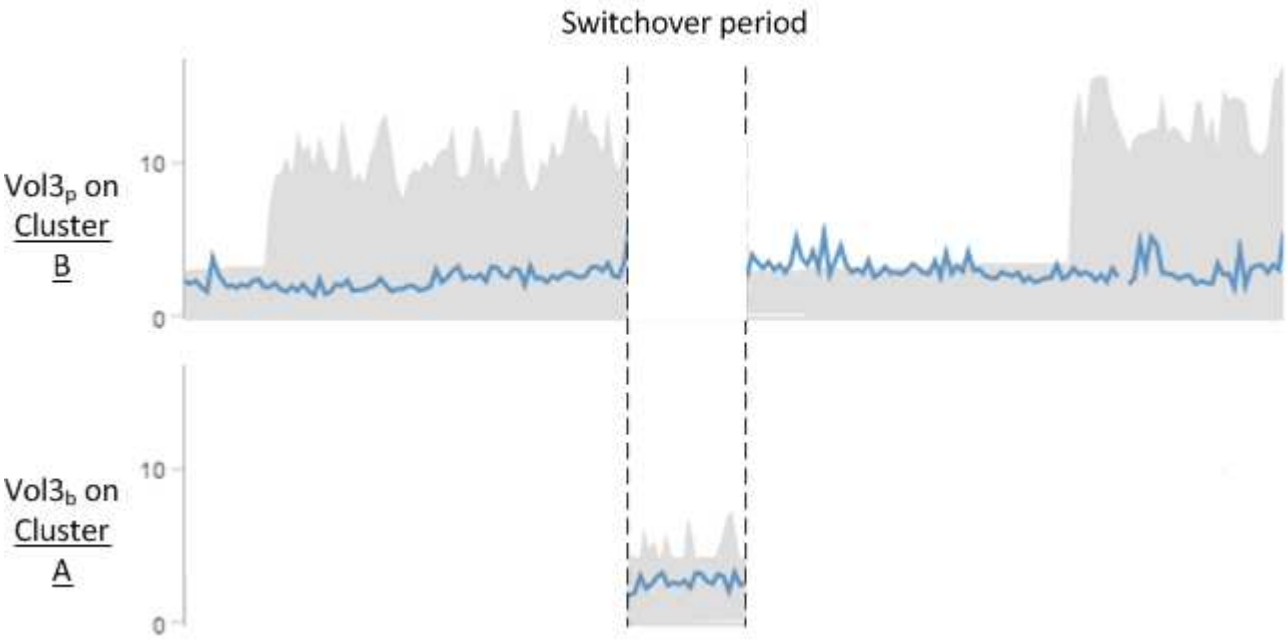
- Il cluster B ha quattro volumi inattivi: Vol3p, Vol4p, Vol1b e Vol2b.

Come durante il normale funzionamento, Unified Manager raccoglie le informazioni relative a ciascuno dei volumi attivi. Tuttavia, in questo caso, le statistiche Vol1p e Vol2p vengono raccolte dal cluster A, mentre le statistiche Vol3b e Vol4b vengono raccolte anche dal cluster A.

Si noti che Vol3p e Vol3b non sono gli stessi volumi, perché si trovano su cluster diversi. Le informazioni di Unified Manager per Vol3p non sono le stesse di Vol3b:

- Durante il passaggio al cluster A, le statistiche e gli eventi di Vol3p non sono visibili.
- Al primo passaggio, Vol3b sembra un nuovo volume senza informazioni storiche.

Quando il cluster B viene riparato e viene eseguito uno switchback, il Vol3p viene nuovamente attivato sul cluster B, con le statistiche storiche e un intervallo di statistiche per il periodo durante lo switchover. Vol3b non è visualizzabile dal cluster A fino a quando non si verifica un altro switchover:



- I volumi MetroCluster inattivi, ad esempio Vol3b sul cluster A dopo lo switchback, vengono identificati con il messaggio “questo volume è stato cancellato”. Il volume non viene effettivamente eliminato, ma non viene attualmente monitorato da Unified Manager perché non è il volume attivo.
- Se un singolo Unified Manager sta monitorando entrambi i cluster in una configurazione MetroCluster, la ricerca del volume restituisce informazioni per il volume attivo in quel momento. Ad esempio, una ricerca di "Vol3" restituisce statistiche ed eventi per Vol3b sul cluster A se si è verificato uno switchover e Vol3 è diventato attivo sul cluster A.

Definizioni dello stato di connettività del cluster per la configurazione MetroCluster su FC

La connettività tra i cluster in una configurazione MetroCluster over FC può essere uno dei seguenti stati: Ottimale, influenzato o inattivo. La comprensione degli stati di connettività consente di gestire in modo efficace le configurazioni MetroCluster.

Stato della connettività	Descrizione	Icona visualizzata
Ottimale	La connettività tra i cluster nella configurazione MetroCluster è normale.	
Interessato	Uno o più errori compromettono lo stato di disponibilità del failover; tuttavia, entrambi i cluster nella configurazione MetroCluster sono ancora in funzione. Ad esempio, quando il collegamento ISL non è attivo, quando il collegamento IP dell'intercluster non è attivo o quando il cluster partner non è raggiungibile.	
Giù	La connettività tra i cluster nella configurazione MetroCluster non è attiva perché uno o entrambi i cluster sono in stato di inattività o i cluster sono in modalità di failover. Ad esempio, quando il cluster del partner è inattivo a causa di un disastro o quando è previsto uno switchover a scopo di test.	Switchover con errori: Switchover riuscito:

Definizioni dello stato del mirroring dei dati per MetroCluster su FC

Le configurazioni MetroCluster su FC offrono il mirroring dei dati e la possibilità aggiuntiva di avviare un failover in caso di indisponibilità di un intero sito. Lo stato del mirroring dei dati tra i cluster in una configurazione MetroCluster su FC può essere normale o mirroring non disponibile. La comprensione dello stato consente di gestire in modo efficace le configurazioni MetroCluster.

Stato del mirroring dei dati	Descrizione	Icona visualizzata
Normale	Il mirroring dei dati tra i cluster nella configurazione MetroCluster è normale.	

Stato del mirroring dei dati	Descrizione	Icona visualizzata
Mirroring non disponibile	Il mirroring dei dati tra i cluster nella configurazione MetroCluster non è disponibile a causa dello switchover. Ad esempio, quando il cluster del partner è inattivo a causa di un disastro o quando è previsto uno switchover a scopo di test.	Switchover con errori: Switchover riuscito:

Monitoraggio delle configurazioni MetroCluster

È possibile monitorare i problemi di connettività nella configurazione MetroCluster. I dettagli includono lo stato dei componenti e della connettività all'interno di un cluster e lo stato della connettività tra i cluster nella configurazione MetroCluster. In questa sezione, è possibile scoprire come monitorare i problemi di connettività nei cluster protetti dalle configurazioni MetroCluster over FC e MetroCluster over IP.

È possibile monitorare le configurazioni MetroCluster dalle seguenti viste dal riquadro di navigazione sinistro di Active IQ Unified Manager:

- **Storage** > **Clusters** > **protezione: Vista MetroCluster**
- **Protezione** > **relazioni** > **relazione: Vista MetroCluster**

Unified Manager utilizza gli avvisi di stato del sistema per indicare lo stato dei componenti e la connettività nella configurazione di MetroCluster.

Cosa ti serve

- I cluster locali e remoti in una configurazione MetroCluster devono essere aggiunti a Active IQ Unified Manager.
- In una configurazione MetroCluster over IP, se si desidera supportare un mediatore, il mediatore deve essere configurato e aggiunto al cluster mediante l'API corrispondente.
- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Monitorare i problemi di connettività nella configurazione MetroCluster over FC

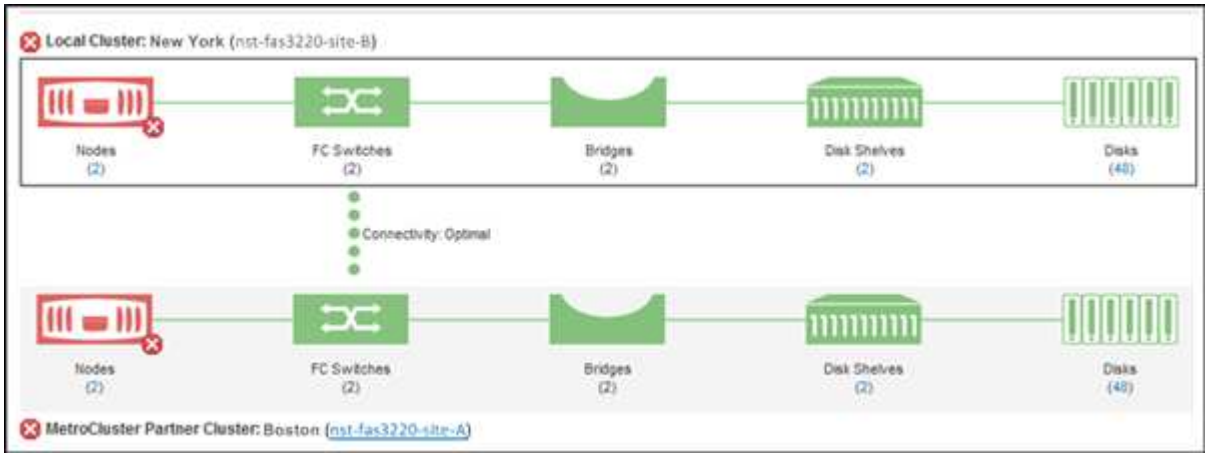
Per i cluster in una configurazione MetroCluster over FC, i grafici di connettività sono visualizzati nella pagina dei dettagli **cluster / integrità**. Seguire questa procedura.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Clusters**.

   Viene visualizzato un elenco di tutti i cluster monitorati.

2. Dalla vista **protezione: MetroCluster**, fare clic sul nome del cluster per il quale si desidera visualizzare i dettagli della configurazione MetroCluster su FC. In alternativa, è possibile filtrare in base ai cluster in una configurazione MetroCluster.
3. Nella pagina dei dettagli **Cluster / integrità**, fare clic sulla scheda **connettività MetroCluster**. La scheda **connettività MetroCluster** è disponibile solo per le configurazioni MetroCluster su FC.



La topologia della configurazione MetroCluster viene visualizzata nell'area degli oggetti del cluster corrispondente. È possibile utilizzare le informazioni visualizzate nella pagina Cluster / Health Details per correggere eventuali problemi di connettività. Ad esempio, se la connettività tra il nodo e lo switch in un cluster non è attiva, viene visualizzata la seguente icona:

Spostando il puntatore sull'icona, è possibile visualizzare informazioni dettagliate sull'evento generato.

Se si riscontrano problemi di connettività nella configurazione MetroCluster, è necessario accedere a Gestione sistema o all'interfaccia utente di ONTAP per risolvere i problemi.

Per ulteriori informazioni sulla determinazione dello stato del cluster, vedere "Determinazione dello stato del cluster nella configurazione MetroCluster over FC".

Monitorare i problemi di connettività nella configurazione MetroCluster over IP

Per i cluster in una configurazione MetroCluster over IP, i grafici di connettività sono visualizzati nella pagina **Clusters**. Seguire questa procedura.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Clusters**.

   Viene visualizzato un elenco di tutti i cluster monitorati.

2. Dalla vista **protezione: MetroClusters**, fare clic sul nome del cluster per il quale si desidera visualizzare i dettagli della configurazione MetroCluster over IP. In alternativa, è possibile filtrare in base ai cluster in una configurazione MetroCluster.
3. Espandere la riga facendo clic sul simbolo di accento circonflesso v icona. L'icona a forma di accento circonflesso viene visualizzata solo per un cluster protetto dalla configurazione MetroCluster over IP.

   È possibile visualizzare la topologia dei siti di origine e mirror, nonché l'eventuale Mediator utilizzato per la connessione. È possibile visualizzare le seguenti informazioni:

- Connettività tra i siti
- Eventuali problemi di salute e disponibilità su entrambi i siti
- Problemi relativi ai mediatori
- Problemi relativi alla replica.

Vengono riportati i seguenti stati: Critico (), errore (), o normale (). È inoltre possibile visualizzare lo stato di replica dei dati aggregati dei dati primari e mirror nella stessa topologia.

Nel diagramma seguente, è possibile osservare che la connettività tra i siti tra i cluster di origine e di destinazione non è disponibile e che il Mediator tra di essi non è configurato.

4. Fare clic sull'icona di stato. Viene visualizzato un messaggio con la definizione dell'errore. Se è stato generato un evento per il problema nella configurazione MetroCluster over IP, fare clic sul pulsante **Visualizza evento** sul messaggio e visualizzare i dettagli dell'evento. Una volta risolto il problema e l'evento, l'icona di stato in questa topologia diventa normale ().
5. È possibile visualizzare ulteriori dettagli di configurazione nelle sezioni **Panoramica MetroCluster** e **protezione** della scheda **Configurazione** della pagina dei dettagli **cluster / integrità**.

Solo per una configurazione MetroCluster over IP, è possibile visualizzare la topologia del cluster nella pagina **Clusters**. Per i cluster in una configurazione MetroCluster over FC, la topologia viene visualizzata nella scheda **connettività MetroCluster** della pagina dei dettagli **cluster / integrità**.

Informazioni correlate

- "Pagina dei dettagli del cluster/stato di salute"
- Per informazioni sulla vista **Relationship:MetroCluster**, vedere "Monitoraggio delle configurazioni MetroCluster".
- Per informazioni sulla vista **Relationship: Last 1 Month Transfer Status** (relazione: Stato trasferimento ultimo 1 mese), vedere "Relazione: Vista Stato trasferimento ultimo 1 mese".
- Per informazioni sulla vista **Relationship: Last 1 Month Transfer Rate** (relazione: Tasso di trasferimento

ultimo 1 mese), vedere "Relazione: Vista tasso di trasferimento dell'ultimo mese".

- Per informazioni sulla vista **relazione: Tutte le relazioni**, vedere "Relazione: Vista tutte le relazioni".

Monitoraggio della replica MetroCluster

È possibile monitorare e diagnosticare le condizioni generali di salute delle connessioni logiche durante il mirroring dei dati. È possibile identificare i problemi o i rischi che interrompono il mirroring dei componenti del cluster come aggregati, nodi e macchine virtuali di storage.

Unified Manager utilizza gli avvisi di stato del sistema per monitorare lo stato dei componenti e la connettività nella configurazione di MetroCluster.

Cosa ti serve

Il cluster locale e remoto nella configurazione MetroCluster deve essere aggiunto a Unified Manager

Visualizzazione della replica per le configurazioni MetroCluster over IP

Per le configurazioni MetroCluster over IP, lo stato della replica dei dati viene visualizzato nella vista topologia per un cluster protetto da MetroCluster over IP dalle seguenti viste dal riquadro di navigazione sinistro di Unified Manager:

- **Storage** > **Clusters** > **protezione: Vista MetroCluster**
- **Protezione** > **relazioni** > **relazione: Vista MetroCluster**

Per ulteriori informazioni, vedere "Monitorare i problemi di connettività in MetroCluster over IP".

Visualizzazione della replica per configurazioni MetroCluster su FC

Per determinare eventuali problemi di replica dei dati per la configurazione MetroCluster su FC, procedere come segue.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Clusters**.

   Viene visualizzato un elenco dei cluster monitorati.

2. Dalla vista **Health: Tutti i cluster**, fare clic sul nome del cluster per il quale si desidera visualizzare i dettagli della replica di MetroCluster. Nella pagina **Dettagli cluster/integrità**, fare clic sulla scheda **Replica MetroCluster**.

   La topologia della configurazione MetroCluster da replicare viene visualizzata nel sito locale nell'area oggetto cluster corrispondente con le informazioni sul sito remoto in cui viene eseguito il mirroring dei dati. Spostando il puntatore sull'icona, è possibile visualizzare informazioni dettagliate sull'evento generato.

È possibile utilizzare le informazioni visualizzate nella pagina Cluster / Health Details per correggere eventuali problemi di replica. Se si riscontrano problemi di mirroring nella configurazione di MetroCluster, è necessario accedere a Gestore di sistema o all'interfaccia utente di ONTAP per risolvere i problemi.

Informazioni correlate

"Pagina dei dettagli del cluster/stato di salute"

Gestione delle quote

È possibile utilizzare le quote utente e di gruppo per limitare la quantità di spazio su disco o il numero di file che un utente o un gruppo di utenti può utilizzare. È possibile visualizzare le informazioni sulle quote di utenti e gruppi di utenti, ad esempio l'utilizzo di dischi e file e i vari limiti impostati sui dischi.

Quali sono i limiti di quota

I limiti di quota utente sono valori che il server Unified Manager utilizza per valutare se il consumo di spazio da parte di un utente si avvicina al limite o ha raggiunto il limite impostato dalla quota dell'utente. Se il limite di tolleranza viene superato o se viene raggiunto il limite massimo, il server Unified Manager genera eventi di quota utente.

Per impostazione predefinita, il server Unified Manager invia un'email di notifica agli utenti che hanno superato il limite di tolleranza della quota o hanno raggiunto il limite massimo della quota e per i quali sono configurati gli eventi di quota utente. Gli utenti con il ruolo di amministratore dell'applicazione possono configurare gli avvisi che notificano ai destinatari specificati gli eventi di quota dell'utente o del gruppo di utenti.

È possibile specificare i limiti di quota utilizzando Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

Visualizzazione delle quote di utenti e gruppi di utenti

La pagina Storage VM / Health Details (Dettagli stato/VM di storage) visualizza informazioni sulle quote utente e gruppo di utenti configurate sulla SVM. È possibile visualizzare il nome dell'utente o del gruppo di utenti, i limiti impostati su dischi e file, lo spazio su disco e file utilizzato e l'indirizzo e-mail per la notifica.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Storage VMS**.
2. Nella vista **Health: All Storage VM**, selezionare una Storage VM, quindi fare clic sulla scheda **User and Group quote** (quote utente e gruppo).

Informazioni correlate

"Aggiunta di utenti"

Creazione di regole per la generazione di indirizzi e-mail

È possibile creare regole per specificare l'indirizzo e-mail in base alla quota utente associata a cluster, storage virtual machine (SVM), volumi, qtree, utenti o gruppi di utenti. Quando si verifica una violazione delle quote, viene inviata una notifica all'indirizzo e-mail specificato.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver esaminato le linee guida nella pagina regole per generare indirizzo email quota utente e gruppo.

È necessario definire le regole per gli indirizzi email di quota e inserirle nell'ordine in cui si desidera eseguirli. Ad esempio, se si desidera utilizzare l'indirizzo e-mail qtree1@xyz.com per ricevere notifiche sulle violazioni delle quote per qtree1 e utilizzare l'indirizzo e-mail admin@xyz.com per tutti gli altri qtree, le regole devono essere elencate nel seguente ordine:

- Se (€ QTREE == 'qtre1') allora qtree1@xyz.com
- Se (QTREE == *) allora admin@xyz.com

Se nessuno dei criteri per le regole specificate viene soddisfatto, viene utilizzata la regola predefinita:

SE (@_USER_OR_GROUP == *), ALLORA IL DOMINIO DI UN UTENTE O DI UN GRUPPO

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **regole email quota**.
2. Inserire la regola in base ai criteri.
3. Fare clic su **Validate** (convalida) per convalidare la sintassi della regola.

   Se la sintassi della regola non è corretta, viene visualizzato un messaggio di errore. Correggere la sintassi e fare nuovamente clic su **Validate**.

4. Fare clic su **Save** (Salva).
5. Verificare che l'indirizzo e-mail creato sia visualizzato nella scheda **quote utente e gruppo** della pagina dei dettagli Storage **VM / Health**.

Creazione di un formato di notifica e-mail per le quote di utenti e gruppi di utenti

È possibile creare un formato di notifica per i messaggi e-mail inviati a un utente o a un gruppo di utenti in caso di problemi relativi alla quota (limite minimo superato o limite massimo raggiunto).

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **formato email quota**.
2. Immettere o modificare i dettagli nei campi **da**, **oggetto** e **Dettagli e-mail**.
3. Fare clic su **Preview** (Anteprima) per visualizzare l'anteprima della notifica via email.
4. Fare clic su **Chiudi** per chiudere la finestra di anteprima.
5. Modificare il contenuto della notifica via email, se necessario.
6. Fare clic su **Save** (Salva).

Modifica degli indirizzi e-mail delle quote di utenti e gruppi

È possibile modificare gli indirizzi e-mail in base alla quota utente associata a cluster, storage virtual machine (SVM), volumi, qtree, utenti o gruppi di utenti. È possibile modificare l'indirizzo e-mail quando si desidera sovrascrivere l'indirizzo e-mail generato dalle regole specificate nella finestra di dialogo regole per generare indirizzo e-mail quota utente e gruppo.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- È necessario aver esaminato "linee guida per la creazione di regole".

Se si modifica un indirizzo e-mail, le regole per generare gli indirizzi e-mail di quota utente e gruppo non sono più applicabili alla quota. Per inviare le notifiche all'indirizzo e-mail generato dalle regole specificate, è necessario eliminare l'indirizzo e-mail e salvare la modifica.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **SVM**.
2. Nella vista **Health: All Storage VMS**, selezionare una SVM e fare clic sulla scheda **User and Group quote** (quote utente e gruppo).
3. Fare clic su **Edit Email Address** (Modifica indirizzo e-mail) sotto la riga delle schede.
4. Nella finestra di dialogo **Modifica indirizzo e-mail**, eseguire l'azione appropriata:

Se…	Quindi…
Si desidera che le notifiche vengano inviate all'indirizzo e-mail generato dalle regole specificate	a. Eliminare l'indirizzo e-mail nel campo **Indirizzo e-mail**. b. Fare clic su **Save** (Salva). c. Aggiornare il browser premendo F5 per ricaricare la finestra di dialogo Modifica indirizzo e-mail. L'indirizzo e-mail generato dalla regola specificata viene visualizzato nel campo **Indirizzo e-mail**.
Si desidera che le notifiche vengano inviate a un indirizzo e-mail specificato	a. Modificare l'indirizzo e-mail nel campo **Indirizzo e-mail**. b. Fare clic su **Save** (Salva). Le regole per generare gli indirizzi email di quota utente e gruppo non sono più applicabili alla quota.

Ulteriori informazioni sulle quote

La comprensione dei concetti relativi alle quote consente di gestire in modo efficiente le quote degli utenti e dei gruppi di utenti.

Panoramica del processo di quota

Le quote possono essere morbide o difficili. Le quote morbide fanno sì che ONTAP invii una notifica quando vengono superati i limiti specificati, mentre le quote rigide impediscono il successo di un'operazione di scrittura quando vengono superati i limiti specificati.

Quando ONTAP riceve una richiesta di scrittura su un volume FlexVol da parte di un utente o di un gruppo di utenti, verifica se le quote sono attivate su tale volume per l'utente o il gruppo di utenti e determina quanto segue:

- Se verrà raggiunto il limite massimo

  In caso affermativo, l'operazione di scrittura non riesce quando viene raggiunto il limite massimo e viene inviata la notifica della quota rigida.

- Se il limite di tolleranza verrà violato

  In caso affermativo, l'operazione di scrittura riesce quando il limite di tolleranza viene superato e viene inviata la notifica della quota di tolleranza.

- Se un'operazione di scrittura non supera il limite di tolleranza

  In caso affermativo, l'operazione di scrittura ha esito positivo e non viene inviata alcuna notifica.

Sulle quote

Le quote consentono di limitare o tenere traccia dello spazio su disco e del numero di file utilizzati da un utente, un gruppo o un qtree. Specificare le quote utilizzando `/etc/quotas` file. Le quote vengono applicate a un volume o qtree specifico.

Perché utilizzare le quote

È possibile utilizzare le quote per limitare l'utilizzo delle risorse nei volumi FlexVol, fornire notifiche quando l'utilizzo delle risorse raggiunge livelli specifici o tenere traccia dell'utilizzo delle risorse.

Specificare una quota per i seguenti motivi:

- Per limitare la quantità di spazio su disco o il numero di file che possono essere utilizzati da un utente o un gruppo o che possono essere contenuti da un qtree
- Per tenere traccia della quantità di spazio su disco o del numero di file utilizzati da un utente, un gruppo o un qtree, senza imporre alcun limite
- Per avvisare gli utenti quando l'utilizzo del disco o del file è elevato

Descrizione delle finestre di dialogo quote

È possibile utilizzare l'opzione appropriata nella scheda quote utente e gruppo nella vista Health: All Storage VM per configurare il formato della notifica e-mail inviata quando si verifica un problema relativo alla quota e per configurare le regole per specificare gli

indirizzi e-mail in base alla quota utente.

Pagina formato notifica email

La pagina formato notifica e-mail visualizza le regole del messaggio e-mail inviato a un utente o a un gruppo di utenti quando si verifica un problema relativo alla quota (limite minimo violato o limite massimo raggiunto).

La notifica e-mail viene inviata solo quando vengono generati i seguenti eventi di quota utente o gruppo di utenti: Limite di spazio su disco per quota utente o gruppo superato, limite di tolleranza per il numero di file per quota utente o gruppo superato, limite di tolleranza per lo spazio su disco per quota utente o gruppo raggiunto o limite massimo per il numero di file per quota utente o gruppo raggiunto.

- **Da**

  Visualizza l'indirizzo e-mail da cui viene inviato il messaggio e-mail, che è possibile modificare. Per impostazione predefinita, si tratta dell'indirizzo e-mail specificato nella pagina Notifiche.

- **Soggetto**

  Visualizza l'oggetto dell'e-mail di notifica.

- **Dettagli e-mail**

  Visualizza il testo dell'e-mail di notifica. È possibile modificare il testo in base alle proprie esigenze. Ad esempio, è possibile fornire informazioni relative agli attributi di quota e ridurre il numero di parole chiave. Tuttavia, non modificare le parole chiave.

  Le parole chiave valide sono le seguenti:

  - NOME_EVENTO

    Specifica il nome dell'evento che ha causato la notifica via email.

  - QUOTA_DESTINAZIONE

    Specifica il qtree o il volume su cui è applicabile la quota.

  - QUOTA_UTILIZZATA_PERCENTUALE DOLLARI

    Specifica la percentuale di limite hard disk, soft limit disk, hard limit file o soft limit file utilizzata dall'utente o dal gruppo di utenti.

  - QUOTA_LIMITE

    Specifica il limite massimo del disco rigido o del file raggiunto dall'utente o dal gruppo di utenti e viene generato uno dei seguenti eventi:

    - Limite massimo di spazio su disco per quota utente o gruppo raggiunto
    - Limite di spazio su disco per quota utente o gruppo raggiunto
    - Numero di file di quota utente o gruppo - limite massimo raggiunto
    - Limite minimo di numero file quota utente o gruppo raggiunto

  - QUOTA_UTILIZZATA

Specifica lo spazio su disco utilizzato o il numero di file creati dall'utente o dal gruppo di utenti.

- QUOTA_UTENTE

  Specifica il nome dell'utente o del gruppo di utenti.

Pulsanti di comando

I pulsanti di comando consentono di visualizzare in anteprima, salvare o annullare le modifiche apportate al formato di notifica e-mail:

- **Anteprima**

  Visualizza un'anteprima dell'email di notifica.

- **Ripristina impostazioni predefinite**

  Consente di ripristinare i valori predefiniti del formato di notifica.

- **Salva**

  Salva le modifiche apportate al formato di notifica.

Regole per generare la pagina Indirizzo email quota utente e gruppo

La pagina Rules to generate User and Group quota Email Address (regole per generare indirizzo email quota utente e gruppo) consente di creare regole per specificare gli indirizzi email in base alla quota utente associata a cluster, SVM, volumi, qtree, utenti, o gruppi di utenti. Quando una quota viene violata, viene inviata una notifica all'indirizzo e-mail specificato.

Area delle regole

È necessario definire le regole per un indirizzo e-mail di quota. Puoi anche aggiungere commenti per spiegare le regole.

Come definire le regole

È necessario immettere le regole nell'ordine in cui si desidera eseguirle. Se il criterio della prima regola viene soddisfatto, l'indirizzo e-mail viene generato in base a questa regola. Se il criterio non viene soddisfatto, viene preso in considerazione il criterio per la regola successiva e così via. Ogni riga elenca una regola separata. La regola predefinita è l'ultima regola dell'elenco. È possibile modificare l'ordine di priorità delle regole. Tuttavia, non è possibile modificare l'ordine della regola predefinita.

Ad esempio, se si desidera utilizzare l'indirizzo e-mail qtree1@xyz.com per ricevere notifiche sulle violazioni delle quote per qtree1 e utilizzare l'indirizzo e-mail admin@xyz.com per tutti gli altri qtree, le regole devono essere elencate nel seguente ordine:

- Se (€ QTREE == 'qtre1') allora qtree1@xyz.com
- Se (QTREE == *) allora admin@xyz.com

Se nessuno dei criteri per le regole specificate viene soddisfatto, viene utilizzata la regola predefinita:

SE (@_USER_OR_GROUP == *), ALLORA IL DOMINIO DI UN UTENTE O DI UN GRUPPO

Se più utenti hanno la stessa quota, i nomi degli utenti vengono visualizzati come valori separati da virgole e le regole non sono applicabili alla quota.

Come aggiungere commenti

È possibile aggiungere commenti per spiegare le regole. All'inizio di ogni commento, devi usare il numero e ogni riga elenca un commento separato.

Sintassi delle regole

La sintassi della regola deve essere una delle seguenti:

- se (`valid variableoperator *`) quindi `email ID@domain name`

  se è una parola chiave ed è in minuscolo. L'operatore è ==. L'ID e-mail può contenere qualsiasi carattere, le variabili valide utente_O_GRUPPO, utente_dollari o gruppo di dollari o una combinazione di qualsiasi carattere e le variabili valide utente_O_GRUPPO, UTENTE_dollari o GRUPPO di dollari. Il nome di dominio può contenere qualsiasi carattere, LA variabile valida dominio dollari o una combinazione di qualsiasi carattere e la variabile valida DOMINIO dollari. Le variabili valide possono essere in lettere maiuscole o minuscole, ma non devono essere una combinazione di entrambe. Ad esempio, il dominio e il DOMINIO sono validi, ma il dominio non è una variabile valida.

- se (`valid variableoperator `string`) quindi `email ID@domain name`

  se è una parola chiave ed è minuscolo. L'operatore può contenere o ==. L'ID e-mail può contenere qualsiasi carattere, le variabili valide utente_O_GRUPPO, utente_dollari o gruppo di dollari o una combinazione di qualsiasi carattere e le variabili valide utente_O_GRUPPO, UTENTE_dollari o GRUPPO di dollari. Il nome di dominio può contenere qualsiasi carattere, LA variabile valida dominio dollari o una combinazione di qualsiasi carattere e la variabile valida DOMINIO dollari. Le variabili valide possono essere in lettere maiuscole o minuscole, ma non devono essere una combinazione di entrambe. Ad esempio, il dominio e il DOMINIO sono validi, ma il dominio non è una variabile valida.

Pulsanti di comando

I pulsanti di comando consentono di salvare, convalidare o annullare le regole create:

- **Convalidare**

  Convalida la sintassi della regola creata. In caso di errori durante la convalida, viene visualizzata la regola che genera l'errore insieme a un messaggio di errore.

- **Ripristina impostazioni predefinite**

  Consente di ripristinare i valori predefiniti delle regole degli indirizzi.

- **Salva**

  Convalida la sintassi della regola e la salva se non sono presenti errori. In caso di errori durante la convalida, viene visualizzata la regola che genera l'errore insieme a un messaggio di errore.

Risoluzione dei problemi

Le informazioni per la risoluzione dei problemi consentono di identificare e risolvere i problemi riscontrati durante l'utilizzo di Unified Manager.

Aggiunta di spazio su disco alla directory del database di Unified Manager

La directory del database di Unified Manager contiene tutti i dati relativi allo stato e alle performance raccolti dai sistemi ONTAP. In alcuni casi, potrebbe essere necessario aumentare le dimensioni della directory del database.

Ad esempio, la directory del database potrebbe essere piena se Unified Manager sta raccogliendo dati da un gran numero di cluster in cui ciascun cluster ha molti nodi. Si riceverà un avviso quando la directory del database è piena al 90% e un evento critico quando la directory è piena al 95%.

> Non vengono raccolti dati aggiuntivi dai cluster dopo che la directory raggiunge il 95% di riempimento.

I passaggi necessari per aggiungere capacità alla directory dei dati sono diversi a seconda che Unified Manager sia in esecuzione su un server VMware ESXi, Red Hat o CentOS Linux o su un server Microsoft Windows.

Aggiunta di spazio al disco dati della macchina virtuale VMware

Se è necessario aumentare la quantità di spazio sul disco dati per il database di Unified Manager, è possibile aggiungere capacità dopo l'installazione aumentando lo spazio su disco utilizzando la console di manutenzione di Unified Manager.

Cosa ti serve

- È necessario disporre dell'accesso al client vSphere.
- La macchina virtuale non deve contenere snapshot memorizzate localmente.
- È necessario disporre delle credenziali utente di manutenzione.

Si consiglia di eseguire il backup della macchina virtuale prima di aumentare le dimensioni dei dischi virtuali.

Fasi

1. Nel client vSphere, selezionare la macchina virtuale Unified Manager, quindi aggiungere ulteriore capacità del disco ai dati `disk 3`. Per ulteriori informazioni, consultare la documentazione di VMware.

   In alcuni rari casi, l'implementazione di Unified Manager utilizza "Hard Disk 2" per il disco dati invece di "Hard Disk 3". Se questo si è verificato durante l'implementazione, aumentare lo spazio di qualsiasi disco più grande. Il disco dati avrà sempre più spazio rispetto all'altro disco.

2. Nel client vSphere, selezionare la macchina virtuale Unified Manager, quindi selezionare la scheda **Console**.
3. Fare clic su nella finestra della console, quindi accedere alla console di manutenzione utilizzando il nome utente e la password.
4. Nel **Menu principale**, inserire il numero dell'opzione **Configurazione di sistema**.

5. Nel menu **System Configuration Menu**, inserire il numero dell'opzione **aumenta dimensioni disco dati**.

Aggiunta di spazio alla directory dei dati dell'host Linux

Se è stato assegnato spazio su disco insufficiente a `/opt/netapp/data` Directory per supportare Unified Manager quando si configura originariamente l'host Linux e si installa Unified Manager, è possibile aggiungere spazio su disco dopo l'installazione aumentando lo spazio su disco su `/opt/netapp/data` directory.

Cosa ti serve

È necessario disporre dell'accesso utente root alla macchina Red Hat Enterprise Linux o CentOS Linux su cui è installato Unified Manager.

Si consiglia di eseguire il backup del database di Unified Manager prima di aumentare le dimensioni della directory dei dati.

Fasi

1. Accedere come utente root alla macchina Linux su cui si desidera aggiungere spazio su disco.
2. Arrestare il servizio Unified Manager e il software MySQL associato nell'ordine indicato: `systemctl stop ocieau ocie mysqld`
3. Creare una cartella di backup temporanea (ad esempio, `/backup-data`) con spazio su disco sufficiente per contenere i dati nella corrente `/opt/netapp/data` directory.
4. Copiare il contenuto e la configurazione dei privilegi dell'esistente `/opt/netapp/data` directory nella directory dei dati di backup:

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

5. Se Linux è attivato:

   a. Ottenere il tipo di se Linux per le cartelle esistenti `/opt/netapp/data` cartella:

      ```
      se_type=`ls -Z /opt/netapp/data| awk '{print $4}'| awk -F: '{print $3}'|
      head -1
      ```

      Il sistema restituisce una conferma simile a quanto segue:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Eseguire `chcon` Per impostare il tipo di se Linux per la directory di backup:

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. Rimuovere il contenuto di `/opt/netapp/data` directory:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. Espandere le dimensioni di `/opt/netapp/data` Directory fino a un minimo di 150 GB tramite comandi LVM o aggiungendo dischi aggiuntivi.

   Se hai creato `/opt/netapp/data` da un disco, quindi non si dovrebbe provare a montare `/opt/netapp/data` Come condivisione NFS o CIFS. Perché, in questo caso, se si tenta di espandere lo spazio su disco, alcuni comandi LVM, ad esempio `resize` e. `extend` potrebbe non funzionare come previsto.

8. Verificare che il `/opt/netapp/data` il proprietario della directory (mysql) e il gruppo (root) rimangono invariati:

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

   Il sistema restituisce una conferma simile a quanto segue:

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

9. Se Linux è attivato, verificare che il contesto per `/opt/netapp/data` la directory è ancora impostata su mysqld_db_t:

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

      Il sistema restituisce una conferma simile a quanto segue:

   ```
   -rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
   /opt/netapp/data/abc
   ```

10. Eliminare il file `abc` in modo che questo file estraneo non causi un errore di database in futuro.
11. Copiare il contenuto da `backup-data` torna all'expanded `/opt/netapp/data` directory:

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

12. Se Linux è attivato, eseguire il seguente comando:

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

13. Avviare il servizio MySQL:

    ```
    systemctl start mysqld
    ```

14. Una volta avviato il servizio MySQL, avviare i servizi ocie e ocieau nell'ordine indicato:

    ```
    systemctl start ocie ocieau
    ```

15. Una volta avviati tutti i servizi, eliminare la cartella di backup `/backup-data`:

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

Aggiunta di spazio all'unità logica del server Microsoft Windows

Se è necessario aumentare la quantità di spazio su disco per il database di Unified Manager, è possibile aggiungere capacità all'unità logica su cui è installato Unified Manager.

Cosa ti serve

È necessario disporre dei privilegi di amministratore di Windows.

Si consiglia di eseguire il backup del database di Unified Manager prima di aggiungere spazio su disco.

Fasi

1. Accedere come amministratore al server Windows su cui si desidera aggiungere spazio su disco.
2. Seguire la procedura corrispondente al metodo che si desidera utilizzare per aggiungere ulteriore spazio:

Opzione	Descrizione
Su un server fisico, aggiungere capacità all'unità logica su cui è installato il server Unified Manager.	Seguire la procedura descritta nell'argomento Microsoft: "Estensione di un volume di base"
Su un server fisico, aggiungere un disco rigido.	Seguire la procedura descritta nell'argomento Microsoft: "Aggiunta di dischi rigidi"
Su una macchina virtuale, aumentare le dimensioni di una partizione del disco.	Seguire la procedura descritta nell'argomento VMware: "Aumento delle dimensioni di una partizione del disco"

Modifica dell'intervallo di raccolta delle statistiche delle performance

L'intervallo di raccolta predefinito per le statistiche delle performance è di 5 minuti. È possibile modificare questo intervallo in 10 o 15 minuti se si rileva che le raccolte di cluster di grandi dimensioni non vengono terminate entro il tempo predefinito. Questa impostazione influisce sulla raccolta di statistiche di tutti i cluster monitorati da questa istanza di Unified Manager.

Cosa ti serve

Per accedere alla console di manutenzione del server Unified Manager, è necessario disporre di un ID utente e di una password autorizzati.

Il problema delle raccolte di statistiche delle performance che non terminano in tempo è indicato dai messaggi banner `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>.`

È necessario modificare l'intervallo di raccolta solo quando richiesto a causa di un problema di raccolta di statistiche. Non modificare questa impostazione per altri motivi.

> La modifica di questo valore dall'impostazione predefinita di 5 minuti può influire sul numero e sulla frequenza degli eventi relativi alle performance segnalati da Unified Manager. Ad esempio, le soglie di performance definite dal sistema attivano eventi quando il criterio viene superato per 30 minuti. Quando si utilizzano raccolte di 5 minuti, la policy deve essere superata per sei raccolte consecutive. Per le raccolte di 15 minuti, la policy deve essere superata solo per due periodi di raccolta.

Un messaggio nella parte inferiore della pagina Cluster Setup indica l'intervallo corrente di raccolta dei dati statistici.

Fasi

1. Accedere utilizzando SSH come utente di manutenzione all'host di Unified Manager.

   Vengono visualizzati i prompt della console di Unified Managermaintenance.

2. Digitare il numero dell'opzione di menu **Performance polling Interval Configuration** (Configurazione intervallo di polling delle prestazioni), quindi premere Invio.
3. Se richiesto, inserire nuovamente la password utente per la manutenzione.
4. Digitare il numero del nuovo intervallo di polling che si desidera impostare, quindi premere Invio.

Se l'intervallo di raccolta di Unified Manager è stato modificato su 10 o 15 minuti e si dispone di una connessione corrente a un provider di dati esterno (ad esempio Graphite), è necessario modificare l'intervallo di trasmissione del provider di dati in modo che sia uguale o superiore all'intervallo di raccolta di Unified Manager.

Modifica del periodo di tempo in cui Unified Manager conserva i dati relativi a eventi e performance

Per impostazione predefinita, Unified Manager memorizza i dati degli eventi e le performance per 6 mesi per tutti i cluster monitorati. Trascorso questo tempo, i dati meno recenti vengono cancellati automaticamente per fare spazio ai nuovi dati. Questo periodo di tempo predefinito funziona bene per la maggior parte delle configurazioni, ma configurazioni molto grandi con molti cluster e nodi potrebbero dover ridurre il periodo di conservazione in modo che Unified Manager funzioni in modo ottimale.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

È possibile modificare i periodi di conservazione per questi due tipi di dati nella pagina conservazione dati. Queste impostazioni influiscono sulla conservazione dei dati di tutti i cluster monitorati da questa istanza di Unified Manager.

> Unified Manager raccoglie le statistiche delle performance ogni 5 minuti. Ogni giorno le statistiche di 5 minuti vengono riepilogate in statistiche orarie delle performance. Conserva 30 giorni di dati storici delle performance di 5 minuti e 6 mesi di dati delle performance riepilogati ogni ora (per impostazione predefinita).

È necessario ridurre il periodo di conservazione solo se lo spazio è esaurito o se il backup e altre operazioni richiedono molto tempo. La riduzione del periodo di conservazione ha i seguenti effetti:

- I vecchi dati sulle performance vengono cancellati dal database di Unified Manager dopo la mezzanotte.
- I vecchi dati degli eventi vengono cancellati immediatamente dal database di Unified Manager.
- Gli eventi precedenti al periodo di conservazione non saranno più disponibili per la visualizzazione nell'interfaccia utente.
- Le posizioni nell'interfaccia utente in cui vengono visualizzate le statistiche delle performance orarie saranno vuote prima del periodo di conservazione.
- Se il periodo di conservazione degli eventi supera il periodo di conservazione dei dati relativi alle performance, sotto il dispositivo di scorrimento delle performance viene visualizzato un messaggio che avvisa che gli eventi relativi alle performance precedenti potrebbero non avere dati di backup nei grafici associati.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Policy** > **Data Retention**.
2. Nella pagina **Data Retention**, selezionare lo strumento di scorrimento nell'area Event Retention (conservazione eventi) o Performance Data Retention (conservazione dati performance) e spostarlo sul numero di mesi in cui i dati devono essere conservati, quindi fare clic su **Save** (Salva).

Errore di autenticazione sconosciuto

Quando si esegue un'operazione correlata all'autenticazione, ad esempio l'aggiunta, la modifica, l'eliminazione o il test di utenti o gruppi remoti, potrebbe essere visualizzato il seguente messaggio di errore: `Unknown authentication error.`

Causa

Questo problema può verificarsi se è stato impostato un valore errato per le seguenti opzioni:

- Nome dell'amministratore del servizio di autenticazione di Active Directory
- BIND Distinguished Name del servizio di autenticazione OpenLDAP

Azione correttiva

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. In base al servizio di autenticazione selezionato, immettere le informazioni appropriate per Nome amministratore o Binding Distinguished Name.
3. Fare clic su **Test Authentication** (verifica autenticazione) per verificare l'autenticazione con i dettagli specificati.
4. Fare clic su **Save** (Salva).

Utente non trovato

Quando si esegue un'operazione correlata all'autenticazione, ad esempio l'aggiunta, la modifica, l'eliminazione o il test di utenti o gruppi remoti, viene visualizzato il seguente messaggio di errore: `User not found.`

Causa

Questo problema può verificarsi se l'utente esiste nel server ad o nel server LDAP e se il nome distinto di base è stato impostato su un valore errato.

Azione correttiva

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Inserire le informazioni appropriate per il nome distinto della base.
3. Fare clic su **Save** (Salva).

Problema con l'aggiunta di LDAP utilizzando altri servizi di autenticazione

Quando si seleziona altri come servizio di autenticazione, l'utente e il gruppo Object Class conservano i valori del modello precedentemente selezionato. Se il server LDAP non utilizza gli stessi valori, l'operazione potrebbe non riuscire.

Causa

Gli utenti non sono configurati correttamente in OpenLDAP.

Azione correttiva

È possibile risolvere manualmente questo problema utilizzando una delle seguenti soluzioni alternative.

Se la classe di oggetti utente LDAP e la classe di oggetti gruppo sono rispettivamente utente e gruppo, eseguire la seguente procedura:

1. Nel riquadro di spostamento a sinistra, fare clic su**General** > **Remote Authentication**.
2. Nel menu a discesa **Servizio di autenticazione**, selezionare **Active Directory**, quindi selezionare **altri**.
3. Compilare i campi di testo.

Se la classe di oggetti utente LDAP e la classe di oggetti di gruppo sono rispettivamente positxAccount e positxGroup, attenersi alla seguente procedura:

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Nel menu a discesa **Authentication Service**, selezionare **OpenLDAP**, quindi **altri**.
3. Compilare i campi di testo.

Se le prime due soluzioni alternative non sono valide, chiamare il `option-set` API e impostare `auth.ldap.userObjectClass` e. `auth.ldap.groupObjectClass` opzioni per i valori corretti.

Gestire eventi e avvisi

Gestione degli eventi

Gli eventi consentono di identificare i problemi dei cluster monitorati.

Quali sono gli eventi della piattaforma Active IQ

Unified Manager può visualizzare gli eventi rilevati dalla piattaforma Active IQ. Questi eventi vengono creati eseguendo una serie di regole per i messaggi AutoSupport generati da tutti i sistemi storage monitorati da Unified Manager.

Per ulteriori informazioni, vedere "Come vengono generati gli eventi della piattaforma Active IQ".

Unified Manager verifica automaticamente la presenza di un nuovo file di regole e lo scarica solo quando sono presenti regole più recenti. Nei siti senza accesso alla rete esterna, è necessario caricare manualmente le regole da **Storage Management** > **Event Setup** > **Upload Rules**.

Questi eventi di Active IQ non si sovrappongono agli eventi di Unified Manager esistenti e identificano incidenti o rischi relativi a configurazione del sistema, cablaggio, Best practice e problemi di disponibilità.

Per ulteriori informazioni sull'attivazione degli eventi della piattaforma, vedere "Attivazione degli eventi del portale Active IQ". Per ulteriori informazioni sul caricamento del file di regole, vedere "Caricamento di un nuovo file di regole Active IQ".

NetApp Active IQ è un servizio basato sul cloud che offre analisi predittive e supporto proattivo per ottimizzare le operazioni del sistema storage nel cloud ibrido NetApp. Vedere "NetApp Active IQ" per ulteriori informazioni.

Quali sono gli eventi del sistema di gestione degli eventi

Il sistema di gestione degli eventi (EMS) raccoglie i dati degli eventi da diverse parti del kernel di ONTAP e fornisce meccanismi di inoltro degli eventi. Questi eventi ONTAP possono essere riportati come eventi EMS in Unified Manager. Il monitoraggio e la gestione centralizzati facilitano la configurazione degli eventi EMS critici e delle notifiche di avviso in base a questi eventi EMS.

L'indirizzo di Unified Manager viene aggiunto come destinazione di notifica al cluster quando si aggiunge il cluster a Unified Manager. Un evento EMS viene segnalato non appena si verifica l'evento nel cluster.

Sono disponibili due metodi per ricevere eventi EMS in Unified Manager:

- Un certo numero di eventi EMS importanti viene segnalato automaticamente.
- È possibile iscriversi per ricevere singoli eventi EMS.

Gli eventi EMS generati da Unified Manager vengono segnalati in modo diverso a seconda del metodo con cui è stato generato l'evento:

Funzionalità	Messaggi EMS automatici	Messaggi EMS sottoscritti
Eventi EMS disponibili	Sottoinsieme di eventi EMS	Tutti gli eventi EMS

Funzionalità	Messaggi EMS automatici	Messaggi EMS sottoscritti
Nome del messaggio EMS quando attivato	Nome evento di Unified Manager (convertito dal nome evento EMS)	Non specifico nel formato "Error EMS Received" (errore EMS ricevuto). Il messaggio dettagliato fornisce il formato di notazione a punti dell'evento EMS effettivo
Messaggi ricevuti	Non appena il cluster viene scoperto	Dopo aver aggiunto ogni evento EMS richiesto a Unified Manager e dopo il successivo ciclo di polling di 15 minuti
Ciclo di vita dell'evento	Come per gli altri eventi di Unified Manager: stato nuovo, riconosciuto, risolto e obsoleto	L'evento EMS viene reso obsoleto dopo l'aggiornamento del cluster, dopo 15 minuti, dalla creazione dell'evento
Acquisisce gli eventi durante il downtime di Unified Manager	Sì, all'avvio del sistema comunica con ciascun cluster per acquisire gli eventi mancanti	No
Dettagli dell'evento	Le azioni correttive suggerite vengono importate direttamente da ONTAP per fornire risoluzioni coerenti	Azioni correttive non disponibili nella pagina Dettagli evento

Alcuni dei nuovi eventi EMS automatici sono eventi informativi che indicano che un evento precedente è stato risolto. Ad esempio, l'evento informativo "FlexGroup costituenti spazio Stato tutto OK" indica che l'evento di errore "FlexGroup costituenti hanno problemi di spazio" è stato risolto. Gli eventi informativi non possono essere gestiti utilizzando lo stesso ciclo di vita degli eventi degli altri tipi di gravità degli eventi, tuttavia, l'evento viene reso obsoleto automaticamente se lo stesso volume riceve un altro evento di errore "problemi di ritmo `S`".

Eventi EMS aggiunti automaticamente a Unified Manager

I seguenti eventi EMS di ONTAP vengono aggiunti automaticamente a Unified Manager. Questi eventi verranno generati quando vengono attivati su qualsiasi cluster monitorato da Unified Manager.

I seguenti eventi EMS sono disponibili durante il monitoraggio dei cluster con software ONTAP 9.5 o superiore:

Nome evento di Unified Manager	Nome evento EMS	Risorsa interessata	Severità di Unified Manager
Accesso al livello cloud negato per il trasferimento aggregato	arl.netra.ca.check.failed	Aggregato	Errore

Nome evento di Unified Manager	Nome evento EMS	Risorsa interessata	Severità di Unified Manager
Accesso di livello cloud negato per il trasferimento aggregato durante il failover dello storage	gb.netra.ca.check.failed	Aggregato	Errore
Risincronizzazione replica mirror FabricPool completata	wafl.ca.resync.complete	Cluster	Errore
Spazio FabricPool quasi pieno	fabricpool.nehly.full	Cluster	Errore
Inizio del periodo NVMe-of Grace	nvmf.graceperiod.start	Cluster	Attenzione
Periodo di tolleranza NVMe attivo	nvmf.graceperiod.active	Cluster	Attenzione
Periodo di tolleranza NVMe scaduto	nvmf.graceperiod.expired	Cluster	Attenzione
LUN distrutta	lun.destroy	LUN	Informazioni
Cloud AWS MetaDataConnFail	Cloud.aws.metadataConnFail	Nodo	Errore
Cloud AWS IAMCredsExpired	Cloud.aws.iamCredsExpired	Nodo	Errore
Cloud AWS IAMCredsInvalid (IAMCrediti AWS cloud non	Cloud.aws.iamCredsInvalid	Nodo	Errore
Cloud AWS IAMCredsNotFound	Cloud.aws.iamCredsNotFound	Nodo	Errore
Cloud AWS IAMCredsNotInitialized	Cloud.aws.iamNotInitialized	Nodo	Informazioni
Cloud AWS IAMRoleInvalid (IAMRoleInvalid	Cloud.aws.iamRoleInvalid	Nodo	Errore

Nome evento di Unified Manager	Nome evento EMS	Risorsa interessata	Severità di Unified Manager
Cloud AWS IAMRoleNotFound	Cloud.aws.iamRoleNotFound	Nodo	Errore
Host di livello cloud irrisolvibile	objstore.host.unresolvable	Nodo	Errore
Livello cloud LIF Intercluster inattivo	objstore.interclusterlifDown	Nodo	Errore
Richiesta di una firma del livello cloud non corrispondente	osc.signatureMismatch	Nodo	Errore
Uno dei pool NFSv4 esaurito	Nblade.nfsV4PoolExhaust	Nodo	Critico
Memoria monitor QoS massima	qos.monitor.memory.maxed	Nodo	Errore
Memoria monitor QoS esaurita	qos.monitor.memory.abated	Nodo	Informazioni
NVMeNS distruggere	NVMeNS.destroy	Namespace	Informazioni
NVMeNS online	NVMeNS.offline	Namespace	Informazioni
NVMNS non in linea	NVMeNS.online	Namespace	Informazioni
NVMeNS fuori spazio	NVMeNS.out.of.space	Namespace	Attenzione
Replica sincrona fuori sincronizzazione	sms.status.out.of.sync	Relazione di SnapMirror	Attenzione
Replica sincrona ripristinata	sms.status.in.sync	Relazione di SnapMirror	Informazioni
Risincronizzazione automatica replica sincrona non riuscita	sms.resync.tentativo.non riuscito	Relazione di SnapMirror	Errore
Molte connessioni CIFS	Nblade.cifsManyAuths	SVM	Errore
Connessione CIFS massima superata	Nblade.cifsMaxOpenSameFile	SVM	Errore

Nome evento di Unified Manager	Nome evento EMS	Risorsa interessata	Severità di Unified Manager
È stato superato il numero massimo di connessioni CIFS per utente	Nblade.cifsMaxSessPerUsrConn	SVM	Errore
Conflitto nome NetBIOS CIFS	Nblade.cifsNbNameConflict	SVM	Errore
Tentativi di connessione di una condivisione CIFS inesistente	Nblade.cifsNoPrivShare	SVM	Critico
Operazione di copia shadow CIFS non riuscita	cifs.shadowcopy.failure	SVM	Errore
Virus rilevato dal server AV	Nblade.vscanVirusDetected	SVM	Errore
Nessuna connessione al server AV per Virus Scan	Nblade.vscanNoSannerConn	SVM	Critico
Nessun server AV registrato	Nblade.vscanNoRegdscanner	SVM	Errore
Nessuna connessione al server AV reattiva	Nblade.vscanConnInactive	SVM	Informazioni
Server AV troppo occupato per accettare una nuova richiesta di scansione	Nblade.vscanConnBackPressure	SVM	Errore
Tentativo di utente non autorizzato di accedere al server AV	Nblade.vscanBadUserPrivAccess	SVM	Errore
I componenti FlexGroup presentano problemi di spazio	flexgroup.costituenti.hanno.spazio.problemi	Volume	Errore
Stato dello spazio dei componenti FlexGroup OK	flexgroup.costituenti.spazio.stato.tutto.ok	Volume	Informazioni
I componenti FlexGroup presentano problemi di nodi	flexgroup.constituents.have.inodes.issues	Volume	Errore

Nome evento di Unified Manager	Nome evento EMS	Risorsa interessata	Severità di Unified Manager
FlexGroup costituenti nodi Stato tutto OK	flexgroup.constituents.inodes.status.all.ok	Volume	Informazioni
Volume Logical Space quasi pieno	monitor.vol.nearFull.inc.sav	Volume	Attenzione
Volume Logical Space Full (spazio logico volume pieno)	monitor.vol.full.inc.sav	Volume	Errore
Volume Logical Space Normal (spazio logico volume normale)	monitor.vol.one.ok.inc.sav	Volume	Informazioni
Errore di dimensionamento automatico del volume WAFL	wafl.vol.autoSize.fail	Volume	Errore
Dimensione automatica volume WAFL completata	wafl.vol.autoSize.done	Volume	Informazioni
Timeout operazione file READDIR WAFL	wafl.readdir.expired	Volume	Errore

Iscrizione a eventi EMS ONTAP

È possibile iscriversi per ricevere gli eventi del sistema di gestione degli eventi (EMS) generati dai sistemi installati con il software ONTAP. Un sottoinsieme di eventi EMS viene segnalato automaticamente a Unified Manager, ma vengono segnalati eventi EMS aggiuntivi solo se si è abbonati a questi eventi.

Cosa ti serve

Non sottoscrivere gli eventi EMS che sono già stati aggiunti automaticamente a Unified Manager, in quanto ciò potrebbe causare confusione quando si ricevono due eventi per lo stesso problema.

È possibile iscriversi a qualsiasi numero di eventi EMS. Tutti gli eventi a cui si è abbonati sono validati e solo gli eventi validati vengono applicati ai cluster monitorati in Unified Manager. Il *Catalogo eventi EMS di ONTAP 9* fornisce informazioni dettagliate su tutti i messaggi EMS per la versione specificata del software ONTAP 9. Individuare la versione appropriata del *Catalogo eventi EMS* dalla pagina della documentazione del prodotto ONTAP 9 per un elenco degli eventi applicabili.

"Libreria di prodotti ONTAP 9"

È possibile configurare gli avvisi per gli eventi EMS di ONTAP a cui si è abbonati ed è possibile creare script personalizzati da eseguire per questi eventi.

Se non si ricevono gli eventi EMS di ONTAP a cui si è abbonati, potrebbe esserci un problema con la configurazione DNS del cluster che impedisce al cluster di raggiungere il server di Unified Manager. Per risolvere questo problema, l'amministratore del cluster deve correggere la configurazione DNS del cluster, quindi riavviare Unified Manager. In questo modo, gli eventi EMS in sospeso verranno reincisi sul server Unified Manager.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Event Setup**.
2. Nella pagina Event Setup (impostazione evento), fare clic sul pulsante **Subscribe to EMS events** (Iscriviti agli eventi EMS).
3. Nella finestra di dialogo Iscriviti agli eventi EMS, immettere il nome dell'evento EMS ONTAP a cui si desidera iscriversi.

   Per visualizzare i nomi degli eventi EMS a cui è possibile iscriversi, dalla shell del cluster ONTAP, è possibile utilizzare `event route show` (Prima di ONTAP 9) o il `event catalog show` Command (ONTAP 9 o versioni successive).

   "Come configurare e ricevere avvisi dall'abbonamento eventi EMS ONTAP in Active IQ Unified Manager"

4. Fare clic su **Aggiungi**.

   L'evento EMS viene aggiunto all'elenco degli eventi EMS registrati, ma nella colonna applicabile al cluster viene visualizzato lo stato "Sconosciuto" per l'evento EMS aggiunto.

5. Fare clic su **Save and Close** (Salva e chiudi) per registrare l'abbonamento agli eventi EMS nel cluster.
6. Fare nuovamente clic su **Subscribe to EMS events** (Iscriviti agli eventi EMS).

   Lo stato "Sì" viene visualizzato nella colonna applicabile al cluster per l'evento EMS aggiunto.

   Se lo stato non è "Sì", controllare l'ortografia del nome dell'evento EMS ONTAP. Se il nome non viene inserito correttamente, rimuovere l'evento errato e aggiungerlo di nuovo.

Quando si verifica l'evento EMS ONTAP, l'evento viene visualizzato nella pagina Eventi. È possibile selezionare l'evento per visualizzare i dettagli relativi all'evento EMS nella pagina Dettagli evento. È inoltre possibile gestire l'eliminazione dell'evento o creare avvisi per l'evento.

Cosa succede quando si riceve un evento

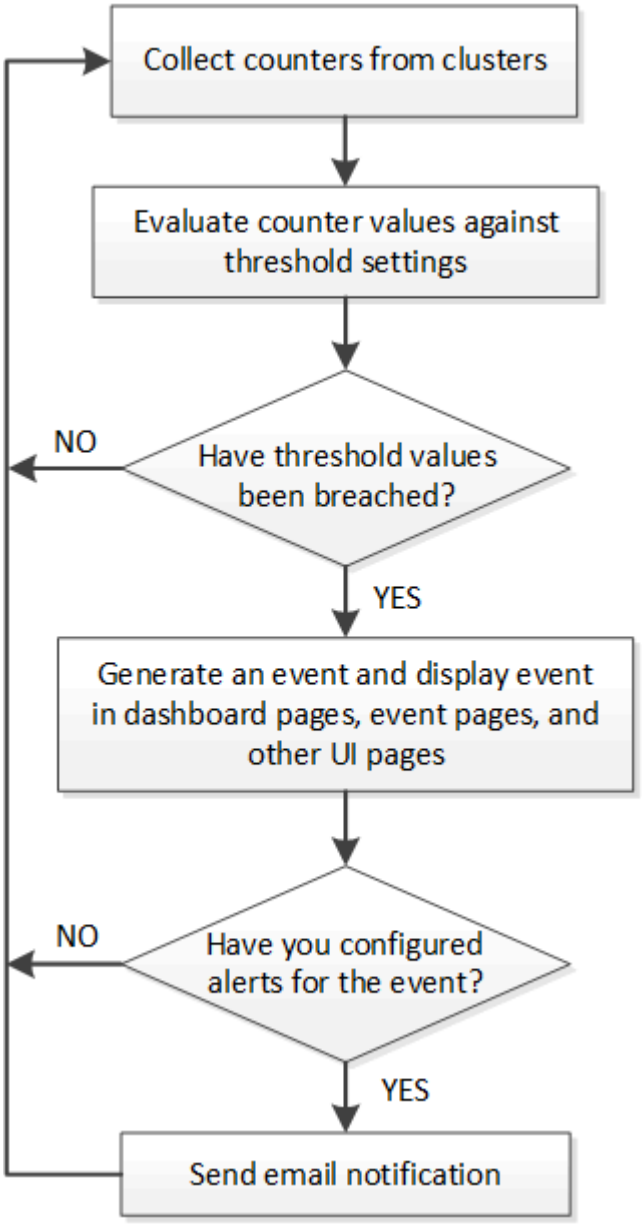
Quando Unified Manager riceve un evento, viene visualizzato nella pagina Dashboard, nella pagina dell'inventario di gestione eventi, nelle schede Summary (Riepilogo) ed Explorer (Esplora risorse) della pagina Cluster/Performance (Cluster/Performance) e nella pagina dell'inventario specifico dell'oggetto (ad esempio, la pagina Volumes/Health Inventory).

Quando Unified Manager rileva più occorrenze continue della stessa condizione di evento per lo stesso componente del cluster, considera tutte le ricorrenze come un singolo evento, non come eventi separati. La durata dell'evento viene incrementata per indicare che l'evento è ancora attivo.

A seconda della configurazione delle impostazioni nella pagina Configurazione avvisi, è possibile inviare notifiche agli altri utenti in merito a questi eventi. L'avviso causa l'avvio delle seguenti azioni:

- È possibile inviare un'e-mail relativa all'evento a tutti gli utenti di Unified Manager Administrator.
- L'evento può essere inviato ad altri destinatari email.
- È possibile inviare una trap SNMP al ricevitore della trap.
- È possibile eseguire uno script personalizzato per eseguire un'azione.

Questo flusso di lavoro è illustrato nel diagramma seguente.



Visualizzazione di eventi e dettagli dell'evento

È possibile visualizzare i dettagli di un evento attivato da Unified Manager per intraprendere azioni correttive. Ad esempio, se è presente un evento di salute Volume Offline, è possibile fare clic su tale evento per visualizzare i dettagli ed eseguire azioni correttive.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

I dettagli dell'evento includono informazioni quali l'origine dell'evento, la causa dell'evento e eventuali note correlate all'evento.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**.

   Per impostazione predefinita, la vista All Active events (tutti gli eventi attivi) visualizza gli eventi nuovi e confermati (attivi) generati nei 7 giorni precedenti con un livello di impatto dell'incidente o del rischio.

2. Se si desidera visualizzare una determinata categoria di eventi, ad esempio eventi di capacità o performance, fare clic su **Visualizza** e selezionare dal menu dei tipi di evento.
3. Fare clic sul nome dell'evento per il quale si desidera visualizzare i dettagli.

   I dettagli dell'evento vengono visualizzati nella pagina Dettagli evento.

Visualizzazione di eventi non assegnati

È possibile visualizzare gli eventi non assegnati e assegnarli a un utente in grado di risolverli.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**.

   Per impostazione predefinita, gli eventi nuovi e confermati vengono visualizzati nella pagina di inventario Gestione eventi.

2. Nel riquadro **Filters**, selezionare l'opzione di filtro **Unassigned** nell'area **Assigned to**.

Riconoscimento e risoluzione degli eventi

È necessario riconoscere un evento prima di iniziare a lavorare sul problema che ha generato l'evento, in modo da non continuare a ricevere notifiche di avviso ripetute. Dopo aver eseguito un'azione correttiva per un determinato evento, è necessario contrassegnare l'evento come risolto.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

È possibile riconoscere e risolvere più eventi contemporaneamente.

Non è possibile riconoscere gli eventi relativi alle informazioni.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**.

2. Dall'elenco degli eventi, eseguire le seguenti azioni per riconoscere gli eventi:

Se si desidera…	Eseguire questa operazione…
Riconoscere e contrassegnare un singolo evento come risolto	a. Fare clic sul nome dell'evento. b. Dalla pagina Dettagli evento, determinare la causa dell'evento. c. Fare clic su **Conferma**. d. Intraprendere un'azione correttiva appropriata. e. Fare clic su **Contrassegna come risolto**.
Riconoscere e contrassegnare più eventi come risolti	a. Determinare la causa degli eventi dalla relativa pagina Dettagli evento. b. Selezionare gli eventi. c. Fare clic su **Conferma**. d. Intraprendere le azioni correttive appropriate. e. Fare clic su **Contrassegna come risolto**.

Una volta contrassegnato come risolto, l'evento viene spostato nell'elenco degli eventi risolti.

3. **Opzionale**: Nella sezione **Note e aggiornamenti**, aggiungere una nota sulla modalità di gestione dell'evento, quindi fare clic su **Post**.

Assegnazione di eventi a utenti specifici

È possibile assegnare eventi non assegnati a se stessi o ad altri utenti, inclusi gli utenti remoti. Se necessario, è possibile riassegnare gli eventi assegnati a un altro utente. Ad esempio, quando si verificano problemi frequenti su un oggetto di storage, è possibile assegnare gli eventi per questi problemi all'utente che gestisce tale oggetto.

Cosa ti serve

- Il nome e l'ID e-mail dell'utente devono essere configurati correttamente.
- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**.
2. Nella pagina di inventario **Gestione eventi**, selezionare uno o più eventi che si desidera assegnare.
3. Assegnare l'evento scegliendo una delle seguenti opzioni:

Se si desidera assegnare l'evento a…	Quindi…
Te stesso	Fare clic su **Assegna a** > **Me**.

Se si desidera assegnare l'evento a…	Quindi…
Un altro utente	a. Fare clic su **Assegna a** > **un altro utente**. b. Nella finestra di dialogo Assegna proprietario, immettere il nome utente o selezionare un utente dall'elenco a discesa. c. Fare clic su **Assegna**. Viene inviata una notifica via email all'utente. Se non si immette un nome utente o si seleziona un utente dall'elenco a discesa e si fa clic su **Assegna**, l'evento rimane non assegnato.

Disattivazione degli eventi indesiderati

Tutti gli eventi sono attivati per impostazione predefinita. È possibile disattivare gli eventi a livello globale per impedire la generazione di notifiche per eventi non importanti nel proprio ambiente. È possibile attivare gli eventi disattivati quando si desidera riprendere la ricezione delle notifiche.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Quando si disattivano gli eventi, gli eventi precedentemente generati nel sistema vengono contrassegnati come obsoleti e gli avvisi configurati per tali eventi non vengono attivati. Quando si abilitano eventi disattivati, le notifiche per questi eventi vengono generate a partire dal ciclo di monitoraggio successivo.

Quando si disattiva un evento per un oggetto (ad esempio, l' `vol offline` E successivamente si attiva l'evento, Unified Manager non genera nuovi eventi per gli oggetti che sono andati fuori linea quando l'evento si trovava nello stato disattivato. Unified Manager genera un nuovo evento solo quando si verifica una modifica nello stato dell'oggetto dopo la riattivazione dell'evento.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Event Setup**.
2. Nella pagina **Setup evento**, disattivare o attivare gli eventi scegliendo una delle seguenti opzioni:

Se si desidera…	Quindi…
Disattivare gli eventi	a. Fare clic su **Disable** (Disattiva). b. Nella finestra di dialogo Disable Events (Disattiva eventi), selezionare la severità dell'evento. c. Nella colonna corrispondente agli eventi, selezionare gli eventi che si desidera disattivare in base alla gravità dell'evento, quindi fare clic sulla freccia destra per spostarli nella colonna Disattiva eventi. d. Fare clic su **Save and Close** (Salva e chiudi). e. Verificare che gli eventi disattivati siano visualizzati nella vista elenco della pagina impostazione eventi.
Attivare gli eventi	a. Selezionare la casella di controllo relativa all'evento o agli eventi che si desidera attivare. b. Fare clic su **Enable** (attiva).

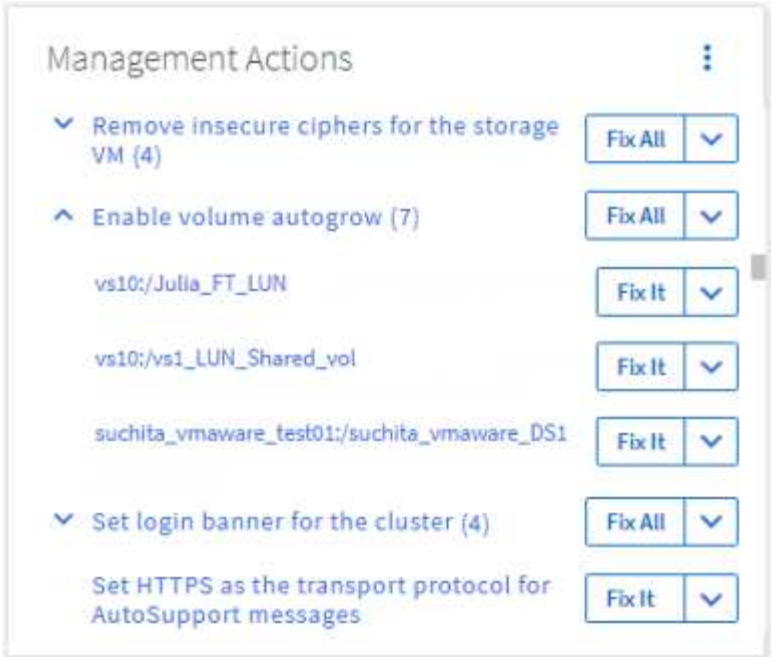
Risoluzione dei problemi con la risoluzione automatica di Unified Manager

Unified Manager è in grado di diagnosticare a fondo alcuni eventi e fornire una singola risoluzione utilizzando il pulsante **Correggi**. Se disponibili, tali risoluzioni vengono visualizzate nella dashboard, nella pagina Dettagli evento e dalla selezione analisi carico di lavoro nel menu di navigazione a sinistra.

La maggior parte degli eventi presenta una serie di possibili risoluzioni, visualizzate nella pagina Dettagli evento, in modo da poter implementare la soluzione migliore utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP. Un'azione **Correggi** è disponibile quando Unified Manager ha stabilito che esiste una singola risoluzione per risolvere il problema e che può essere risolta utilizzando un comando CLI di ONTAP.

Fasi

1. Per visualizzare gli eventi che è possibile correggere dal dashboard, fare clic su **Dashboard**.



2. Per risolvere i problemi che Unified Manager può risolvere, fare clic sul pulsante **Correggi**. Per risolvere un problema che si verifica su più oggetti, fare clic sul pulsante **Correggi tutto**.

Per informazioni sui problemi che possono essere risolti mediante la risoluzione automatica dei problemi, vedere "Quali problemi possono risolvere Unified Manager".

Attivazione e disattivazione del reporting degli eventi Active IQ

Gli eventi della piattaforma Active IQ vengono generati e visualizzati nell'interfaccia utente di Unified Manager per impostazione predefinita. Se questi eventi sono troppo "rumorosi" o non si desidera visualizzarli in Unified Manager, è possibile disattivare la generazione di tali eventi. Se si desidera riprendere la ricezione di queste notifiche, è possibile attivarle in un secondo momento.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Quando si disattiva questa funzione, Unified Manager interrompe immediatamente la ricezione degli eventi della piattaforma Active IQ.

Quando si attiva questa funzione, Unified Manager inizia a ricevere gli eventi della piattaforma Active IQ poco dopo la mezzanotte in base al fuso orario del cluster. L'ora di inizio si basa sul momento in cui Unified Manager riceve i messaggi AutoSupport da ciascun cluster.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Impostazioni funzionalità**, disattivare o attivare gli eventi della piattaforma Active IQ scegliendo una delle seguenti opzioni:

Se si desidera…	Quindi…
Disattivare gli eventi della piattaforma Active IQ	Nel pannello **Eventi portale Active IQ**, spostare il pulsante di scorrimento verso sinistra.
Attivare gli eventi della piattaforma Active IQ	Nel pannello **Eventi portale Active IQ**, spostare il pulsante di scorrimento verso destra.

Caricamento di un nuovo file di regole Active IQ

Unified Manager verifica automaticamente la presenza di un nuovo file di eventi (regole) Active IQ e scarica un nuovo file quando sono presenti regole più recenti. Tuttavia, nei siti senza accesso alla rete esterna, è necessario caricare manualmente il file di regole.

Le regole Active IQ sono anche denominate regole sicure Config Advisor (CA).

Quando si installa o si aggiorna Unified Manager a una release specifica in un sito senza connettività di rete, le regole Active IQ in bundle sono automaticamente disponibili per il caricamento. Tuttavia, si consiglia di scaricare un nuovo file di regole circa una volta al mese dal sito di supporto di NetApp per assicurarsi che vengano generati eventi aggiornati e che i sistemi storage continuino a funzionare in modo ottimale.

Cosa ti serve

- È necessario attivare il reporting degli eventi del portale Active IQ. Questa funzione è attivata per impostazione predefinita. Per ulteriori informazioni, vedere "Attivazione degli eventi del portale Active IQ".
- È necessario scaricare il file di regole dal sito del supporto NetApp.

  Il file di regole si trova in: https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

Fasi

1. Su un computer con accesso alla rete, accedere al sito del supporto NetApp e scaricare le regole correnti `.zip` file.

   Il pacchetto di regole in bundle include il repository di regole, le origini dati e un articolo della Knowledge base di NetApp.

   Nei sistemi Windows, in un sito senza connettività di rete, l'articolo della Knowledge base di NetApp non viene fornito in bundle per impostazione predefinita con il programma di installazione. È possibile scaricare il file *Secure_rules.zip* dal sito di supporto e caricarlo per visualizzare l'articolo della Knowledge base relativo a tutte le regole.

2. Trasferire il file di regole su alcuni supporti che è possibile inserire nell'area protetta e copiarlo su un sistema nell'area protetta.
3. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Event Setup**.
4. Nella pagina **impostazione evento**, fare clic sul pulsante **regole di caricamento**.
5. Nella finestra di dialogo **regole di caricamento**, selezionare le regole e selezionarle `.zip` File scaricato e fare clic su **carica**.

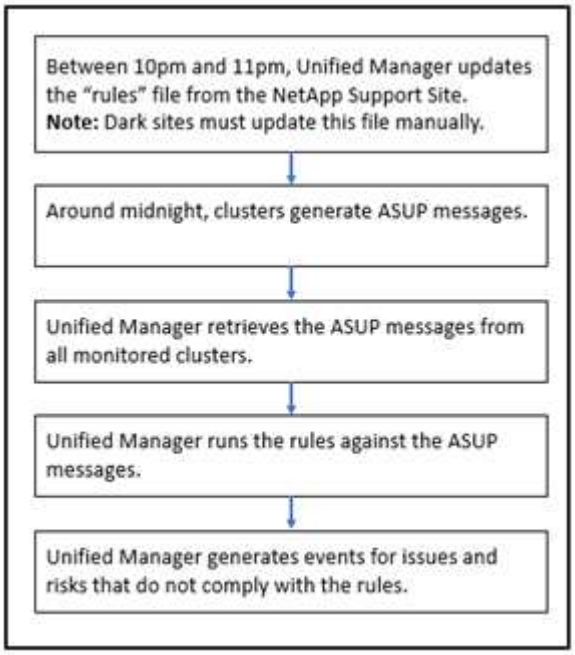
Questo processo può richiedere alcuni minuti.

Il file di regole viene decompresso sul server Unified Manager. Una volta che i cluster gestiti generano un file AutoSupport dopo la mezzanotte, Unified Manager controlla i cluster in base al file di regole e genera nuovi eventi di rischio e incidente, se necessario.

Per ulteriori informazioni, consultare l'articolo della Knowledge base (KB): "Come aggiornare manualmente le regole AIQCASecure in Active IQ Unified Manager".

Come vengono generati gli eventi della piattaforma Active IQ

Gli incidenti e i rischi della piattaforma Active IQ vengono convertiti in eventi di Unified Manager come mostrato nel diagramma seguente.

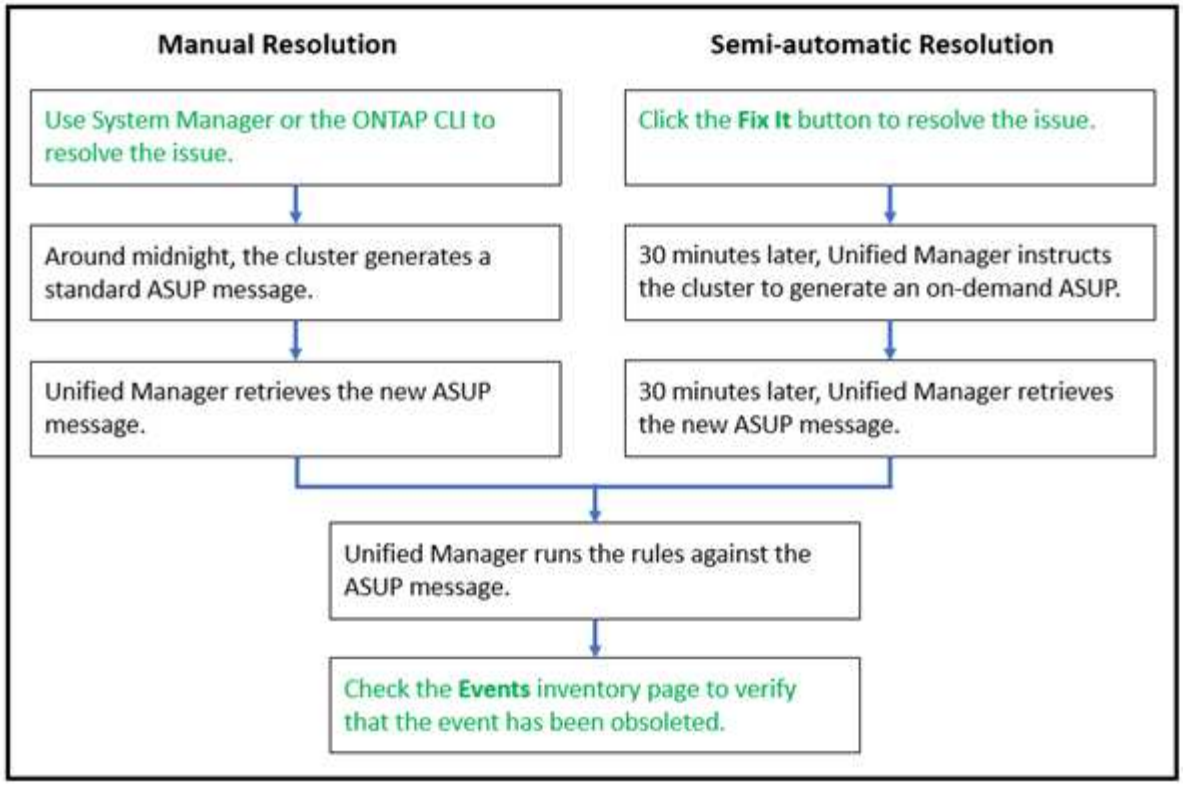


Come si può vedere, il file di regole compilato sulla piattaforma Active IQ viene mantenuto aggiornato, i messaggi AutoSupport del cluster vengono generati ogni giorno e Unified Manager aggiorna l'elenco degli eventi ogni giorno.

Risoluzione degli eventi della piattaforma Active IQ

Gli incidenti e i rischi della piattaforma Active IQ sono simili ad altri eventi di Unified Manager, in quanto possono essere assegnati ad altri utenti per la risoluzione e hanno gli stessi stati disponibili. Tuttavia, quando si risolvono questi tipi di eventi utilizzando il pulsante **Correggi**, è possibile verificare la risoluzione entro poche ore.

Il seguente diagramma mostra le azioni da eseguire (in verde) e l'azione che Unified Manager esegue (in nero) durante la risoluzione degli eventi generati dalla piattaforma Active IQ.



Quando si esegue una risoluzione manuale, è necessario accedere a Gestione sistema o all'interfaccia della riga di comando di ONTAP per risolvere il problema. Sarà possibile verificare il problema solo dopo che il cluster avrà generato un nuovo messaggio AutoSupport a mezzanotte.

Quando si esegue una risoluzione semi-automatica utilizzando il pulsante **Fix it**, è possibile verificare che la correzione sia stata eseguita correttamente in poche ore.

Configurazione delle impostazioni di conservazione degli eventi

È possibile specificare il numero di mesi in cui un evento viene conservato nel server di Unified Manager prima che venga eliminato automaticamente.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

La conservazione di eventi per più di 6 mesi potrebbe influire sulle prestazioni del server e non è consigliabile.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **conservazione dei dati**.
2. Nella pagina **Data Retention**, selezionare il dispositivo di scorrimento nell'area Event Retention (conservazione eventi) e spostarlo sul numero di mesi in cui gli eventi devono essere conservati, quindi fare clic su **Save** (Salva).

Cos'è una finestra di manutenzione di Unified Manager

È possibile definire una finestra di manutenzione di Unified Manager per eliminare eventi e avvisi per un intervallo di tempo specifico quando è stata pianificata la manutenzione del cluster e non si desidera ricevere un flusso di notifiche indesiderate.

All'avvio della finestra di manutenzione, viene visualizzato un evento "Object Maintenance Window Started" (finestra di manutenzione oggetto avviata) nella pagina dell'inventario di gestione eventi. Questo evento viene reso obsoleto automaticamente al termine della finestra di manutenzione.

Durante una finestra di manutenzione, gli eventi correlati a tutti gli oggetti del cluster vengono ancora generati, ma non vengono visualizzati in nessuna delle pagine dell'interfaccia utente e non vengono inviati avvisi o altri tipi di notifica per questi eventi. Tuttavia, è possibile visualizzare gli eventi generati per tutti gli oggetti di storage durante una finestra di manutenzione selezionando una delle opzioni di visualizzazione nella pagina di inventario di Event Management.

È possibile pianificare l'avvio di una finestra di manutenzione in futuro, modificare l'ora di inizio e di fine di una finestra di manutenzione programmata ed annullare una finestra di manutenzione programmata.

Pianificazione di una finestra di manutenzione per disattivare le notifiche degli eventi del cluster

Se si dispone di un downtime pianificato per un cluster, ad esempio per aggiornare il cluster o per spostare uno dei nodi, è possibile eliminare gli eventi e gli avvisi che normalmente verrebbero generati durante tale periodo di tempo, programmando una finestra di manutenzione di Unified Manager.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Durante una finestra di manutenzione, gli eventi correlati a tutti gli oggetti del cluster vengono ancora generati, ma non vengono visualizzati nella pagina degli eventi e non vengono inviati avvisi o altri tipi di notifica per tali eventi.

L'ora immessa per la finestra di manutenzione si basa sull'ora del server Unified Manager.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Cluster Setup**.
2. Nella colonna **modalità di manutenzione** del cluster, selezionare il pulsante a scorrimento e spostarlo verso destra.

   Viene visualizzata la finestra del calendario.

3. Selezionare la data e l'ora di inizio e di fine della finestra di manutenzione e fare clic su **Apply** (Applica).

   Accanto al pulsante di scorrimento viene visualizzato il messaggio "Scheduled" (pianificato).

Una volta raggiunta l'ora di inizio, il cluster passa alla modalità di manutenzione e viene generato un evento "Object Maintenance Window Started" (finestra di manutenzione oggetto avviata).

Modifica o annullamento di una finestra di manutenzione pianificata

Se è stata configurata una finestra di manutenzione di Unified Manager in modo che si verifichi in futuro, è possibile modificare l'ora di inizio e di fine o annullare la finestra di manutenzione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

L'annullamento di una finestra di manutenzione attualmente in esecuzione è utile se la manutenzione del cluster è stata completata prima dell'ora di fine della finestra di manutenzione pianificata e si desidera iniziare nuovamente a ricevere eventi e avvisi dal cluster.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Cluster Setup**.
2. Nella colonna **Maintenance Mode** del cluster:

Se si desidera…	Eseguire questo passaggio…
Modificare l'intervallo di tempo per una finestra di manutenzione pianificata	a. Fare clic sul testo "Scheduled" (pianificato) accanto al pulsante del dispositivo di scorrimento. b. Modificare la data e l'ora di inizio e/o di fine e fare clic su **Apply** (Applica).
Estendere la lunghezza di una finestra di manutenzione attiva	a. Fare clic sul testo "Active" (attivo) accanto al pulsante del dispositivo di scorrimento. b. Modificare la data e l'ora di fine e fare clic su **Apply** (Applica).
Consente di annullare una finestra di manutenzione programmata	Selezionare il pulsante a scorrimento e spostarlo verso sinistra.
Consente di annullare una finestra di manutenzione attiva	Selezionare il pulsante a scorrimento e spostarlo verso sinistra.

Visualizzazione degli eventi verificatisi durante una finestra di manutenzione

Se necessario, è possibile visualizzare gli eventi generati per tutti gli oggetti di storage durante una finestra di manutenzione di Unified Manager. La maggior parte degli eventi viene visualizzata nello stato obsoleto una volta completata la finestra di manutenzione e dopo aver eseguito il backup e l'esecuzione di tutte le risorse di sistema.

Cosa ti serve

Almeno una finestra di manutenzione deve essere completata prima che siano disponibili eventi.

Per impostazione predefinita, gli eventi che si sono verificati durante una finestra di manutenzione non vengono visualizzati nella pagina dell'inventario di gestione degli eventi.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Eventi**.

   Per impostazione predefinita, tutti gli eventi attivi (nuovi e riconosciuti) vengono visualizzati nella pagina inventario gestione eventi.

2. Dal riquadro di visualizzazione, selezionare l'opzione **tutti gli eventi generati durante la manutenzione**.

   Viene visualizzato l'elenco degli eventi che sono stati provati durante gli ultimi 7 giorni da tutte le sessioni della finestra di manutenzione e da tutti i cluster.

3. Se sono state visualizzate più finestre di manutenzione per un singolo cluster, fare clic sull'icona del calendario **ora di attivazione** e selezionare il periodo di tempo per gli eventi della finestra di manutenzione che si desidera visualizzare.

Gestione degli eventi delle risorse del sistema host

Unified Manager include un servizio che monitora i problemi relativi alle risorse sul sistema host su cui è installato Unified Manager. Problemi come la mancanza di spazio su disco disponibile o la mancanza di memoria nel sistema host possono attivare eventi della stazione di gestione visualizzati come messaggi banner nella parte superiore dell'interfaccia utente.

Gli eventi delle stazioni di gestione indicano un problema con il sistema host su cui è installato Unified Manager. Alcuni esempi di problemi relativi alle stazioni di gestione includono lo spazio su disco insufficiente nel sistema host, Unified Manager non dispone di un normale ciclo di raccolta dei dati e il mancato completamento o il completamento ritardato dell'analisi delle statistiche a causa dell'avvio del successivo polling della raccolta.

A differenza di tutti gli altri messaggi di evento di Unified Manager, questi particolari avvisi e eventi critici della stazione di gestione vengono visualizzati in messaggi banner.

Fase

1. Per visualizzare le informazioni sugli eventi della stazione di gestione, eseguire le seguenti operazioni:

Se si desidera…	Eseguire questa operazione…
Visualizza i dettagli dell'evento	Fare clic sul banner dell'evento per visualizzare la pagina Dettagli evento che contiene le soluzioni suggerite per il problema.
Visualizzare tutti gli eventi delle stazioni di gestione	a. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**. b. Nel riquadro filtri della pagina inventario gestione eventi, fare clic sulla casella Stazione di gestione nell'elenco tipo di origine.

Ulteriori informazioni sugli eventi

La comprensione dei concetti relativi agli eventi consente di gestire i cluster e gli oggetti del cluster in modo efficiente e di definire gli avvisi in modo appropriato.

Definizioni dello stato dell'evento

Lo stato di un evento aiuta a identificare se è necessaria un'azione correttiva appropriata. Un evento può essere nuovo, confermato, risolto o obsoleto. Si noti che sia gli eventi

nuovi che quelli confermati sono considerati eventi attivi.

Gli stati dell'evento sono i seguenti:

- **Nuovo**

  Lo stato di un nuovo evento.

- **Riconosciuto**

  Lo stato di un evento confermato.

- **Risolto**

  Lo stato di un evento quando viene contrassegnato come risolto.

- **Obsoleto**

  Lo stato di un evento quando viene corretto automaticamente o quando la causa dell'evento non è più valida.

  Non è possibile riconoscere o risolvere un evento obsoleto.

Esempio di stati diversi di un evento

I seguenti esempi illustrano le modifiche manuali e automatiche dello stato degli eventi.

Quando viene attivato l'evento Cluster Not Reachable (Cluster non raggiungibile), lo stato dell'evento è New (nuovo). Quando si riconosce l'evento, lo stato dell'evento diventa confermato. Una volta eseguita un'azione correttiva appropriata, è necessario contrassegnare l'evento come risolto. Lo stato dell'evento diventa Resolved (risolto).

Se l'evento Cluster Not Reachable (Cluster non raggiungibile) viene generato a causa di un'interruzione dell'alimentazione, quando viene ripristinata l'alimentazione, il cluster inizia a funzionare senza alcun intervento dell'amministratore. Pertanto, l'evento Cluster Not Reachable non è più valido e lo stato dell'evento diventa obsoleto nel ciclo di monitoraggio successivo.

Unified Manager invia un avviso quando un evento si trova nello stato obsoleto o risolto. L'oggetto dell'e-mail e il contenuto dell'e-mail di un avviso forniscono informazioni sullo stato dell'evento. Un trap SNMP include anche informazioni sullo stato dell'evento.

Descrizione dei tipi di severità degli eventi

Ogni evento è associato a un tipo di severità per aiutarti a definire la priorità degli eventi che richiedono un'azione correttiva immediata.

- **Critico**

  Si è verificato un problema che potrebbe causare un'interruzione del servizio se non viene intrapresa immediatamente un'azione correttiva.

  Gli eventi critici relativi alle performance vengono inviati solo da soglie definite dall'utente.

- **Errore**

L'origine dell'evento continua a essere in esecuzione; tuttavia, è necessaria un'azione correttiva per evitare interruzioni del servizio.

- **Attenzione**

  L'origine dell'evento ha riscontrato un evento di cui si dovrebbe essere a conoscenza oppure un contatore delle prestazioni per un oggetto cluster non rientra nell'intervallo normale e deve essere monitorato per assicurarsi che non raggiunga la severità critica. Gli eventi di questo livello di gravità non causano interruzioni del servizio e potrebbero non essere necessarie azioni correttive immediate.

  Gli eventi di avviso relativi alle performance vengono inviati da soglie definite dall'utente, definite dal sistema o dinamiche.

- **Informazioni**

  L'evento si verifica quando viene rilevato un nuovo oggetto o quando viene eseguita un'azione dell'utente. Ad esempio, quando un oggetto di storage viene cancellato o quando vengono apportate modifiche alla configurazione, viene generato l'evento con tipo di severità informazioni.

  Gli eventi informativi vengono inviati direttamente da ONTAP quando rileva una modifica della configurazione.

Descrizione dei livelli di impatto degli eventi

Ogni evento è associato a un livello di impatto (incidente, rischio, evento o aggiornamento) per aiutarti a definire la priorità degli eventi che richiedono un'azione correttiva immediata.

- **Incidente**

  Un incidente è un insieme di eventi che possono causare l'interruzione della fornitura dei dati al client da parte di un cluster e l'esaurimento dello spazio per l'archiviazione dei dati. Gli eventi con un livello di impatto dell'incidente sono i più gravi. È necessario intraprendere un'azione correttiva immediata per evitare interruzioni del servizio.

- **Rischio**

  Un rischio è costituito da una serie di eventi che possono potenzialmente causare l'interruzione della fornitura dei dati al client da parte di un cluster e l'esaurimento dello spazio per l'archiviazione dei dati. Gli eventi con un livello di rischio di impatto possono causare interruzioni del servizio. Potrebbe essere necessaria un'azione correttiva.

- **Evento**

  Un evento è un cambiamento di stato o stato degli oggetti di storage e dei relativi attributi. Gli eventi con un livello di impatto dell'evento sono informativi e non richiedono azioni correttive.

- **Upgrade**

  Gli eventi di upgrade sono un tipo specifico di evento segnalato dalla piattaforma Active IQ. Questi eventi identificano i problemi in cui la risoluzione richiede l'aggiornamento del software ONTAP, del firmware del nodo o del software del sistema operativo (per gli avvisi di sicurezza). Potrebbe essere necessario eseguire un'azione correttiva immediata per alcuni di questi problemi, mentre altri potrebbero essere in grado di attendere la successiva manutenzione pianificata.

Descrizione delle aree di impatto degli eventi

Gli eventi sono suddivisi in sei aree di impatto (disponibilità, capacità, configurazione, performance, protezione, e sicurezza) per consentirti di concentrarti sui tipi di eventi di cui sei responsabile.

- **Disponibilità**

  Gli eventi di disponibilità avvisano l'utente se un oggetto di storage passa fuori linea, se un servizio di protocollo non funziona, se si verifica un problema di failover dello storage o se si verifica un problema con l'hardware.

- **Capacità**

  Gli eventi di capacità avvisano l'utente se aggregati, volumi, LUN o spazi dei nomi si stanno avvicinando o hanno raggiunto una soglia di dimensione o se il tasso di crescita è insolito per il proprio ambiente.

- **Configurazione**

  Gli eventi di configurazione informano dell'individuazione, dell'eliminazione, dell'aggiunta, della rimozione o della ridenominazione degli oggetti di storage. Gli eventi di configurazione hanno un livello di impatto dell'evento e un tipo di gravità delle informazioni.

- **Prestazioni**

  Gli eventi relativi alle performance avvisano l'utente di condizioni di risorse, configurazione o attività sul cluster che potrebbero influire negativamente sulla velocità di input o recupero dello storage dei dati sugli oggetti di storage monitorati.

- **Protezione**

  Gli eventi di protezione avvisano l'utente di incidenti o rischi che coinvolgono relazioni SnapMirror, problemi con la capacità di destinazione, problemi con le relazioni SnapVault o problemi con i processi di protezione. Tutti gli oggetti ONTAP (in particolare aggregati, volumi e SVM) che ospitano volumi secondari e relazioni di protezione sono classificati nell'area di impatto della protezione.

- **Sicurezza**

  Gli eventi di sicurezza ti avvisano della protezione dei cluster ONTAP, delle storage virtual machine (SVM) e dei volumi in base ai parametri definiti in "Guida al rafforzamento della sicurezza di NetApp per ONTAP 9".

  Inoltre, quest'area include gli eventi di upgrade riportati dalla piattaforma Active IQ.

Come viene calcolato lo stato dell'oggetto

Lo stato dell'oggetto è determinato dall'evento più grave che attualmente contiene uno stato nuovo o riconosciuto. Ad esempio, se lo stato di un oggetto è Error, uno degli eventi dell'oggetto ha un tipo di severità Error. Una volta intrapresa un'azione correttiva, lo stato dell'evento passa a Resolved (risolto).

Dettagli del grafico degli eventi delle performance dinamiche

Per gli eventi di performance dinamiche, la sezione System Diagnosis della pagina Event Details elenca i carichi di lavoro principali con la latenza o l'utilizzo più elevati del componente del cluster in conflitto.

Le statistiche delle performance si basano sull'ora in cui l'evento è stato rilevato fino all'ultima volta in cui è stato analizzato l'evento. I grafici visualizzano anche le statistiche cronologiche delle performance per il componente del cluster in conflitto.

Ad esempio, è possibile identificare i carichi di lavoro con un elevato utilizzo di un componente per determinare quale carico di lavoro spostare in un componente meno utilizzato. Lo spostamento del carico di lavoro ridurrebbe la quantità di lavoro sul componente corrente, possibilmente portando il componente fuori dai conflitti. Nella parte superiore di questa sezione sono riportati l'intervallo di tempo e data in cui è stato rilevato un evento e l'ultima analisi. Per gli eventi attivi (nuovi o riconosciuti), viene aggiornata l'ultima ora analizzata.

I grafici di latenza e attività visualizzano i nomi dei carichi di lavoro principali quando si sposta il cursore sul grafico. Facendo clic sul menu tipo di carico di lavoro a destra del grafico, è possibile ordinare i carichi di lavoro in base al loro ruolo nell'evento, tra cui *squali*, *bulli* o *vittime*, e visualizzare i dettagli relativi alla latenza e al loro utilizzo sul componente del cluster in conflitto. È possibile confrontare il valore effettivo con il valore previsto per vedere quando il carico di lavoro non rientra nell'intervallo di latenza o utilizzo previsto. Per ulteriori informazioni, vedere "Tipi di workload monitorati da Unified Manager".

> Quando si effettua l'ordinamento in base alla deviazione di picco nella latenza, i carichi di lavoro definiti dal sistema non vengono visualizzati nella tabella, perché la latenza si applica solo ai carichi di lavoro definiti dall'utente. I carichi di lavoro con valori di latenza molto bassi non vengono visualizzati nella tabella.

Per ulteriori informazioni sulle soglie di performance dinamiche, vedere "Analisi degli eventi dalle soglie di performance dinamiche".

Per informazioni su come Unified Manager classifica i carichi di lavoro e determina l'ordinamento, vedere "In che modo Unified Manager determina l'impatto delle performance di un evento".

I dati nei grafici mostrano 24 ore di statistiche delle performance prima dell'ultima analisi dell'evento. I valori effettivi e quelli previsti per ciascun carico di lavoro si basano sul tempo in cui il carico di lavoro è stato coinvolto nell'evento. Ad esempio, un carico di lavoro potrebbe essere coinvolto in un evento dopo il rilevamento dell'evento, pertanto le relative statistiche sulle prestazioni potrebbero non corrispondere ai valori al momento del rilevamento dell'evento. Per impostazione predefinita, i carichi di lavoro vengono ordinati in base alla deviazione di picco (massima) nella latenza.

> Poiché Unified Manager conserva un massimo di 30 giorni di dati storici relativi alle performance e agli eventi di 5 minuti, se l'evento ha più di 30 giorni, non vengono visualizzati dati relativi alle performance.

- **Colonna ordinamento carico di lavoro**
  - **Grafico di latenza**

    Visualizza l'impatto dell'evento sulla latenza del carico di lavoro durante l'ultima analisi.
  - **Colonna utilizzo componente**

    Visualizza i dettagli sull'utilizzo del carico di lavoro del componente del cluster in conflitto. Nei grafici,

l'utilizzo effettivo è una linea blu. Una barra rossa evidenzia la durata dell'evento, dal tempo di rilevamento all'ultimo tempo analizzato. Per ulteriori informazioni, vedere "Valori di misurazione delle performance del carico di lavoro".

Per il componente di rete, poiché le statistiche delle performance di rete provengono dall'attività al di fuori del cluster, questa colonna non viene visualizzata.

- **Utilizzo dei componenti**

  Visualizza la cronologia dell'utilizzo, in percentuale, per l'elaborazione di rete, l'elaborazione dei dati e i componenti aggregati o la cronologia dell'attività, in percentuale, per il componente del gruppo di criteri QoS. Il grafico non viene visualizzato per i componenti di rete o di interconnessione. È possibile puntare alle statistiche per visualizzare le statistiche di utilizzo in un momento specifico.

- **Total Write MB/s History**

  Solo per il componente risorse MetroCluster, mostra il throughput di scrittura totale, in megabyte al secondo (Mbps), per tutti i carichi di lavoro dei volumi sottoposti a mirroring nel cluster partner in una configurazione MetroCluster.

- **Cronologia eventi**

  Visualizza linee ombreggiate in rosso per indicare gli eventi storici per il componente in conflitto. Per gli eventi obsoleti, il grafico visualizza gli eventi che si sono verificati prima del rilevamento e dopo la risoluzione dell'evento selezionato.

Modifiche alla configurazione rilevate da Unified Manager

Unified Manager monitora i cluster per verificare la presenza di modifiche alla configurazione per determinare se una modifica potrebbe aver causato o contribuito a un evento di performance. Le pagine Performance Explorer (Esplora prestazioni) visualizzano un'icona di modifica dell'evento ( ) per indicare la data e l'ora in cui è stata rilevata la modifica.

È possibile esaminare i grafici delle prestazioni nelle pagine Performance Explorer e nella pagina workload Analysis per verificare se l'evento di modifica ha influito sulle prestazioni dell'oggetto cluster selezionato. Se la modifica è stata rilevata in corrispondenza o intorno a un evento di performance, la modifica potrebbe aver contribuito al problema, causando l'attivazione dell'avviso di evento.

Unified Manager è in grado di rilevare i seguenti eventi di cambiamento, classificati come eventi informativi:

- Un volume si sposta tra gli aggregati.

  Unified Manager è in grado di rilevare quando lo spostamento è in corso, completato o non riuscito. Se Unified Manager è inattivo durante lo spostamento di un volume, durante il backup rileva lo spostamento del volume e visualizza un evento di modifica.

- Il limite di throughput (MB/s o IOPS) di un gruppo di policy QoS che contiene una o più modifiche dei carichi di lavoro monitorati.

  La modifica del limite di un gruppo di criteri può causare picchi intermittenti della latenza (tempo di risposta), che potrebbero anche attivare eventi per il gruppo di criteri. La latenza ritorna gradualmente alla normalità e gli eventi causati dai picchi diventano obsoleti.

- Un nodo in una coppia ha assume il controllo o restituisce lo storage del nodo partner.

  Unified Manager è in grado di rilevare quando l'operazione di Takeover, Takeover parziale o giveback è stata completata. Se il takeover è causato da un nodo in Panicked, Unified Manager non rileva l'evento.

- Un'operazione di aggiornamento o revert ONTAP è stata completata correttamente.

  Vengono visualizzate la versione precedente e la nuova.

Elenco degli eventi e dei tipi di severità

È possibile utilizzare l'elenco degli eventi per acquisire una maggiore familiarità con le categorie di eventi, i nomi degli eventi e il tipo di severità di ciascun evento visualizzato in Unified Manager. Gli eventi sono elencati in ordine alfabetico per categoria di oggetti.

Aggregare gli eventi

Gli eventi aggregati forniscono informazioni sullo stato degli aggregati, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Aggregato offline (ocumEvtAggregateStateOffline)	Incidente	Aggregato	Critico
Aggregato non riuscito (ocumEvtAggregateStateFailed)	Incidente	Aggregato	Critico
Aggregato con restrizioni (ocumEvtAggregateStateRestricted)	Rischio	Aggregato	Attenzione
Ricostruzione aggregata(ocumEvtAggregateRaidStateReconstructing)	Rischio	Aggregato	Attenzione
Aggregato degradato(ocumEvtAggregateRaidStateDegraded)	Rischio	Aggregato	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Livello cloud parzialmente raggiungibile (ocumEventCloudTierPartiallyReachable)	Rischio	Aggregato	Attenzione
Livello cloud non raggiungibile (ocumEventCloudTierUnreachable)	Rischio	Aggregato	Errore
Accesso al livello cloud negato per il trasferimento degli aggregati *(arlNetraCaCheckFailed)	Rischio	Aggregato	Errore
Accesso al livello cloud negato per il trasferimento dell'aggregato durante il failover dello storage *(gbNetraCaCheckFailed)	Rischio	Aggregato	Errore
Aggregato MetroCluster lasciato dietro(ocumEvtMetroClusterAggregateLeftBehind)	Rischio	Aggregato	Errore
Mirroring aggregato MetroCluster degradato(ocumEvtMetroClusterAggregateMirrordegradato)	Rischio	Aggregato	Errore

Area di impatto: Capacità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Spazio aggregato quasi pieno (ocumEvtAggregateNearlyFull)	Rischio	Aggregato	Attenzione
Spazio aggregato pieno (ocumEvtAggregateFull)	Rischio	Aggregato	Errore

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Aggregate Days until Full (ocumEvtAggregateDaysUntilFullSoon)	Rischio	Aggregato	Errore
Aggregato con overcommit(ocumEvtAggregateOvercommit)	Rischio	Aggregato	Errore
Aggregare quasi in eccesso(ocumEvtAggregateAlmostOvercommit)	Rischio	Aggregato	Attenzione
Riserva snapshot aggregata completa (ocumEvtAggregateSnapReserveFull)	Rischio	Aggregato	Attenzione
Tasso di crescita aggregato anomalo(ocumEvtAggregateGrowthRateAbnormal)	Rischio	Aggregato	Attenzione

Area di impatto: Configurazione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Aggregato rilevato (non applicabile)	Evento	Aggregato	Informazioni
Aggregato rinominato (non applicabile)	Evento	Aggregato	Informazioni
Aggregato cancellato (non applicabile)	Evento	Nodo	Informazioni

Area di impatto: Performance

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Violazione della soglia critica degli IOPS aggregati (ocumAggregateIopsIncident)	Incidente	Aggregato	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Soglia di avviso IOPS aggregato violata (ocumAggregateIopsWarning)	Rischio	Aggregato	Attenzione
Violazione della soglia critica aggregata MB/s (ocumAggregateMbpsIncident)	Incidente	Aggregato	Critico
Soglia di avviso MB/s aggregata violata (ocumAggregateMbpsWarning)	Rischio	Aggregato	Attenzione
Violazione della soglia critica di latenza aggregata (ocumAggregateLatencyIncident)	Incidente	Aggregato	Critico
Violazione della soglia di avviso di latenza aggregata (ocumAggregateLatencyWarning)	Rischio	Aggregato	Attenzione
Violazione della soglia critica utilizzata dalla capacità di performance aggregata (ocumAggregatePerfCapacityUsedIncident)	Incidente	Aggregato	Critico
Soglia di avviso utilizzata per la capacità di performance aggregata non rispettata (ocumAggregatePerfCapacityUsedWarning)	Rischio	Aggregato	Attenzione
Violazione della soglia critica di utilizzo dell'aggregato (ocumAggregateUtilisationIncident)	Incidente	Aggregato	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Soglia di avviso utilizzo aggregato violata (ocumAggregateUtilizationWarning)	Rischio	Aggregato	Attenzione
Violazione della soglia di utilizzo eccessivo dei dischi aggregati (ocumAggregateDisksOverUtilizedWarning)	Rischio	Aggregato	Attenzione
Violazione della soglia dinamica aggregata (ocumAggregateDynamicEventWarning)	Rischio	Aggregato	Attenzione

Eventi del cluster

Gli eventi del cluster forniscono informazioni sullo stato dei cluster, che consentono di monitorare i cluster alla ricerca di potenziali problemi. Gli eventi sono raggruppati per area di impatto e includono nome dell'evento, nome della trap, livello di impatto, tipo di origine e severità.

Area di impatto: Disponibilità

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Il cluster non dispone di dischi di riserva (ocumEvtDisksNoSpare)	Rischio	Cluster	Attenzione
Cluster non raggiungibile (ocumEvtClusterUnreachable)	Rischio	Cluster	Errore
Monitoraggio del cluster non riuscito (ocumEvtClusterMonitoringFailed)	Rischio	Cluster	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Limiti di capacità della licenza Cluster FabricPool violati (ocumEvtExternalCapacityTierSpaceFull)	Rischio	Cluster	Attenzione
Periodo di valutazione NVMe-of iniziato *(nvmfGracePeriodStart)	Rischio	Cluster	Attenzione
Periodo di prova NVMe-of Active *(nvmfGracePeriodActive)	Rischio	Cluster	Attenzione
Periodo di prova NVMe scaduto *(nvmfGracePeriodExpired)	Rischio	Cluster	Attenzione
Finestra di manutenzione oggetti avviata (objectMaintenanceWindowStarted)	Evento	Cluster	Critico
Finestra di manutenzione oggetti terminata(objectMaintenanceWindowEnded)	Evento	Cluster	Informazioni
Dischi di ricambio MetroCluster rimasti indietro (ocumEvtSpareDiskLeftBehind)	Rischio	Cluster	Errore
Switchover automatico non pianificato MetroCluster disattivato (ocumEvtMccAutomaticUnplannedSwitchOverDisabilitato)	Rischio	Cluster	Attenzione
Password utente cluster modificata *(cluster.passwd.changed)	Evento	Cluster	Informazioni

Area di impatto: Capacità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Soglia di squilibrio della capacità del cluster violata (ocumConformanceNodeImbalanceWarning)	Rischio	Cluster	Attenzione
Pianificazione del livello di cloud cluster (clusterCloudTierPlanningWarning)	Rischio	Cluster	Attenzione
Risincronizzazione replica mirror FabricPool completata * (waferCaResyncComplete)	Evento	Cluster	Attenzione
Spazio FabricPool quasi pieno *(fabricpoolNearlyFull)	Rischio	Cluster	Errore

Area di impatto: Configurazione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Nodo aggiunto (non applicabile)	Evento	Cluster	Informazioni
Nodo rimosso (non applicabile)	Evento	Cluster	Informazioni
Cluster rimosso (non applicabile)	Evento	Cluster	Informazioni
Aggiunta cluster non riuscita (non applicabile)	Evento	Cluster	Errore
Nome cluster modificato (non applicabile)	Evento	Cluster	Informazioni
EMS di emergenza ricevuto (non applicabile)	Evento	Cluster	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
EMS critico ricevuto (non applicabile)	Evento	Cluster	Critico
Avviso EMS ricevuto (non applicabile)	Evento	Cluster	Errore
Errore EMS ricevuto (non applicabile)	Evento	Cluster	Attenzione
Avviso EMS ricevuto (non applicabile)	Evento	Cluster	Attenzione
EMS di debug ricevuto (non applicabile)	Evento	Cluster	Attenzione
Avviso EMS ricevuto (non applicabile)	Evento	Cluster	Attenzione
EMS informativo ricevuto (non applicabile)	Evento	Cluster	Attenzione

Gli eventi EMS di ONTAP sono suddivisi in tre livelli di severità degli eventi di Unified Manager.

Livello di severità degli eventi di Unified Manager	Livello di severità dell'evento EMS ONTAP
Critico	Emergenza Critico
Errore	Avviso
Attenzione	Errore Attenzione Debug Avviso Informativo

Area di impatto: Performance

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Soglia di squilibrio del carico del cluster violata()	Rischio	Cluster	Attenzione
Violazione della soglia critica IOPS del cluster (ocumClusterIopsIncident)	Incidente	Cluster	Critico
Violazione della soglia di avviso IOPS del cluster (ocumClusterIopsWarning)	Rischio	Cluster	Attenzione
Violazione della soglia critica di MB/s del cluster (ocumClusterMbpsIncident)	Incidente	Cluster	Critico
Soglia di avviso cluster MB/s violata (ocumClusterMbpsWarning)	Rischio	Cluster	Attenzione
Violazione della soglia dinamica del cluster (ocumClusterDynamicEventWarning)	Rischio	Cluster	Attenzione

Area di impatto: Sicurezza

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Trasporto HTTPS AutoSupport disattivato (ocumClusterASUPHtpsConfiguredDisabilitato)	Rischio	Cluster	Attenzione
Inoltro log non crittografato (ocumClusterAuditLogUnEncrypted)	Rischio	Cluster	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Default Local Admin User Enabled (utente amministratore locale predefinito abilitato) (ocumClusterDefaultAdminEnabled)	Rischio	Cluster	Attenzione
FIPS Mode Disabled (modalità FIPS disattivata) (ocumClusterFipsDisabled)	Rischio	Cluster	Attenzione
Banner di accesso disattivato (ocumClusterLoginBannerDisabilitato)	Rischio	Cluster	Attenzione
Banner di accesso modificato(ocumClusterLoginBannerChanged)	Rischio	Cluster	Attenzione
Destinazioni di inoltro log modificate(ocumLogForwardDestinationsChanged)	Rischio	Cluster	Attenzione
Nomi server NTP modificati (ocumNtpServerNamesChanged)	Rischio	Cluster	Attenzione
Numero di server NTP basso (securityConfigNTPServerCountLowRisk)	Rischio	Cluster	Attenzione
Comunicazione peer cluster non crittografata (ocumClusterPeerEncryptionDisabilitato)	Rischio	Cluster	Attenzione
SSH utilizza crittografia non sicura(ocumClusterSSHInSecure)	Rischio	Cluster	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Protocollo Telnet attivato (ocumClusterTelnetEnabled)	Rischio	Cluster	Attenzione
Le password di alcuni account utente ONTAP utilizzano la funzione hash MD5 meno sicura (ocumClusterMD5PasswordHashUsed)	Rischio	Cluster	Attenzione
Il cluster utilizza un certificato autofirmato (ocumClusterSelfSignedCertificate)	Rischio	Cluster	Attenzione
Cluster Remote Shell abilitato (ocumClusterRshDisabilitato)	Rischio	Cluster	Attenzione
Il certificato del cluster sta per scadere(ocumEvtClusterCertificateAboutToExpire)	Rischio	Cluster	Attenzione
Certificato cluster scaduto(ocumEvtClusterCertificateExpired)	Rischio	Cluster	Errore

Eventi dei dischi

Gli eventi dei dischi forniscono informazioni sullo stato dei dischi, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Dischi flash - blocchi di riserva quasi consumati (ocumEvtClusterFlashDiskFewerSpareBlockError)	Rischio	Cluster	Errore

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Dischi flash - Nessun blocco di ricambio (ocumEvtClusterFlashDiskNoSpareBlockCritical)	Incidente	Cluster	Critico
Alcuni dischi non assegnati (ocumEvtClusterUnassignedDisksSome)	Rischio	Cluster	Attenzione
Alcuni dischi non riusciti (ocumEvtDisksSomeFailed)	Incidente	Cluster	Critico

Eventi di enclosure

Gli eventi enclosure forniscono informazioni sullo stato degli shelf enclosure di dischi nel data center, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Ventole shelf disco non riuscite (ocumEvtShelfFanFailed)	Incidente	Shelf di storage	Critico
Alimentatori shelf di dischi non riusciti (ocumEvtShelfPowerSupplyFailed)	Incidente	Shelf di storage	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Percorso multiplo shelf disco non configurato (ocumDiskShelfConnectivityNotInMultiPath) Questo evento non si applica a: • Cluster in una configurazione MetroCluster • Le seguenti piattaforme: FAS2554, FAS2552, FAS2520 e FAS2240	Rischio	Nodo	Attenzione
Errore percorso shelf disco (ocumDiskShelfConnectivityPathFailure)	Rischio	Shelf. Storage	Attenzione

Area di impatto: Configurazione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Shelf di dischi rilevato (non applicabile)	Evento	Nodo	Informazioni
Shelf di dischi rimossi (non applicabile)	Evento	Nodo	Informazioni

Eventi dei fan

Gli eventi Fans ti forniscono informazioni sullo stato delle ventole sui nodi del tuo data center, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Una o più ventole non riuscite(ocumEvtFansOneOrMoreFailed)	Incidente	Nodo	Critico

Eventi della scheda flash

Gli eventi della scheda flash forniscono informazioni sullo stato delle schede flash installate nei nodi del data center, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Flash Card offline (ocumEvtFlashCardOffline)	Incidente	Nodo	Critico

Eventi inode

Gli eventi inode forniscono informazioni quando l'inode è pieno o quasi pieno in modo da poter monitorare potenziali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Capacità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Inodes quasi pieno (ocumEvtInodesAlmostFull)	Rischio	Volume	Attenzione
Inodes Full (ocumEvtInodesFull)	Rischio	Volume	Errore

Eventi LIF (Network Interface)

Gli eventi dell'interfaccia di rete forniscono informazioni sullo stato dell'interfaccia di rete (LIF), in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Stato interfaccia di rete inattivo (ocumEvtLifStatusDown)	Rischio	Interfaccia	Errore
Stato interfaccia di rete FC/FCoE inattivo (ocumEvtFCLifStatusDown)	Rischio	Interfaccia	Errore
Failover dell'interfaccia di rete non possibile (ocumEvtLifFailoverNotable)	Rischio	Interfaccia	Attenzione
Interfaccia di rete non sulla porta home (ocumEvtLifNotAtHomePort)	Rischio	Interfaccia	Attenzione

Area di impatto: Configurazione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Routing interfaccia di rete non configurato (non applicabile)	Evento	Interfaccia	Informazioni

Area di impatto: Performance

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Violazione della soglia critica dell'interfaccia di rete MB/s (ocumNetworkLifMbpsIncident)	Incidente	Interfaccia	Critico
Network Interface MB/s Warning Threshold Breached(ocumNetworkLifMbpsWarning)	Rischio	Interfaccia	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Violazione della soglia critica dell'interfaccia di rete FC in MB/s (ocumFcpLifMbpsIncident)	Incidente	Interfaccia	Critico
Soglia di avviso MB/s interfaccia di rete FC violata (ocumFcpLifMbpsWarning)	Rischio	Interfaccia	Attenzione
Soglia critica interfaccia di rete FC NVMf MB/s violata (ocumNvmfFcLifMbpsIncident)	Incidente	Interfaccia	Critico
NVMf FC Network Interface MB/s Warning Threshold Breached(ocumNvmfFcLifMbpsAvvertenza)	Rischio	Interfaccia	Attenzione

Eventi LUN

Gli eventi LUN forniscono informazioni sullo stato delle LUN, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
LUN offline (ocumEvtLunOffline)	Incidente	LUN	Critico
LUN distrutta *(lunDestroy)	Evento	LUN	Informazioni

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
LUN mappato con sistema operativo non supportato in igroup(igroupUnsupportedOsType)	Incidente	LUN	Attenzione
Singolo percorso attivo per accedere al LUN (ocumEvtLunSingleActivePath)	Rischio	LUN	Attenzione
Nessun percorso attivo per accedere al LUN (ocumEvtLunNotReachable)	Incidente	LUN	Critico
Nessun percorso ottimizzato per accedere al LUN (ocumEvtLunOptimizedPathInactive)	Rischio	LUN	Attenzione
Nessun percorso per accedere al LUN dal partner ha (ocumEvtLunHaPathInactive)	Rischio	LUN	Attenzione
Nessun percorso per accedere alla LUN da un nodo in ha-pair(ocumEvtLunNodePathStatusGiù)	Rischio	LUN	Errore

Area di impatto: Capacità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Spazio insufficiente per la copia Snapshot del LUN (ocumEvtLunSnapshotNotPosible)	Rischio	Volume	Attenzione

Area di impatto: Configurazione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
LUN mappato con sistema operativo non supportato in igroup(igroupUnsupportedOsType)	Rischio	LUN	Attenzione

Area di impatto: Performance

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Limite critico IOPS LUN superato (ocumLunIopsIncident)	Incidente	LUN	Critico
Soglia di avviso LUN IOPS violata (ocumLunIopsWarning)	Rischio	LUN	Attenzione
Limite critico LUN MB/s superato(ocumLunMbpsIncident)	Incidente	LUN	Critico
Limite di avviso LUN MB/s superato(ocumLunMbpsWarning)	Rischio	LUN	Attenzione
Latenza LUN ms/soglia critica op violata (ocumLunLatencyIncident)	Incidente	LUN	Critico
Latenza LUN ms/op soglia di avviso violata (ocumLunLatencyWarning)	Rischio	LUN	Attenzione
Latenza LUN e soglia critica IOPS violate (ocumLunLatencyIopsIncident)	Incidente	LUN	Critico
Latenza LUN e soglia di avviso IOPS violate (ocumLunLatencyIopsWarning)	Rischio	LUN	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Latenza LUN e soglia critica MB/s violate (ocumLunLatencyMbpsIncident)	Incidente	LUN	Critico
Latenza LUN e soglia di avviso MB/s violate (ocumLunLatencyMbpsWarning)	Rischio	LUN	Attenzione
Latenza LUN e performance aggregate capacità utilizzata soglia critica violata (ocumLunLatencyAggregatePerfCapacityUsedIncident)	Incidente	LUN	Critico
Latenza LUN e performance aggregate capacità utilizzata soglia di avviso violata (ocumLunLatencyAggregatePerfCapacityUsedWarning)	Rischio	LUN	Attenzione
Latenza LUN e utilizzo aggregato soglia critica violata (ocumLunLatencyAggregateUtilizationIncident)	Incidente	LUN	Critico
Latenza LUN e soglia di avviso di utilizzo aggregato violata (ocumLunLatencyAggregateUtilizationWarning)	Rischio	LUN	Attenzione
Latenza LUN e performance nodo capacità utilizzata soglia critica violata (ocumLunLatencyNodePerfCapacityUsedIncident)	Incidente	LUN	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Latenza LUN e performance nodo capacità utilizzata soglia di avviso violata (ocumLunLatencyNodePerfCapacityUsedWarning)	Rischio	LUN	Attenzione
Latenza del LUN e capacità di performance dei nodi utilizzata - soglia critica di Takeover violata (ocumLunLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incidente	LUN	Critico
Latenza LUN e capacità di performance dei nodi utilizzata - soglia di avviso Takeover violata (ocumLunLatencyAggregatePerfCapacityUsedTakeoverWarning)	Rischio	LUN	Attenzione
Latenza LUN e soglia critica utilizzo nodi violati (ocumLunLatencyNodeUtilisationIncident)	Incidente	LUN	Critico
Latenza LUN e soglia di avviso utilizzo nodo violata(ocumLunLatencyNodeUtilizationWarning)	Rischio	LUN	Attenzione
Soglia di avviso massima IOPS del LUN QoS violata (ocumQosLunMaxIopsWarning)	Rischio	LUN	Attenzione
QoS LUN Max MB/s soglia di avviso violata (ocumQosLunMaxMbpsWarning)	Rischio	LUN	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Soglia di latenza LUN del carico di lavoro violata come definito dalla policy sui livelli di servizio delle performance (ocumConformanceLatencyWarning)	Rischio	LUN	Attenzione

Eventi della stazione di gestione

Gli eventi delle stazioni di gestione forniscono informazioni sullo stato del server su cui è installato Unified Manager, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Configurazione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Spazio su disco del server di gestione quasi pieno (ocumEvtUnifiedManagerDiskSpaceNearlyFull)	Rischio	Stazione di gestione	Attenzione
Spazio su disco del server di gestione pieno (ocumEvtUnifiedManagerDiskSpaceFull)	Incidente	Stazione di gestione	Critico
Memoria server di gestione insufficiente (ocumEvtUnifiedManagerMemoryLow)	Rischio	Stazione di gestione	Attenzione
Server di gestione quasi esaurito (ocumEvtUnifiedManagerMemoryAlmostOut)	Incidente	Stazione di gestione	Critico
Dimensioni del file di log MySQL aumentate; riavvio richiesto (ocumEvtMysqlLogFileSizeWarning)	Incidente	Stazione di gestione	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Total Audit Log Size Allocation sta per essere piena	Rischio	Stazione di gestione	Attenzione
Il certificato server syslog sta per scadere	Rischio	Stazione di gestione	Attenzione
Certificato server syslog scaduto	Rischio	Stazione di gestione	Errore
File di log di audit manomesso	Rischio	Stazione di gestione	Attenzione
File di log di audit cancellato	Rischio	Stazione di gestione	Attenzione
Errore di connessione del server syslog	Rischio	Stazione di gestione	Errore
Configurazione del server syslog modificata	Evento	Stazione di gestione	Attenzione

Area di impatto: Performance

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Impatto sull'analisi dei dati delle performance (ocumEvtUnifiedManagerDataMissingAnalyze)	Rischio	Stazione di gestione	Attenzione
La raccolta dati sulle performance è interessata(ocumEvtUnifiedManagerDataMissingCollection)	Incidente	Stazione di gestione	Critico

Questi ultimi due eventi relativi alle performance erano disponibili solo per Unified Manager 7.2. Se uno di questi eventi si trova nello stato New (nuovo) e si esegue l'aggiornamento a una versione più recente del software Unified Manager, gli eventi non verranno eliminati automaticamente. Sarà necessario spostare manualmente gli eventi nello stato Resolved (risolto).

Eventi del bridge MetroCluster

Gli eventi del bridge MetroCluster forniscono informazioni sullo stato dei bridge, in modo da poter monitorare potenziali problemi in una configurazione MetroCluster su FC. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Bridge Unreachable (ocumEvtBridgeUnreachable) (Bridge non raggiungibile)	Incidente	Ponte di MetroCluster	Critico
Anomalia temperatura ponte (ocumEvtBridgeTemperaturaAbnormalità)	Incidente	Ponte di MetroCluster	Critico

Eventi di connettività MetroCluster

Gli eventi di connettività forniscono informazioni sulla connettività tra i componenti di un cluster e tra i cluster nelle configurazioni MetroCluster over FC e MetroCluster over IP, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Eventi comuni in entrambe le configurazioni

Questi eventi di connettività sono comuni per le configurazioni MetroCluster over FC e MetroCluster over IP.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Tutti i collegamenti tra i partner MetroCluster (ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Incidente	Relazione MetroCluster	Critico
Partner MetroCluster non raggiungibili tramite rete peering(ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Incidente	Relazione MetroCluster	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Funzionalità di disaster recovery MetroCluster interessata(ocumEvtMetroClusterDRStatusImpacted)	Rischio	Relazione MetroCluster	Critico
Configurazione MetroCluster commutata (ocumEvtMetroClusterDRStatusImpacted)	Rischio	Relazione MetroCluster	Attenzione

Configurazione MetroCluster su FC

Questi eventi riguardano le configurazioni MetroCluster su FC.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Tutti i collegamenti inter-switch non attivi(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Incidente	Connessione MetroCluster inter-switch	Critico
Collegamento tra bridge FC-SAS e stack di storage inattivo (ocumEvtBridgeSasPortDown)	Incidente	Connessione MetroCluster bridge stack	Critico
Configurazione MetroCluster parzialmente commutata (ocumEvtMetroClusterDRStatusPartiallyImpacted)	Rischio	Relazione MetroCluster	Errore
Nodo a switch FC tutti i collegamenti di interconnessione FC-VI sono disattivi (ocumEvtMccNodeSwitchFcviLinksDown)	Incidente	Connessione dello switch del nodo MetroCluster	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Nodo allo switch FC: Uno o più collegamenti FC-initiator non attivi (ocumEvtMccNodeSwitchFcLinksOneOrMoreDown)	Rischio	Connessione dello switch del nodo MetroCluster	Attenzione
Nodo a switch FC tutti i collegamenti FC-initiator non sono attivi (ocumEvtMccNodeSwitchFcLinksDown)	Incidente	Connessione dello switch del nodo MetroCluster	Critico
Switch to FC-SAS Bridge FC link Down (ocumEvtMccSwitchBridgeFcLinksDown)	Incidente	Connessione a ponte con switch MetroCluster	Critico
Tutti i collegamenti di interconnessione FC VI tra nodi non attivi (ocumEvtMccInterNodeLinksDown)	Incidente	Connessione tra nodi	Critico
Nodo interno uno o più collegamenti di interconnessione FC VI non attivi (ocumEvtMccInterNodeLinksOneOrMoreDown)	Rischio	Connessione tra nodi	Attenzione
Collegamento da nodo a ponte inattivo (ocumEvtMccNodeBridgeLinksDown)	Incidente	Connessione a bridge di nodi	Critico
Nodo a stack di storage tutti i collegamenti SAS non attivi (ocumEvtMccNodeStackLinksDown)	Incidente	Connessione dello stack di nodi	Critico
Nodo a stack di storage uno o più collegamenti SAS non attivi (ocumEvtMccNodeStackLinksOneOrMoreDown)	Rischio	Connessione dello stack di nodi	Attenzione

Configurazione MetroCluster over IP

Questi eventi riguardano le configurazioni MetroCluster over IP.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Lo stato della connettività tra siti IP MetroCluster è inattivo (mccIntersiteconnectivityStatusDown)	Rischio	Relazione MetroCluster	Critico
Connessione da nodo a switch MetroCluster-IP offline (mcIpPortStatusOffline)	Rischio	Nodo	Errore

Eventi dello switch MetroCluster

Gli eventi dello switch MetroCluster per le configurazioni MetroCluster over FC forniscono informazioni sullo stato degli switch MetroCluster, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Temperatura interruttore anomala(ocumEvtSwitchTemperaturaAbnormalità)	Incidente	Switch MetroCluster	Critico
Switch Unreachable(ocumEvtSwitchUnreachable) (interruttore non raggiungibile)	Incidente	Switch MetroCluster	Critico
Ventole switch non riuscite (ocumEvtSwitchFansOneOrMoreFailed)	Incidente	Switch MetroCluster	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Alimentatori switch non funzionanti (ocumEvtSwitchPowerSuppliesOneOrMoreFailed)	Incidente	Switch MetroCluster	Critico
Errore sensori di temperatura interruttore (ocumEvtSwitchTemperatureSensorFailed) Questo evento è valido solo per gli switch Cisco.	Incidente	Switch MetroCluster	Critico

Eventi NVMe namespace

Gli eventi dello spazio dei nomi NVMe forniscono informazioni sullo stato degli spazi dei nomi, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
NVMeNS non in linea *(nvmeNamespaceStatusOffline)	Evento	Namespace	Informazioni
NVMeNS Online *(nvmeNamespaceStatusOnline)	Evento	Namespace	Informazioni
NVMeNS fuori spazio *(nvmeNamespaceSpaceOutOfSpace)	Rischio	Namespace	Attenzione
NVMeNS Destroy *(nvmeNamespaceDestroy)	Evento	Namespace	Informazioni

Area di impatto: Performance

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Violazione della soglia critica IOPS dello spazio dei nomi NVMe (ocumNvmeNamespaceIopsIncident)	Incidente	Namespace	Critico
Soglia di avviso IOPS dello spazio dei nomi NVMe non rispettata (ocumNvmeNamespaceIopsWarning)	Rischio	Namespace	Attenzione
Soglia critica dello spazio dei nomi NVMe MB/s violata(ocumNvmeNamespaceMbpsIncident)	Incidente	Namespace	Critico
Soglia di avviso dello spazio dei nomi NVMe MB/s violata(ocumNvmeNamespaceMbpsWarning)	Rischio	Namespace	Attenzione
Latenza dello spazio dei nomi NVMe ms/soglia critica operativa violata (ocumNvmeNamespaceLatencyIncident)	Incidente	Namespace	Critico
Latenza dello spazio dei nomi NVMe ms/op soglia di avviso violata (ocumNvmeNamespaceLatencyWarning)	Rischio	Namespace	Attenzione
Latenza dello spazio dei nomi NVMe e soglia critica IOPS violate (ocumNvmeNamespaceLatencyIopsIncident)	Incidente	Namespace	Critico
Latenza dello spazio dei nomi NVMe e soglia di avviso IOPS violata (ocumNvmeNamespaceLatencyIopsWarning)	Rischio	Namespace	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Latenza dello spazio dei nomi NVMe e soglia critica MB/s violate (ocumNvmeNamespaceLatencyMbpsIncident)	Incidente	Namespace	Critico
Latenza dello spazio dei nomi NVMe e soglia di avviso MB/s violata (ocumNvmeNamespaceLatencyMbpsWarning)	Rischio	Namespace	Attenzione

Eventi del nodo

Gli eventi dei nodi forniscono informazioni sullo stato dei nodi in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Spazio volume radice nodo quasi pieno (ocumEvtClusterNodeRootVolumeSpaceNearlyFull)	Rischio	Nodo	Attenzione
Cloud AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	Rischio	Nodo	Errore
Cloud AWS IAMCredsExpired *(ocumCloudAwsIamCredsExpired)	Rischio	Nodo	Errore
Cloud AWS IAMCredsInvalid *(ocumCloudAwsIamCredsInvalid)	Rischio	Nodo	Errore

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Cloud AWS IAMCredsNotFound *(ocumCloudAwsIamCredsNotFound)	Rischio	Nodo	Errore
Cloud AWS IAMCredsNotInitialized *(ocumCloudAwsIamCredsNotInitialized)	Evento	Nodo	Informazioni
Cloud AWS IAMRoleInvalid *(ocumCloudAwsIamRoleInvalid)	Rischio	Nodo	Errore
Cloud AWS IAMRoleNotFound *(ocumCloudAwsIamRoleNotFound)	Rischio	Nodo	Errore
Host di livello cloud non risolvibile *(ocumObjstoreHostUnresolvable)	Rischio	Nodo	Errore
Livello cloud LIF Intercluster inattivo *(ocumObjstoreInterClusterLifDown)	Rischio	Nodo	Errore
Uno dei pool NFSv4 esaurito *(nBladeNfsv4PoolEXhaust)	Incidente	Nodo	Critico
Richiesta di mancata corrispondenza della firma del livello cloud *(oscSignatureMismatch)	Rischio	Nodo	Errore

Area di impatto: Capacità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
QoS Monitor Memory maxed *(ocumQosMonitorMemoryMaxed)	Rischio	Nodo	Errore
Memoria monitor QoS abated *(ocumQosMonitorMemoryAbated)	Evento	Nodo	Informazioni

Area di impatto: Configurazione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Nodo rinominato (non applicabile)	Evento	Nodo	Informazioni

Area di impatto: Performance

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Soglia critica IOPS nodo violata (ocumNodeIopsIncident)	Incidente	Nodo	Critico
Soglia di avviso IOPS nodo violata (ocumNodeIopsWarning)	Rischio	Nodo	Attenzione
Soglia critica nodo MB/s violata (ocumNodeMbpsIncident)	Incidente	Nodo	Critico
Soglia di avviso MB/s nodo violata (ocumNodeMbpsWarning)	Rischio	Nodo	Attenzione
Latenza nodo ms/soglia critica operativa violata (ocumNodeLatencyIncident)	Incidente	Nodo	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Latenza nodo ms/op soglia di avviso violata (ocumNodeLatencyWarning)	Rischio	Nodo	Attenzione
Violazione della soglia critica utilizzata per la capacità di performance del nodo (ocumNodePerfCapacityUsedIncident)	Incidente	Nodo	Critico
Soglia di avviso utilizzata capacità di performance nodo violata (ocumNodePerfCapacityUsedWarning)	Rischio	Nodo	Attenzione
Capacità di performance del nodo utilizzata - superamento della soglia critica (ocumNodePerfCapacityUsedTakeoverIncident)	Incidente	Nodo	Critico
Capacità di performance del nodo utilizzata - soglia di avviso Takeover violata (ocumNodePerfCapacityUsedTakeoverWarning)	Rischio	Nodo	Attenzione
Violazione della soglia critica di utilizzo del nodo (ocumNodeUtilizationIncident)	Incidente	Nodo	Critico
Soglia di avviso utilizzo nodo violata (ocumNodeUtilizationWarning)	Rischio	Nodo	Attenzione
Soglia di sovrautilizzo della coppia ha del nodo violata (ocumNodeHaPairOverUtilisedInformation)	Evento	Nodo	Informazioni

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Soglia di frammentazione del disco del nodo violata (ocumNodeDiskFragmentationWarning)	Rischio	Nodo	Attenzione
Violazione della soglia di utilizzo della capacità di performance (ocumNodeOverUtilisedWarning)	Rischio	Nodo	Attenzione
Soglia dinamica del nodo violata (ocumNodeDynamicEventWarning)	Rischio	Nodo	Attenzione

Area di impatto: Sicurezza

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
ID avviso: NTAP-<__advisory ID_>(ocumx)	Rischio	Nodo	Critico

Eventi della batteria NVRAM

Gli eventi relativi alla batteria NVRAM forniscono informazioni sullo stato delle batterie in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Batteria NVRAM scarica (ocumEvtNvramBatteryLow)	Rischio	Nodo	Attenzione
Batteria NVRAM scarica (ocumEvtNvramBatteryDischarged)	Rischio	Nodo	Errore

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Batteria NVRAM carica eccessivamente (ocumEvtNvvramBatteryOvercharged)	Incidente	Nodo	Critico

Eventi delle porte

Gli eventi delle porte forniscono informazioni sullo stato delle porte del cluster, in modo da poter monitorare le modifiche o i problemi della porta, ad esempio se la porta non è attiva.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Stato porta inattivo(ocumEvtPortStatusDown)	Incidente	Nodo	Critico

Area di impatto: Performance

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Violazione della soglia critica della porta di rete MB/s (ocumNetworkPortMbpsIncident)	Incidente	Porta	Critico
Soglia di avviso della porta di rete MB/s non rispettata (ocumNetworkPortMbpsWarning)	Rischio	Porta	Attenzione
Violazione della soglia critica della porta FCP MB/s (ocumFcpPortMbpsIncident)	Incidente	Porta	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Soglia di avviso MB/s della porta FCP non rispettata (ocumFcpPortMbpsWarning)	Rischio	Porta	Attenzione
Violazione della soglia critica di utilizzo della porta di rete (ocumNetworkPortUtilisationIncident)	Incidente	Porta	Critico
Soglia avviso utilizzo porta di rete non rispettata (ocumNetworkPortUtilisationWarning)	Rischio	Porta	Attenzione
Violazione della soglia critica di utilizzo della porta FCP (ocumFcpPortUtilisationIncident)	Incidente	Porta	Critico
Soglia avviso utilizzo porta FCP non rispettata (ocumFcpPortUtilizationWarning)	Rischio	Porta	Attenzione

Eventi relativi agli alimentatori

Gli eventi relativi agli alimentatori forniscono informazioni sullo stato dell'hardware in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Uno o più alimentatori non funzionanti (ocumEvtPowerSupplyOneOrMoreFailed)	Incidente	Nodo	Critico

Eventi di protezione

Gli eventi di protezione indicano se un lavoro è stato interrotto o non è riuscito, in modo da poter monitorare i problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Protezione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Processo di protezione non riuscito (ocumEvtProtectionJobTaskFailed)	Incidente	Servizio di storage o volume	Critico
Processo di protezione interrotto (ocumEvtProtectionJobAborted)	Rischio	Servizio di storage o volume	Attenzione

Eventi qtree

Gli eventi qtree forniscono informazioni sulla capacità di qtree e sui limiti di file e dischi, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Capacità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Spazio qtree quasi pieno (ocumEvtQtreeSpaceNearlyFull)	Rischio	Qtree	Attenzione
Spazio qtree pieno (ocumEvtQtreeSpaceFull)	Rischio	Qtree	Errore
Spazio qtree normale(ocumEvtQtreeSpaceThresholdOk)	Evento	Qtree	Informazioni
Limite massimo di file qtree raggiunto (ocumEvtQtreeFilesHardLimitReached)	Incidente	Qtree	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
File qtree limite di software superato(ocumEvtQtreeFilesSoftLimitBreached)	Rischio	Qtree	Attenzione
Limite massimo spazio qtree raggiunto (ocumEvtQtreeSpaceHardLimitReached)	Incidente	Qtree	Critico
Limite soft spazio qtree superato(ocumEvtQtreeSpaceSoftLimitBreached)	Rischio	Qtree	Attenzione

Eventi del Service Processor

Gli eventi del Service Processor forniscono informazioni sullo stato del processore, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Service Processor non configurato(ocumEvtServiceProcessorNotConfigured)	Rischio	Nodo	Attenzione
Service Processor offline (ocumEvtServiceProcessoroffline)	Rischio	Nodo	Errore

Eventi di relazione SnapMirror

Gli eventi di relazione di SnapMirror forniscono informazioni sullo stato delle relazioni asincrone e sincrona SnapMirror, in modo da poter monitorare eventuali problemi. Gli eventi di relazione SnapMirror asincroni vengono generati sia per le VM di storage che per i volumi, ma gli eventi di relazione SnapMirror sincroni vengono generati solo per le relazioni dei volumi. Non vengono generati eventi per i volumi costituenti che fanno parte delle relazioni di disaster recovery di Storage VM. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Protezione

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Gli eventi delle relazioni SnapMirror vengono generati per le VM di storage protette dal disaster recovery delle VM di storage, ma non per le relazioni tra gli oggetti costituenti.

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Replica mirror non sana(ocumEvtSnapmirrorRelationshipUnsana)	Rischio	Relazione di SnapMirror	Attenzione
Replica mirror interrotta(ocumEvtSnapmirrorRelationshipStateBrokenoff)	Rischio	Relazione di SnapMirror	Errore
Inizializzazione replica mirror non riuscita (ocumEvtSnapmirrorRelationshipInitializeFailed)	Rischio	Relazione di SnapMirror	Errore
Aggiornamento replica mirror non riuscito (ocumEvtSnapmirrorRelationshipUpdateFailed)	Rischio	Relazione di SnapMirror	Errore
Errore ritardo replica mirror (ocumEvtSnapMirrorRelationshipLagError)	Rischio	Relazione di SnapMirror	Errore
Mirror Replication Lag Warning(ocumEvtSnapMirrorRelationshipLagWarning)	Rischio	Relazione di SnapMirror	Attenzione
Risincronizzazione replica mirror non riuscita (ocumEvtSnapmirrorRelationshipResyncFailed)	Rischio	Relazione di SnapMirror	Errore
Replica sincrona fuori sincronizzazione *(syncSnapmirrorRelationshipOutofsync)	Rischio	Relazione di SnapMirror	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Replica sincrona ripristinata *(syncSnapmirrorRelationshipInSync)	Evento	Relazione di SnapMirror	Informazioni
Risincronizzazione automatica replica sincrona non riuscita *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Rischio	Relazione di SnapMirror	Errore
Il mediatore ONTAP viene aggiunto al cluster (SnapmirrorMediatorAdded)	Evento	Cluster	Informazioni
Il supporto ONTAP viene rimosso dal cluster (SnapmirrorMediatorRemoved)	Evento	Cluster	Informazioni
Il mediatore ONTAP non è raggiungibile dal cluster (snapmirrorMediatorUnreachable)	Rischio	Mediatore	Attenzione
Il mediatore ONTAP non è accessibile dal cluster (snapmirrorMediatorMisconfigured)	Rischio	Mediatore	Errore
La connettività dei mediatori ONTAP è stata ristabilita ed è pronta per SMBC (SnapmirrorMediatorInQuorum)	Evento	Mediatore	Informazioni

Eventi di relazione di mirroring asincrono e vault

Gli eventi di relazione di mirroring asincrono e vault forniscono informazioni sullo stato delle relazioni di SnapMirror asincrono e Vault in modo da poter monitorare eventuali problemi. Gli eventi di relazione asincroni Mirror e Vault sono supportati sia per le relazioni di protezione dei volumi che per le Storage VM. Tuttavia, solo le relazioni del vault non sono supportate per il disaster recovery delle macchine virtuali di storage. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della

trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Protezione

Gli eventi delle relazioni SnapMirror e Vault vengono generati anche per le VM di storage protette dal disaster recovery delle VM di storage, ma non per le relazioni tra gli oggetti costituenti.

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Mirroring asincrono e vault non integri(ocumEvtMirrorVaultRelationshipUnintegro)	Rischio	Relazione di SnapMirror	Attenzione
Mirroring asincrono e vault interrotto(ocumEvtMirrorVaultRelationshipStateBrokenoff)	Rischio	Relazione di SnapMirror	Errore
Mirroring asincrono e inizializzazione del vault non riuscita (ocumEvtMirrorVaultRelationshipInitializeFailed)	Rischio	Relazione di SnapMirror	Errore
Aggiornamento asincrono del mirror e del vault non riuscito (ocumEvtMirrorVaultRelationshipUpdateFailed)	Rischio	Relazione di SnapMirror	Errore
Errore di mirroring asincrono e ritardo del vault (ocumEvtMirrorVaultRelationshipLagError)	Rischio	Relazione di SnapMirror	Errore
Mirror asincrono e Vault Lag Warning(ocumEvtMirrorVaultRelationshipLagWarning)	Rischio	Relazione di SnapMirror	Attenzione
Mirroring asincrono e risincronizzazione del vault non riuscita (ocumEvtMirrorVaultRelationshipResyncFailed)	Rischio	Relazione di SnapMirror	Errore

L’evento "errore di aggiornamento di SnapMirror" viene generato dal portale Active IQ (Config Advisor).

Eventi Snapshot

Gli eventi Snapshot forniscono informazioni sullo stato delle snapshot che consentono di monitorare le snapshot per individuare potenziali problemi. Gli eventi sono raggruppati per area di impatto e includono nome dell’evento, nome della trap, livello di impatto, tipo di origine e severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Eliminazione automatica di Snapshot disattivata (non applicabile)	Evento	Volume	Informazioni
Eliminazione automatica snapshot abilitata (non applicabile)	Evento	Volume	Informazioni
Configurazione dell’eliminazione automatica di Snapshot modificata (non applicabile)	Evento	Volume	Informazioni

Eventi di relazione SnapVault

Gli eventi di relazione SnapVault forniscono informazioni sullo stato delle relazioni SnapVault in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all’area di impatto e includono il nome dell’evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Protezione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Vault asincrono non integro(ocumEvtSnapVaultRelationshipUnintegro)	Rischio	Relazione di SnapMirror	Attenzione
Vault asincrono interrotto(ocumEvtSnapVaultRelationshipStateBrokenoff)	Rischio	Relazione di SnapMirror	Errore

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Inizializzazione asincrona del vault non riuscita (ocumEvtSnapVaultRelationshipInitializeFailed)	Rischio	Relazione di SnapMirror	Errore
Aggiornamento asincrono del vault non riuscito (ocumEvtSnapVaultRelationshipUpdateFailed)	Rischio	Relazione di SnapMirror	Errore
Errore di ritardo del vault asincrono (ocumEvtSnapVaultRelationshipLagError)	Rischio	Relazione di SnapMirror	Errore
Asincrono Vault Lag Warning(ocumEvtSnapVaultRelationshipLagWarning)	Rischio	Relazione di SnapMirror	Attenzione
Risincronizzazione asincrona del vault non riuscita (ocumEvtSnapvaultRelationshipResyncFailed)	Rischio	Relazione di SnapMirror	Errore

Eventi delle impostazioni di failover dello storage

Gli eventi delle impostazioni di failover dello storage (SFO) forniscono informazioni sulla disattivazione o meno del failover dello storage, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Storage failover Interconnect uno o più collegamenti non attivi(ocumEvtsfoInterconnectOneOrMoreLinksDown)	Rischio	Nodo	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Failover dello storage disattivato (ocumEvtsfoSettingsDisabilitato)	Rischio	Nodo	Errore
Failover dello storage non configurato(ocumEvtSfoSettingsNotConfigured)	Rischio	Nodo	Errore
Stato di failover dello storage - Takeover (ocumEvtSfoStateTakeover)	Rischio	Nodo	Attenzione
Stato di failover dello storage - Giveback parziale(ocumEvtSfoStatePartialGiveback)	Rischio	Nodo	Errore
Stato del nodo di failover dello storage inattivo (ocumEvtsfoNodeStatusDown)	Rischio	Nodo	Errore
Takeover di failover dello storage non possibile (ocumEvtSfoTakeoverNotPosible)	Rischio	Nodo	Errore

Eventi relativi ai servizi di storage

Gli eventi relativi ai servizi di storage forniscono informazioni sulla creazione e l'abbonamento dei servizi di storage, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Configurazione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Servizio di storage creato (non applicabile)	Evento	Servizio di storage	Informazioni
Servizio di storage iscritto (non applicabile)	Evento	Servizio di storage	Informazioni

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Servizio di storage non sottoscritto (non applicabile)	Evento	Servizio di storage	Informazioni

Area di impatto: Protezione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Eliminazione imprevista della RelationshippoumEvtStorageServiceUnsupportedRelationshipDeletion gestita da SnapMirror	Rischio	Servizio di storage	Attenzione
Eliminazione imprevista del volume membro del servizio di storage (ocumEvtStorageServiceUnespectedVolumeDeletion)	Incidente	Servizio di storage	Critico

Eventi di shelf storage

Gli eventi relativi agli shelf di storage indicano se lo shelf di storage presenta anomalie, in modo da poter monitorare potenziali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Intervallo di tensione anomalo (ocumEvtShelfVoltageAbnormal)	Rischio	Shelf di storage	Attenzione
Intervallo di corrente anomalo (ocumEvtShelfCurrentAbnormal)	Rischio	Shelf di storage	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Temperatura anomala(ocumEvtShelfTemperatureAbnormal)	Rischio	Shelf di storage	Attenzione

Eventi di storage VM

Gli eventi Storage VM (Storage Virtual Machine, noto anche come SVM) forniscono informazioni sullo stato delle VM di storage, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
SVM CIFS Service Down(ocumEvtVserverCifsServiceStatusDown)	Incidente	SVM	Critico
Servizio SVM CIFS non configurato (non applicabile)	Evento	SVM	Informazioni
Tentativi di connessione di CIFS Share * inesistente (nbladeCifsNoPrivShare)	Incidente	SVM	Critico
Conflitto nome NetBIOS CIFS *(nbladeCifsNbNameConflict)	Rischio	SVM	Errore
Operazione di copia shadow CIFS non riuscita *(cifsShadowCopyFailure)	Rischio	SVM	Errore
Molte connessioni CIFS *(nbladeCifsManyAuths)	Rischio	SVM	Errore
Connessione CIFS massima superata *(nbladeCifsMaxOpenSameFile)	Rischio	SVM	Errore

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Numero massimo di connessioni CIFS per utente superato *(nbladeCifsMaxSessPerUsrConn)	Rischio	SVM	Errore
Servizio SVM FC/FCoE inattivo(ocumEvtVserverFcServiceStatusDown)	Incidente	SVM	Critico
Servizio iSCSI SVM inattivo(ocumEvtVserverIscsiServiceStatusDown)	Incidente	SVM	Critico
SVM NFS Service Down(ocumEvtVserverNfsServiceStatusDown)	Incidente	SVM	Critico
Servizio SVM FC/FCoE non configurato (non applicabile)	Evento	SVM	Informazioni
Servizio iSCSI SVM non configurato (non applicabile)	Evento	SVM	Informazioni
Servizio NFS SVM non configurato (non applicabile)	Evento	SVM	Informazioni
SVM interrotta(ocumEvtVserverGiù)	Rischio	SVM	Attenzione
Server AV troppo occupato per accettare nuova richiesta di scansione *(nbladeVscanConnBackPressure)	Rischio	SVM	Errore
Nessuna connessione al server AV per Virus Scan *(nbladeVscanNoScannerConn)	Incidente	SVM	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Nessun server AV registrato *(nBladeVscanNoRegdscanner)	Rischio	SVM	Errore
Nessuna connessione al server AV reattiva *(nbladeVscanConnInactive)	Evento	SVM	Informazioni
Tentativo di utente non autorizzato di accedere al server AV *(nbladeVscanBadUserPrivAccess)	Rischio	SVM	Errore
Virus rilevato da AV Server *(nbladeVscanVirusDetected)	Rischio	SVM	Errore

Area di impatto: Configurazione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
SVM rilevato (non applicabile)	Evento	SVM	Informazioni
SVM cancellato (non applicabile)	Evento	Cluster	Informazioni
SVM rinominato (non applicabile)	Evento	SVM	Informazioni

Area di impatto: Performance

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Violazione della soglia critica IOPS SVM (ocumSvmIopsIncident)	Incidente	SVM	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Soglia di avviso IOPS SVM non rispettata (ocumSvmIopsWarning)	Rischio	SVM	Attenzione
Soglia critica SVM MB/s violata (ocumSvmMbpsIncident)	Incidente	SVM	Critico
Soglia di avviso SVM MB/s violata (ocumSvmMbpsWarning)	Rischio	SVM	Attenzione
Violazione della soglia critica di latenza SVM (ocumSvmLatencyIncident)	Incidente	SVM	Critico
Soglia di avviso latenza SVM violata (ocumSvmLatencyWarning)	Rischio	SVM	Attenzione

Area di impatto: Sicurezza

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Log di audit disattivato (ocumVserverAuditLogDisabilitato)	Rischio	SVM	Attenzione
Banner di accesso disattivato (ocumVserverLoginBannerDisabilitato)	Rischio	SVM	Attenzione
SSH sta utilizzando crittografia non sicura(ocumVserverSSHInSecure)	Rischio	SVM	Attenzione
Banner di accesso modificato(ocumVserverLoginBannerChanged)	Rischio	SVM	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Il monitoraggio anti-ransomware delle VM di storage è disattivato (antiRansomwareSvmStateDisabilitato)	Rischio	SVM	Attenzione
Il monitoraggio anti-ransomware delle VM di storage è attivato (modalità di apprendimento) (antiRansomwareSvmStateDrun)	Evento	SVM	Informazioni
Storage VM adatto per il monitoraggio anti-ransomware (Learning Mode) (ocumEvtSvmArwCandidate)	Evento	SVM	Informazioni

Eventi quota utente e gruppo

Gli eventi di quota di utenti e gruppi forniscono informazioni sulla capacità della quota di utenti e gruppi di utenti, nonché sui limiti di file e dischi, in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Capacità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Limite minimo spazio su disco quota utente o gruppo superato(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Rischio	Quota utente o di gruppo	Attenzione
Limite massimo di spazio su disco per quota utente o gruppo raggiunto (ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Incidente	Quota utente o di gruppo	Critico

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Numero di file di quota utente o gruppo - limite minimo superato (ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Rischio	Quota utente o di gruppo	Attenzione
Numero di file di quota utente o gruppo - limite massimo raggiunto (ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Incidente	Quota utente o di gruppo	Critico

Eventi di volume

Gli eventi di volume forniscono informazioni sullo stato dei volumi che consentono di monitorare eventuali problemi. Gli eventi sono raggruppati per area di impatto e includono nome dell'evento, nome della trap, livello di impatto, tipo di origine e severità.

Un asterisco (*) identifica gli eventi EMS che sono stati convertiti in eventi Unified Manager.

Area di impatto: Disponibilità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Volume Restricted (ocumEvtVolumeRestricted) (Volume limitato)	Rischio	Volume	Attenzione
Volume offline (ocumEvtVolumeOffline)	Incidente	Volume	Critico
Volume parzialmente disponibile(ocumEvtVolumePartiallyAvailable)	Rischio	Volume	Errore
Volume non montato (non applicabile)	Evento	Volume	Informazioni
Montato sul volume (non applicabile)	Evento	Volume	Informazioni
Volume rimontato (non applicabile)	Evento	Volume	Informazioni

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Percorso di giunzione del volume inattivo(ocumEvtVolumeJunctionPathInactive)	Rischio	Volume	Attenzione
Volume Autodimensiona abilitato (non applicabile)	Evento	Volume	Informazioni
Volume Autodimensiona - Disabilitato (non applicabile)	Evento	Volume	Informazioni
Volume Autodimensiona capacità massima modificata (non applicabile)	Evento	Volume	Informazioni
Volume Autodize Increment Size Modified (dimensione incremento dimensionamento automatico volume modificata) (non applicabile)	Evento	Volume	Informazioni

Area di impatto: Capacità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Spazio dei volumi con thin provisioning a rischio(ocumThinProvisionVolumeSpaceAtRisk)	Rischio	Volume	Attenzione
Spazio volume pieno (ocumEvtVolumeFull)	Rischio	Volume	Errore
Spazio volume quasi pieno (ocumEvtVolumeNearlyFull)	Rischio	Volume	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Volume Logical Space Full (spazio logico volume pieno) *(volumeLogicalSpaceFull)	Rischio	Volume	Errore
Spazio logico volume quasi pieno *(volumeLogicalSpaceNearlyFull)	Rischio	Volume	Attenzione
Volume Logical Space Normal (spazio logico volume normale) *(volumeLogicalSpaceAllOK)	Evento	Volume	Informazioni
Volume Snapshot Reserve Space Full (spazio riserva snapshot volume pieno) (ocumEvtSnapshotFull)	Rischio	Volume	Attenzione
Troppe copie Snapshot(ocumEvtSnapshotTooMany)	Rischio	Volume	Errore
Quota Qtree volume overcommitted(ocumEvtVolumeQtreeQuotaOvercommitted)	Rischio	Volume	Errore
Quota Qtree volume quasi sovrascrittura(ocumEvtVolumeQtreeQuotaAlmostOvercommit)	Rischio	Volume	Attenzione
Tasso di crescita del volume anomalo (ocumEvtVolumeGrowthRateAbnormal)	Rischio	Volume	Attenzione
Volume Days until Full (ocumEvtVolumeDaysUntilFullSoon)	Rischio	Volume	Errore

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Garanzia spazio volume disabilitata (non applicabile)	Evento	Volume	Informazioni
Garanzia spazio volume abilitata (non applicabile)	Evento	Volume	Informazioni
Garanzia spazio volume modificata (non applicabile)	Evento	Volume	Informazioni
Volumi Snapshot Reserve Days until Full (ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Rischio	Volume	Errore
I componenti FlexGroup hanno problemi di spazio *(FlexGroupConstituentsHaveSpaceIssues)	Rischio	Volume	Errore
Stato dello spazio dei componenti FlexGroup OK *(flexGroupConstitutsSpaceStatusAllOK)	Evento	Volume	Informazioni
I componenti FlexGroup hanno problemi di nodi *(FlexGroupConstitutsHaveInodesIssues)	Rischio	Volume	Errore
FlexGroup costituenti nodi Stato tutti OK *(FlexGroupConstitutsInodesStatusAllOK)	Evento	Volume	Informazioni
Errore di dimensionamento automatico del volume WAFL *(waflVolAutoSizeFail)	Rischio	Volume	Errore

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Dimensionamento automatico volume WAFL eseguito *(waflVolAutoSizeDone)	Evento	Volume	Informazioni
Il volume FlexGroup viene utilizzato per oltre il 80%*	Incidente	Volume	Errore
Il volume FlexGroup viene utilizzato per oltre il 90%*	Incidente	Volume	Critico
Anomalia nell'efficienza dello storage dei volumi (ocumVolumeAbnormalStorageEfficiencyWarning)	Rischio	Volume	Attenzione
Volume Snapshot Reserve sottoutilizzato (volumeSnaphotReserveUnderutilisedWarning)	Evento	Volume	Attenzione
Volume Snapshot Reserve sottoutilizzato (volumeSnaphotReserveUnderutilisedCleared)	Evento	Volume	Attenzione

Area di impatto: Configurazione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Volume rinominato (non applicabile)	Evento	Volume	Informazioni
Volume rilevato (non applicabile)	Evento	Volume	Informazioni
Volume cancellato (non applicabile)	Evento	Volume	Informazioni

Area di impatto: Performance

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Soglia di avviso IOPS massima volume QoS violata (ocumQosVolumeMaxIopsWarning)	Rischio	Volume	Attenzione
Soglia di avviso max MB/s volume QoS violata (ocumQosVolumeMaxMbpsWarning)	Rischio	Volume	Attenzione
Soglia di avviso massima IOPS/TB volume QoS violata (ocumQosVolumeMaxIopsPerTbWarning)	Rischio	Volume	Attenzione
Soglia di latenza del volume del carico di lavoro violata come definito dalla policy sui livelli di servizio delle performance (ocumConformanceLatencyWarning)	Rischio	Volume	Attenzione
Violazione della soglia critica IOPS del volume (ocumVolumeIopsIncident)	Incidente	Volume	Critico
Soglia di avviso IOPS volume violata (ocumVolumeIopsWarning)	Rischio	Volume	Attenzione
Soglia critica volume MB/s violata (ocumVolumeMbpsIncident)	Incidente	Volume	Critico
Limite di avviso MB/s volume superato(ocumVolumeMbpsWarning)	Rischio	Volume	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Latenza volume ms/soglia critica operativa violata (ocumVolumeLatencyIncident)	Incidente	Volume	Critico
Latenza volume ms/op soglia di avviso violata (ocumVolumeLatencyWarning)	Rischio	Volume	Attenzione
Soglia critica del rapporto miss cache volume violata (ocumVolumeCacheMissRatioIncident)	Incidente	Volume	Critico
Soglia di avviso rapporto perdita cache volume - violazione (ocumVolumeCacheMissRatioWarning)	Rischio	Volume	Attenzione
Latenza del volume e soglia critica IOPS violate (ocumVolumeLatencyIopsIncident)	Incidente	Volume	Critico
Latenza del volume e soglia di avviso IOPS violate (ocumVolumeLatencyIopsWarning)	Rischio	Volume	Attenzione
Latenza del volume e soglia critica MB/s violate(ocumVolumeLatencyMbpsIncident)	Incidente	Volume	Critico
Latenza del volume e soglia di avviso MB/s violata(ocumVolumeLatencyMbpsWarning)	Rischio	Volume	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Latenza del volume e performance aggregate capacità utilizzata soglia critica violata (ocumVolumeLatencyAggregatePerfCapacityUsedIncident)	Incidente	Volume	Critico
Latenza del volume e performance aggregate capacità utilizzata soglia di avviso violata (ocumVolumeLatencyAggregatePerfCapacityUsedWarning)	Rischio	Volume	Attenzione
Latenza del volume e utilizzo dell'aggregato soglia critica violata(ocumVolumeLatencyAggregateUtilizationIncident)	Incidente	Volume	Critico
Latenza del volume e utilizzo dell'aggregato soglia di avviso violata(ocumVolumeLatencyAggregateUtilizationWarning)	Rischio	Volume	Attenzione
Latenza del volume e performance del nodo capacità utilizzata soglia critica violata (ocumVolumeLatencyNodePerfCapacityUsedIncident)	Incidente	Volume	Critico
Latenza del volume e performance del nodo capacità utilizzata soglia di avviso violata (ocumVolumeLatencyNodePerfCapacityUsedWarning)	Rischio	Volume	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Latenza del volume e capacità di performance del nodo utilizzata - superamento della soglia critica di Takeover (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverIncident)	Incidente	Volume	Critico
Latenza del volume e capacità di performance del nodo utilizzata - soglia di avviso Takeover violata (ocumVolumeLatencyAggregatePerfCapacityUsedTakeoverWarning)	Rischio	Volume	Attenzione
Latenza del volume e soglia critica di utilizzo del nodo violata(ocumVolumeLatencyNodeUtilizationIncident)	Incidente	Volume	Critico
Latenza del volume e soglia di avviso di utilizzo del nodo violata(ocumVolumeLatencyNodeUtilizationWarning)	Rischio	Volume	Attenzione

Area di impatto: Sicurezza

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Il monitoraggio anti-ransomware del volume è attivato (modalità attiva) (antiRansomwareVolumeStateEnabled)	Evento	Volume	Informazioni
Il monitoraggio anti-ransomware del volume è disattivato (antiRansomwareVolumeStateDisabilitato)	Rischio	Volume	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Il monitoraggio anti-ransomware del volume è attivato (modalità apprendimento) (antiRansomwareVolumeStateDryrun)	Evento	Volume	Informazioni
Il monitoraggio anti-ransomware del volume è in pausa (modalità di apprendimento) (antiRansomwareVolumeStateDrunPaused)	Rischio	Volume	Attenzione
Il monitoraggio anti-ransomware del volume è in pausa (modalità attiva) (antiRansomwareVolumeStateEnablePaused)	Rischio	Volume	Attenzione
Il monitoraggio anti-ransomware del volume è in fase di disabilitazione (antiRansomwareVolumeStateDisableInProgress)	Rischio	Volume	Attenzione
Attività ransomware vista (callHomeRansomwareActivitySeen)	Incidente	Volume	Critico
Volume adatto per il monitoraggio anti-ransomware (modalità apprendimento) (ocumEvtVolumeArwCandidate)	Evento	Volume	Informazioni
Volume adatto per il monitoraggio anti-ransomware (Active Mode) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Rischio	Volume	Attenzione

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Il volume presenta avvisi anti-ransomware rumorosi (antiRansomwareFeature NoisyVolume)	Rischio	Volume	Attenzione

Area di impatto: Protezione dei dati

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Il volume non dispone di una protezione Snapshot locale sufficiente (volumeLacksLocalProtectionWarning)	Rischio	Volume	Attenzione
Il volume non dispone di una protezione Snapshot locale sufficiente (volumeLacksLocalProtectionCleared)	Rischio	Volume	Attenzione

Eventi di stato dello spostamento del volume

Gli eventi di stato dello spostamento del volume indicano lo stato dello spostamento del volume in modo da poter monitorare eventuali problemi. Gli eventi sono raggruppati in base all'area di impatto e includono il nome dell'evento e della trap, il livello di impatto, il tipo di origine e la severità.

Area di impatto: Capacità

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Stato spostamento volume: In corso (non applicabile)	Evento	Volume	Informazioni
Stato spostamento volume - non riuscito (ocumEvtVolumeMoveFailed)	Rischio	Volume	Errore
Stato spostamento volume: Completato (non applicabile)	Evento	Volume	Informazioni

Nome evento (nome trap)	Livello di impatto	Tipo di origine	Severità
Spostamento del volume - Cutover rinviato (ocumEvtVolumeMoveCutoverrinviato)	Rischio	Volume	Attenzione

Descrizione delle finestre di dialogo e degli eventi

Gli eventi ti avvisano di eventuali problemi nel tuo ambiente. È possibile utilizzare la pagina inventario gestione eventi e la pagina Dettagli evento per monitorare tutti gli eventi. È possibile utilizzare la finestra di dialogo Opzioni di impostazione delle notifiche per configurare le notifiche. È possibile utilizzare la pagina impostazione eventi per disattivare o attivare gli eventi.

Pagina delle notifiche

È possibile configurare il server Unified Manager in modo che invii notifiche quando viene generato un evento o quando viene assegnato a un utente. È inoltre possibile configurare i meccanismi di notifica. Ad esempio, le notifiche possono essere inviate come e-mail o trap SNMP.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

E-mail

Questa area consente di configurare le seguenti impostazioni e-mail per la notifica degli avvisi:

- **Indirizzo mittente**

  Specifica l'indirizzo e-mail da cui viene inviata la notifica di avviso. Questo valore viene utilizzato anche come indirizzo di origine per un report quando condiviso. Se l'indirizzo da è pre-compilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", è necessario modificarlo in un indirizzo e-mail reale e funzionante per assicurarsi che tutte le notifiche e-mail vengano inviate correttamente.

Server SMTP

Questa sezione consente di configurare le seguenti impostazioni del server SMTP:

- **Nome host o Indirizzo IP**

  Specifica il nome host del server host SMTP utilizzato per inviare la notifica di avviso ai destinatari specificati.

- **Nome utente**

  Specifica il nome utente SMTP. Il nome utente SMTP è obbligatorio solo se SMTPAUTH è attivato nel server SMTP.

- **Password**

Specifica la password SMTP. Il nome utente SMTP è obbligatorio solo se SMTPAUTH è attivato nel server SMTP.

- **Porta**

  Specifica la porta utilizzata dal server host SMTP per inviare la notifica di avviso.

  Il valore predefinito è 25.

- **Usa START/TLS**

  La selezione di questa casella consente una comunicazione sicura tra il server SMTP e il server di gestione utilizzando i protocolli TLS/SSL (noti anche come start_tls e STARTTLS).

- **Usa SSL**

  Selezionando questa casella si attiva la comunicazione sicura tra il server SMTP e il server di gestione mediante il protocollo SSL.

SNMP

Quest'area consente di configurare le seguenti impostazioni di trap SNMP:

- **Versione**

  Specifica la versione SNMP che si desidera utilizzare in base al tipo di protezione richiesto. Le opzioni includono versione 1, versione 3, versione 3 con autenticazione e versione 3 con autenticazione e crittografia. Il valore predefinito è versione 1.

- **Host di destinazione trap**

  Specifica il nome host o l'indirizzo IP (IPv4 o IPv6) che riceve i trap SNMP inviati dal server di gestione. Per specificare più destinazioni di trap, separare ciascun host con una virgola.

  > Tutte le altre impostazioni SNMP, ad esempio "versione" e "porta in uscita", devono essere identiche per tutti gli host dell'elenco.

- **Outbound Trap Port** (porta trap in uscita)

  Specifica la porta attraverso la quale il server SNMP riceve i trap inviati dal server di gestione.

  Il valore predefinito è 162.

- **Comunità**

  Stringa di comunità per accedere all'host.

- **ID motore**

  Specifica l'identificatore univoco dell'agente SNMP e viene generato automaticamente dal server di gestione. L'ID motore è disponibile con SNMP versione 3, SNMP versione 3 con autenticazione e SNMP versione 3 con autenticazione e crittografia.

- **Nome utente**

Specifica il nome utente SNMP. Il nome utente è disponibile con SNMP versione 3, SNMP versione 3 con autenticazione e SNMP versione 3 con autenticazione e crittografia.

- **Protocollo di autenticazione**

  Specifica il protocollo utilizzato per autenticare un utente. Le opzioni del protocollo includono MD5 e SHA. MD5 è il valore predefinito. Il protocollo di autenticazione è disponibile con SNMP versione 3 con autenticazione e SNMP versione 3 con autenticazione e crittografia.

- **Password di autenticazione**

  Specifica la password utilizzata per l'autenticazione di un utente. La password di autenticazione è disponibile con SNMP versione 3 con autenticazione e SNMP versione 3 con autenticazione e crittografia.

- **Protocollo sulla privacy**

  Specifica il protocollo di privacy utilizzato per crittografare i messaggi SNMP. Le opzioni del protocollo includono AES 128 e DES. Il valore predefinito è AES 128. Il protocollo Privacy è disponibile con SNMP versione 3 con autenticazione e crittografia.

- **Password privacy**

  Specifica la password quando si utilizza il protocollo di privacy. La password per la privacy è disponibile con SNMP versione 3 con autenticazione e crittografia.

Per ulteriori informazioni sugli oggetti e i trap SNMP, è possibile scaricare "MIB Active IQ Unified Manager" Dal NetApp Support Site.

Pagina dell'inventario di Event Management

La pagina inventario gestione eventi consente di visualizzare un elenco degli eventi correnti e delle relative proprietà. È possibile eseguire attività come il riconoscimento, la risoluzione e l'assegnazione di eventi. È inoltre possibile aggiungere un avviso per eventi specifici.

Le informazioni contenute in questa pagina vengono aggiornate automaticamente ogni 5 minuti per garantire la visualizzazione dei nuovi eventi più recenti.

Componenti del filtro

Consente di personalizzare le informazioni visualizzate nell'elenco degli eventi. È possibile perfezionare l'elenco degli eventi visualizzati utilizzando i seguenti componenti:

- Menu View (Visualizza) per selezionare da un elenco predefinito di filtri selezionati.

  Sono inclusi elementi come tutti gli eventi attivi (nuovi e riconosciuti), gli eventi delle performance attivi, gli eventi assegnati a me (l'utente connesso) e tutti gli eventi generati durante tutte le finestre di manutenzione.

- Riquadro di ricerca per perfezionare l'elenco degli eventi immettendo termini completi o parziali.
- Pulsante Filter (filtro) che avvia il pannello Filters (filtri), in modo da poter selezionare da ogni campo e attributo di campo disponibile per perfezionare l'elenco degli eventi.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Assegna a**

  Consente di selezionare l'utente a cui è assegnato l'evento. Quando si assegna un evento a un utente, il nome utente e l'ora in cui è stato assegnato l'evento vengono aggiunti all'elenco degli eventi selezionati.

  - Io

    Assegna l'evento all'utente attualmente connesso.

  - Un altro utente

    Visualizza la finestra di dialogo Assegna proprietario, che consente di assegnare o riassegnare l'evento ad altri utenti. È inoltre possibile annullare l'assegnazione degli eventi lasciando vuoto il campo Ownership (proprietà).

- **Riconoscere**

  Riconosce gli eventi selezionati.

  Quando si riconosce un evento, il nome utente e l'ora in cui l'evento è stato confermato vengono aggiunti all'elenco degli eventi selezionati. Quando si riconosce un evento, si è responsabili della gestione di tale evento.

  Non è possibile riconoscere gli eventi relativi alle informazioni.

- **Contrassegna come risolto**

  Consente di modificare lo stato dell'evento in Resolved (risolto).

  Quando si risolve un evento, il nome utente e l'ora in cui l'evento è stato risolto vengono aggiunti all'elenco degli eventi selezionati. Dopo aver eseguito un'azione correttiva per l'evento, è necessario contrassegnare l'evento come risolto.

- **Aggiungi avviso**

  Visualizza la finestra di dialogo Aggiungi avviso, che consente di aggiungere avvisi per gli eventi selezionati.

- **Report**

  Consente di esportare i dettagli della vista dell'evento corrente in un file con valori separati da virgola (.csv) o in un documento PDF.

- **Mostra/Nascondi selettore colonna**

  Consente di scegliere le colonne visualizzate nella pagina e di selezionare l'ordine in cui vengono visualizzate.

Elenco degli eventi

Visualizza i dettagli di tutti gli eventi ordinati in base all'ora di attivazione.

Per impostazione predefinita, viene visualizzata la vista All Active events (tutti gli eventi attivi) che mostra gli eventi New (nuovi) e Acknowledged (confermati) relativi ai sette giorni precedenti che hanno un livello di impatto dell'incidente o del rischio.

- **Tempo di attivazione**

  L'ora in cui è stato generato l'evento.

- **Severità**

  La severità dell'evento: Critica ( ), errore ( ), Avviso ( ) E informazioni ( ).

- **Stato**

  Lo stato dell'evento: Nuovo, riconosciuto, risolto o obsoleto.

- **Livello di impatto**

  Il livello di impatto dell'evento: Incidente, rischio, evento o aggiornamento.

- **Area di impatto**

  L'area di impatto dell'evento: Disponibilità, capacità, performance, protezione, configurazione, O sicurezza.

- **Nome**

  Il nome dell'evento. È possibile selezionare il nome per visualizzare la pagina Dettagli evento relativa all'evento.

- **Origine**

  Il nome dell'oggetto in cui si è verificato l'evento. È possibile selezionare il nome per visualizzare la pagina dei dettagli relativi allo stato di salute o alle prestazioni dell'oggetto.

  Quando si verifica una violazione della policy QoS condivisa, in questo campo viene visualizzato solo l'oggetto workload che consuma il maggior numero di IOPS o MB/s. I carichi di lavoro aggiuntivi che utilizzano questa policy vengono visualizzati nella pagina Dettagli evento.

- **Tipo di origine**

  Il tipo di oggetto (ad esempio Storage VM, Volume o Qtree) a cui è associato l'evento.

- **Assegnato a**

  Il nome dell'utente a cui è assegnato l'evento.

- **Origine evento**

  Sia che l'evento sia stato originato dal "portale Active IQ" o direttamente da "Active IQ Unified Manager".

- **Nome annotazione**

  Il nome dell'annotazione assegnata all'oggetto di storage.

- **Note**

Il numero di note aggiunte per un evento.

- **Giorni in sospeso**

  Il numero di giorni trascorsi dalla generazione iniziale dell'evento.

- **Tempo assegnato**

  Il tempo trascorso dall'assegnazione dell'evento a un utente. Se il tempo trascorso supera una settimana, viene visualizzata l'indicazione dell'ora in cui l'evento è stato assegnato a un utente.

- **Riconosciuto da**

  Il nome dell'utente che ha confermato l'evento. Il campo è vuoto se l'evento non viene riconosciuto.

- **Tempo riconosciuto**

  Il tempo trascorso dalla conferma dell'evento. Se il tempo trascorso supera una settimana, viene visualizzata l'indicazione dell'ora in cui l'evento è stato confermato.

- **Risolto da**

  Il nome dell'utente che ha risolto l'evento. Il campo è vuoto se l'evento non viene risolto.

- **Tempo di risoluzione**

  Il tempo trascorso da quando l'evento è stato risolto. Se il tempo trascorso supera una settimana, viene visualizzata l'indicazione dell'ora in cui l'evento è stato risolto.

- **Tempo obsoleto**

  L'ora in cui lo stato dell'evento è diventato obsoleto.

Pagina dei dettagli dell'evento

Dalla pagina Dettagli evento è possibile visualizzare i dettagli di un evento selezionato, ad esempio la gravità dell'evento, il livello di impatto, l'area di impatto e l'origine dell'evento. È inoltre possibile visualizzare ulteriori informazioni sulle possibili soluzioni per risolvere il problema.

- **Nome evento**

  Il nome dell'evento e l'ora dell'ultima visualizzazione dell'evento.

  Per gli eventi che non riguardano le performance, mentre l'evento si trova nello stato New (nuovo) o Acknowledged (confermato), le ultime informazioni visualizzate non sono note e pertanto nascoste.

- **Descrizione dell'evento**

  Una breve descrizione dell'evento.

  In alcuni casi, nella descrizione dell'evento viene indicato un motivo per l'attivazione dell'evento.

- **Componente in conflitto**

Per gli eventi di performance dinamiche, questa sezione visualizza le icone che rappresentano i componenti logici e fisici del cluster. Se un componente è in conflitto, la relativa icona viene cerchiata ed evidenziata in rosso.

Per una descrizione dei componenti visualizzati, consulta la sezione *componenti del cluster e perché possono essere in conflitto*.

Le sezioni informazioni evento, Diagnosi del sistema e azioni consigliate sono descritte in altri argomenti.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- Icona **Note**

  Consente di aggiungere o aggiornare una nota sull'evento e di rivedere tutte le note lasciate da altri utenti.

Menu azioni

- **Assegna a me**

  Assegna l'evento all'utente.

- **Assegna ad altri**

  Apre la finestra di dialogo Assegna proprietario, che consente di assegnare o riassegnare l'evento ad altri utenti.

  Quando si assegna un evento a un utente, il nome dell'utente e l'ora in cui l'evento è stato assegnato vengono aggiunti all'elenco degli eventi selezionati.

  È inoltre possibile annullare l'assegnazione degli eventi lasciando vuoto il campo Ownership (proprietà).

- **Riconoscere**

  Riconosce gli eventi selezionati in modo da non continuare a ricevere notifiche di avviso ripetute.

  Quando si riconosce un evento, il nome utente e l'ora in cui si è confermato l'evento vengono aggiunti all'elenco degli eventi (riconosciuti da) per gli eventi selezionati. Quando si riconosce un evento, si assume la responsabilità della gestione di tale evento.

- **Contrassegna come risolto**

  Consente di modificare lo stato dell'evento in Resolved (risolto).

  Quando si risolve un evento, il nome utente e l'ora in cui l'evento è stato risolto vengono aggiunti all'elenco degli eventi (risolti da) per gli eventi selezionati. Dopo aver eseguito un'azione correttiva per l'evento, è necessario contrassegnare l'evento come risolto.

- **Aggiungi avviso**

  Visualizza la finestra di dialogo Aggiungi avviso, che consente di aggiungere un avviso per l'evento selezionato.

Visualizzazione della sezione informazioni evento

La sezione informazioni evento della pagina Dettagli evento consente di visualizzare i dettagli relativi a un evento selezionato, ad esempio la gravità, il livello di impatto, l'area di impatto e l'origine dell'evento.

I campi non applicabili al tipo di evento sono nascosti. È possibile visualizzare i seguenti dettagli dell'evento:

- **Tempo di attivazione dell'evento**

  L'ora in cui è stato generato l'evento.

- **Stato**

  Lo stato dell'evento: Nuovo, riconosciuto, risolto o obsoleto.

- **Causa obsoleta**

  Le azioni che hanno causato l'obsoleto dell'evento, ad esempio, il problema è stato risolto.

- **Durata evento**

  Per gli eventi attivi (nuovi e riconosciuti), si tratta del tempo che intercorre tra il rilevamento e l'ultima analisi dell'evento. Per gli eventi obsoleti, si tratta del tempo che intercorre tra il rilevamento e la risoluzione dell'evento.

  Questo campo viene visualizzato per tutti gli eventi relativi alle performance e per altri tipi di eventi solo dopo che sono stati risolti o resi obsoleti.

- **Ultimo visto**

  La data e l'ora in cui l'evento è stato considerato come attivo per l'ultima volta.

  Per gli eventi relativi alle performance, questo valore potrebbe essere più recente del tempo di attivazione dell'evento, in quanto questo campo viene aggiornato dopo ogni nuova raccolta di dati relativi alle performance finché l'evento è attivo. Per altri tipi di eventi, quando si trova nello stato nuovo o confermato, questo contenuto non viene aggiornato e il campo viene quindi nascosto.

- **Severità**

  La severità dell'evento: Critica ( ), errore ( ), Avviso ( ) E informazioni ( ).

- **Livello di impatto**

  Il livello di impatto dell'evento: Incidente, rischio, evento o aggiornamento.

- **Area di impatto**

  L'area di impatto dell'evento: Disponibilità, capacità, performance, protezione, configurazione, O sicurezza.

- **Origine**

  Il nome dell'oggetto in cui si è verificato l'evento.

  Quando si visualizzano i dettagli di un evento di policy QoS condivisa, in questo campo vengono elencati fino a tre degli oggetti del carico di lavoro che consumano il maggior numero di IOPS o Mbps.

È possibile fare clic sul collegamento del nome di origine per visualizzare la pagina dei dettagli relativi allo stato o alle prestazioni dell'oggetto.

- **Annotazioni di origine**

  Visualizza il nome e il valore dell'annotazione per l'oggetto a cui è associato l'evento.

  Questo campo viene visualizzato solo per gli eventi di integrità su cluster, SVM e volumi.

- **Gruppi di origine**

  Visualizza i nomi di tutti i gruppi di cui è membro l'oggetto interessato.

  Questo campo viene visualizzato solo per gli eventi di integrità su cluster, SVM e volumi.

- **Tipo di origine**

  Il tipo di oggetto (ad esempio, SVM, Volume o Qtree) a cui è associato l'evento.

- **Sul cluster**

  Il nome del cluster in cui si è verificato l'evento.

  È possibile fare clic sul collegamento del nome del cluster per visualizzare la pagina dei dettagli relativi allo stato o alle prestazioni del cluster.

- **Conteggio oggetti interessati**

  Il numero di oggetti interessati dall'evento.

  È possibile fare clic sul collegamento Object (oggetto) per visualizzare la pagina di inventario contenente gli oggetti attualmente interessati dall'evento.

  Questo campo viene visualizzato solo per gli eventi relativi alle performance.

- **Volumi interessati**

  Il numero di volumi interessati da questo evento.

  Questo campo viene visualizzato solo per gli eventi di performance su nodi o aggregati.

- **Criterio attivato**

  Il nome del criterio di soglia che ha emesso l'evento.

  Per visualizzare i dettagli del criterio di soglia, spostare il cursore del mouse sul nome del criterio. Per i criteri QoS adattivi vengono visualizzati anche il criterio, la dimensione del blocco e il tipo di allocazione (spazio allocato o spazio utilizzato) definiti.

  Questo campo viene visualizzato solo per gli eventi relativi alle performance.

- **ID regola**

  Per gli eventi della piattaforma Active IQ, si tratta del numero della regola che è stata attivata per generare l'evento.

- **Riconosciuto da**

  Il nome della persona che ha confermato l'evento e l'ora in cui l'evento è stato riconosciuto.

- **Risolto da**

  Il nome della persona che ha risolto l'evento e l'ora in cui l'evento è stato risolto.

- **Assegnato a**

  Il nome della persona assegnata all'evento.

- **Impostazioni avvisi**

  Vengono visualizzate le seguenti informazioni sugli avvisi:

  - Se non sono presenti avvisi associati all'evento selezionato, viene visualizzato il collegamento **Add alert** (Aggiungi avviso).

    Per aprire la finestra di dialogo Aggiungi avviso, fare clic sul collegamento.

  - Se all'evento selezionato è associato un avviso, viene visualizzato il nome dell'avviso.

    Per aprire la finestra di dialogo Modifica avviso, fare clic sul collegamento.

  - Se all'evento selezionato sono associati più avvisi, viene visualizzato il numero di avvisi.

    È possibile aprire la pagina Configurazione avvisi facendo clic sul collegamento per visualizzare ulteriori dettagli su tali avvisi.

  Gli avvisi disattivati non vengono visualizzati.

- **Ultima notifica inviata**

  La data e l'ora in cui è stata inviata la notifica di avviso più recente.

- **Invia per**

  Meccanismo utilizzato per inviare la notifica di avviso: Email o trap SNMP.

- **Esecuzione script precedente**

  Il nome dello script eseguito al momento della generazione dell'avviso.

Viene visualizzata la sezione azioni consigliate

La sezione azioni consigliate della pagina Dettagli evento fornisce i possibili motivi dell'evento e suggerisce alcune azioni per tentare di risolvere l'evento autonomamente. Le azioni suggerite sono personalizzate in base al tipo di evento o al tipo di soglia violato.

Questa area viene visualizzata solo per alcuni tipi di eventi.

In alcuni casi, nella pagina sono disponibili collegamenti **Help** che fanno riferimento a informazioni aggiuntive per molte azioni suggerite, incluse le istruzioni per eseguire un'azione specifica. Alcune delle azioni possono comportare l'utilizzo di Unified Manager, Gestore di sistema di ONTAP, OnCommand Workflow Automation,

comandi CLI di ONTAP o una combinazione di questi strumenti.

Le azioni suggerite in questo documento devono essere considerate solo una guida per la risoluzione di questo evento. L'azione intrapresa per risolvere questo evento deve basarsi sul contesto dell'ambiente.

Se si desidera analizzare più dettagliatamente l'oggetto e l'evento, fare clic sul pulsante **Analyze workload** (analizza carico di lavoro) per visualizzare la pagina workload Analysis (analisi del carico di lavoro).

Unified Manager è in grado di diagnosticare a fondo alcuni eventi e fornire una singola risoluzione. Quando disponibili, queste risoluzioni vengono visualizzate con il pulsante **Correggi**. Fare clic su questo pulsante per consentire a Unified Manager di risolvere il problema che causa l'evento.

Per gli eventi della piattaforma Active IQ, questa sezione potrebbe contenere un link a un articolo della Knowledge base di NetApp, se disponibile, che descrive il problema e le possibili soluzioni. Nei siti senza accesso alla rete esterna, viene aperto localmente un PDF dell'articolo della Knowledge base; il PDF fa parte del file di regole che viene scaricato manualmente nell'istanza di Unified Manager.

Viene visualizzata la sezione Diagnosi del sistema

La sezione Diagnosi del sistema della pagina Dettagli evento fornisce informazioni utili per diagnosticare i problemi che potrebbero essere stati responsabili dell'evento.

Quest'area viene visualizzata solo per alcuni eventi.

Alcuni eventi relativi alle performance forniscono grafici rilevanti per l'evento specifico che è stato attivato. In genere, questo include un grafico IOPS o Mbps e un grafico di latenza per i dieci giorni precedenti. Se disposti in questo modo, puoi vedere quali componenti dello storage influenzano maggiormente la latenza o sono influenzati dalla latenza, quando l'evento è attivo.

Per gli eventi di performance dinamiche, vengono visualizzati i seguenti grafici:

- Latenza del carico di lavoro - Visualizza la cronologia della latenza per i carichi di lavoro più importanti delle vittime, dei carichi di lavoro più voluminosi o degli squali nel componente in conflitto.
- Workload Activity (attività del carico di lavoro) - Visualizza i dettagli sull'utilizzo del carico di lavoro del componente del cluster in conflitto.
- Resource Activity (attività risorsa) - Visualizza le statistiche cronologiche delle performance per il componente del cluster in conflitto.

Altri grafici vengono visualizzati quando alcuni componenti del cluster sono in conflitto.

Altri eventi forniscono una breve descrizione del tipo di analisi che il sistema sta eseguendo sull'oggetto di storage. In alcuni casi ci saranno una o più righe, una per ogni componente analizzato, per policy di performance definite dal sistema che analizzano più contatori di performance. In questo scenario, accanto alla diagnosi viene visualizzata un'icona verde o rossa per indicare se è stato rilevato o meno un problema in quella particolare diagnosi.

Pagina Event Setup

La pagina impostazione eventi visualizza l'elenco degli eventi disattivati e fornisce informazioni quali il tipo di oggetto associato e la gravità dell'evento. È inoltre possibile eseguire attività come la disattivazione o l'abilitazione di eventi a livello globale.

È possibile accedere a questa pagina solo se si dispone del ruolo di amministratore dell'applicazione o di

amministratore dello storage.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività per gli eventi selezionati:

- **Disattiva**

  Consente di aprire la finestra di dialogo Disable Events (Disattiva eventi), che può essere utilizzata per disattivare gli eventi.

- **Enable** (attiva)

  Attiva gli eventi selezionati che si era scelto di disattivare in precedenza.

- **Regole di caricamento**

  Apre la finestra di dialogo regole di caricamento, che consente ai siti senza accesso alla rete esterna di caricare manualmente il file di regole Active IQ in Unified Manager. Le regole vengono eseguite in base ai messaggi AutoSupport del cluster per generare eventi per la configurazione del sistema, il cablaggio, le Best practice e la disponibilità come definiti dalla piattaforma Active IQ.

- **Iscriviti agli eventi EMS**

  Apre la finestra di dialogo Iscriviti agli eventi EMS, che consente di iscriversi per ricevere eventi specifici del sistema di gestione degli eventi (EMS) dai cluster monitorati. EMS raccoglie informazioni sugli eventi che si verificano nel cluster. Quando si riceve una notifica per un evento EMS sottoscritto, viene generato un evento Unified Manager con la severità appropriata.

Vista elenco

La vista elenco visualizza (in formato tabulare) le informazioni sugli eventi disattivati. È possibile utilizzare i filtri di colonna per personalizzare i dati visualizzati.

- **Evento**

  Visualizza il nome dell'evento disattivato.

- **Severità**

  Visualizza la severità dell'evento. La gravità può essere critica, errore, Avviso o informazioni.

- **Tipo di origine**

  Visualizza il tipo di origine per cui viene generato l'evento.

Finestra di dialogo Disattiva eventi

La finestra di dialogo Disable Events (Disattiva eventi) visualizza l'elenco dei tipi di evento per i quali è possibile disattivare gli eventi. È possibile disattivare gli eventi per un tipo di evento in base a una determinata severità o a una serie di eventi.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Area Event Properties (Proprietà evento

L'area Proprietà evento specifica le seguenti proprietà dell'evento:

- **Severità evento**

  Consente di selezionare gli eventi in base al tipo di severità, che può essere critico, errore, Avviso o informazioni.

- **Il nome dell'evento contiene**

  Consente di filtrare gli eventi il cui nome contiene i caratteri specificati.

- **Eventi corrispondenti**

  Visualizza l'elenco degli eventi corrispondenti al tipo di severità dell'evento e alla stringa di testo specificata.

- **Disattiva eventi**

  Visualizza l'elenco degli eventi selezionati per la disattivazione.

  Viene inoltre visualizzata la severità dell'evento insieme al nome dell'evento.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività per gli eventi selezionati:

- **Salva e chiudi**

  Disattiva il tipo di evento e chiude la finestra di dialogo.

- **Annulla**

  Elimina le modifiche e chiude la finestra di dialogo.

Gestione degli avvisi

È possibile configurare gli avvisi in modo che inviino automaticamente una notifica quando si verificano eventi o eventi specifici di determinati tipi di gravità. È inoltre possibile associare un avviso a uno script eseguito quando viene attivato un avviso.

Quali sono gli avvisi

Mentre gli eventi si verificano continuamente, Unified Manager genera un avviso solo quando un evento soddisfa i criteri di filtro specificati. È possibile scegliere gli eventi per i quali devono essere generati gli avvisi, ad esempio quando viene superata una soglia di spazio o un oggetto non è in linea. È inoltre possibile associare un avviso a uno script eseguito quando viene attivato un avviso.

I criteri di filtro includono la classe di oggetti, il nome o la severità dell'evento.

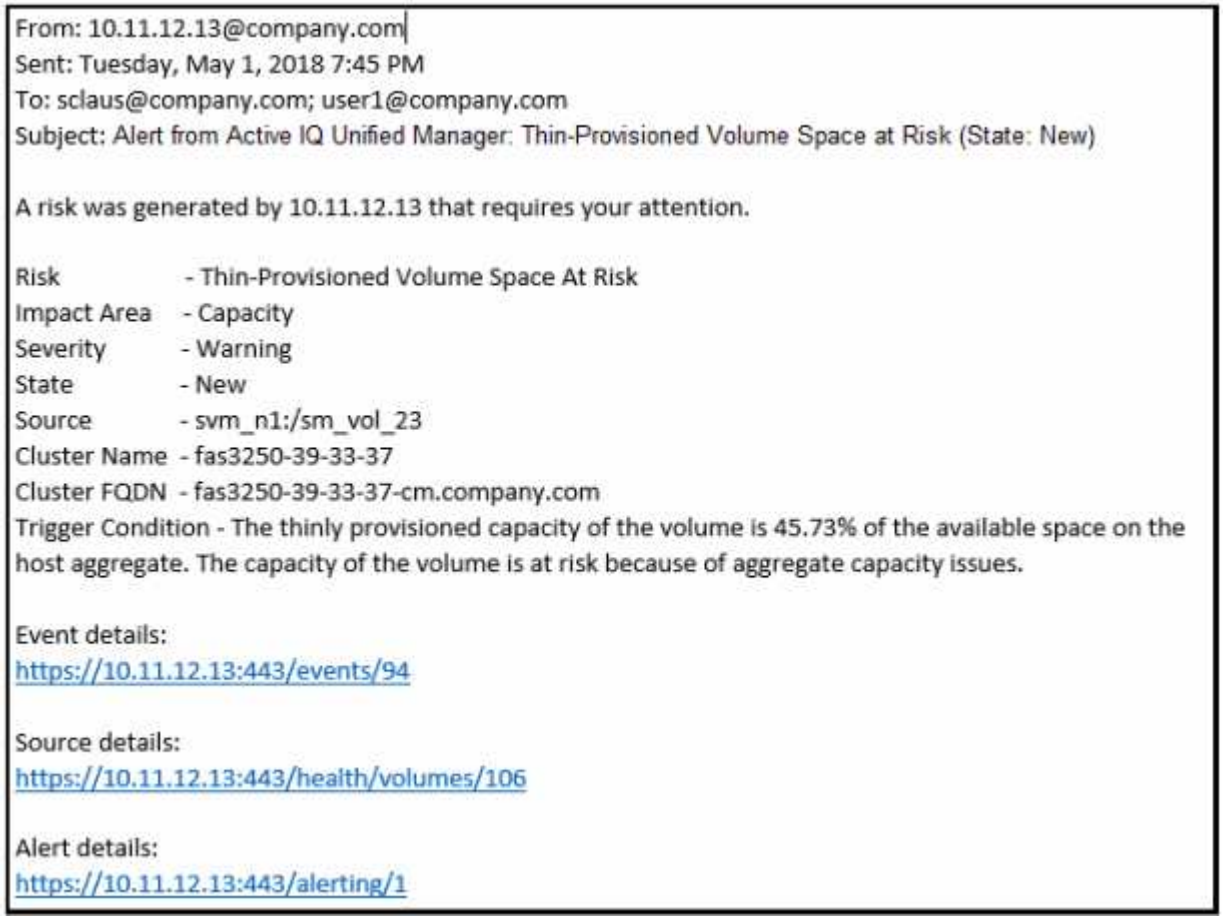
Quali informazioni sono contenute in un messaggio di posta elettronica di avviso

Le email di avviso di Unified Manager forniscono il tipo di evento, la severità dell'evento, il nome della policy o della soglia che è stata violata per causare l'evento e una descrizione dell'evento. Il messaggio di posta elettronica fornisce inoltre un collegamento ipertestuale per ciascun evento che consente di visualizzare la pagina dei dettagli dell'evento nell'interfaccia utente.

Le email di avviso vengono inviate a tutti gli utenti che si sono abbonati per ricevere avvisi.

Se un contatore di performance o un valore di capacità presenta una grande modifica durante un periodo di raccolta, potrebbe causare l'attivazione contemporanea di un evento critico e di un avviso per la stessa policy di soglia. In questo caso, è possibile ricevere un'e-mail per l'evento di avviso e un'email per l'evento critico. In quanto Unified Manager ti consente di iscriverti separatamente per ricevere avvisi in caso di avvisi e violazioni di soglia critiche.

Di seguito è riportato un esempio di messaggio di avviso:


From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

Aggiunta di avvisi

È possibile configurare gli avvisi in modo che notifichino quando viene generato un determinato evento. È possibile configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un particolare tipo di severità. È possibile specificare la frequenza con cui si desidera ricevere una notifica e associare uno script all'avviso.

Cosa ti serve

- Per consentire al server Active IQ Unified Manager di utilizzare queste impostazioni per inviare notifiche agli utenti quando viene generato un evento, è necessario aver configurato le impostazioni di notifica, ad esempio l'indirizzo e-mail dell'utente, il server SMTP e l'host trap SNMP.
- È necessario conoscere le risorse e gli eventi per i quali si desidera attivare l'avviso, nonché i nomi utente o gli indirizzi e-mail degli utenti che si desidera notificare.
- Se si desidera eseguire uno script in base all'evento, è necessario aggiungere lo script a Unified Manager utilizzando la pagina script.
- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a creare un avviso dalla pagina Configurazione avviso, come descritto di seguito.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina **Alert Setup**, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo **Aggiungi avviso**, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.
4. Fare clic su **risorse** e selezionare le risorse da includere o escludere dall'avviso.

   È possibile impostare un filtro specificando una stringa di testo nel campo **Nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse corrispondenti alla regola di filtro. La stringa di testo specificata fa distinzione tra maiuscole e minuscole.

   Se una risorsa è conforme alle regole di inclusione ed esclusione specificate, la regola di esclusione ha la precedenza sulla regola di inclusione e l'avviso non viene generato per gli eventi correlati alla risorsa esclusa.

5. Fare clic su **Eventi** e selezionare gli eventi in base al nome dell'evento o al tipo di severità per cui si desidera attivare un avviso.

   Per selezionare più eventi, premere il tasto Ctrl mentre si effettuano le selezioni.

6. Fare clic su **azioni**, selezionare gli utenti che si desidera notificare, scegliere la frequenza di notifica, scegliere se inviare una trap SNMP al ricevitore della trap e assegnare uno script da eseguire quando viene generato un avviso.

   Se si modifica l'indirizzo di posta elettronica specificato per l'utente e si riapre l'avviso per la modifica, il campo Nome appare vuoto perché l'indirizzo di posta elettronica modificato non è più associato all'utente precedentemente selezionato. Inoltre, se l'indirizzo e-mail dell'utente selezionato è stato modificato dalla pagina utenti, l'indirizzo e-mail modificato non viene aggiornato per l'utente selezionato.

   È inoltre possibile scegliere di inviare una notifica agli utenti tramite trap SNMP.

7. Fare clic su **Save** (Salva).

Esempio di aggiunta di un avviso

Questo esempio mostra come creare un avviso che soddisfi i seguenti requisiti:

- Nome avviso: HealthTest
- Risorse: Include tutti i volumi il cui nome contiene "abc" ed esclude tutti i volumi il cui nome contiene "xyz"
- Eventi: Include tutti gli eventi sanitari critici
- Azioni: Include "sample@domain.com", uno script "Test" e l'utente deve ricevere una notifica ogni 15 minuti

Nella finestra di dialogo Aggiungi avviso, attenersi alla seguente procedura:

1. Fare clic su **Nome** e digitare **`HealthTest`** Nel campo **Nome avviso**.
2. Fare clic su **Resources** (risorse) e nella scheda include (Includi) selezionare **Volumes** (volumi) dall'elenco a discesa.
   a. Invio **`abc`** Nel campo **Nome contiene** per visualizzare i volumi il cui nome contiene "abc".
   b. Selezionare **<<All Volumes whose name contains 'abc'>>** dall'area risorse disponibili e spostarla nell'area risorse selezionate.
   c. Fare clic su **Escludi** e digitare **`xyz`** Nel campo **il nome contiene**, quindi fare clic su **Aggiungi**.
3. Fare clic su **Eventi** e selezionare **critico** dal campo gravità evento.
4. Selezionare **All Critical Events** (tutti gli eventi critici) dall'area Matching Events (Eventi corrispondenti) e spostarla nell'area Selected Events (Eventi selezionati).
5. Fare clic su **azioni** e digitare **`sample@domain.com`** Nel campo Alert these users (Avvisa questi utenti).
6. Selezionare **promemoria ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

   È possibile configurare un avviso per inviare ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario determinare l'ora in cui la notifica dell'evento è attiva per l'avviso.
7. Nel menu Select script to Execute (Seleziona script da eseguire), selezionare **Test** script.
8. Fare clic su **Save** (Salva).

Linee guida per l'aggiunta di avvisi

È possibile aggiungere avvisi in base a una risorsa, ad esempio un cluster, un nodo, un aggregato o un volume, nonché eventi di un particolare tipo di severità. Come procedura consigliata, è possibile aggiungere un avviso per qualsiasi oggetto critico dopo aver aggiunto il cluster a cui appartiene l'oggetto.

È possibile utilizzare le seguenti linee guida e considerazioni per creare avvisi per gestire i sistemi in modo efficace:

- Descrizione dell'avviso

  È necessario fornire una descrizione per l'avviso, in modo che possa essere utile per tenere traccia degli avvisi in modo efficace.

- Risorse

  È necessario decidere quale risorsa fisica o logica richiede un avviso. È possibile includere ed escludere le

risorse, in base alle esigenze. Ad esempio, se si desidera monitorare attentamente gli aggregati configurando un avviso, è necessario selezionare gli aggregati richiesti dall'elenco delle risorse.

Se si seleziona una categoria di risorse, ad esempio **<<All User or Group Quotas>>**, quindi riceverai avvisi per tutti gli oggetti della categoria.

> La selezione di un cluster come risorsa non seleziona automaticamente gli oggetti di storage all'interno di quel cluster. Ad esempio, se si crea un avviso per tutti gli eventi critici per tutti i cluster, si riceveranno avvisi solo per gli eventi critici del cluster. Non riceverai avvisi per eventi critici su nodi, aggregati e così via.

- Severità dell'evento

  È necessario decidere se un evento con un tipo di severità specificato (critico, errore, Avviso) deve attivare l'avviso e, in caso affermativo, quale tipo di severità.

- Eventi selezionati

  Se si aggiunge un avviso in base al tipo di evento generato, è necessario decidere quali eventi richiedono un avviso.

  Se si seleziona un livello di gravità dell'evento, ma non si selezionano singoli eventi (se si lascia vuota la colonna "Eventi selezionati"), si riceveranno avvisi per tutti gli eventi della categoria.

- Azioni

  È necessario fornire i nomi utente e gli indirizzi e-mail degli utenti che ricevono la notifica. È inoltre possibile specificare un trap SNMP come modalità di notifica. È possibile associare gli script a un avviso in modo che vengano eseguiti quando viene generato un avviso.

- Frequenza delle notifiche

  È possibile configurare un avviso per inviare ripetutamente una notifica ai destinatari per un periodo di tempo specificato. È necessario determinare l'ora in cui la notifica dell'evento è attiva per l'avviso. Se si desidera che la notifica dell'evento venga ripetuta fino alla conferma dell'evento, è necessario determinare la frequenza con cui si desidera che la notifica venga ripetuta.

- Esegui script

  È possibile associare lo script a un avviso. Lo script viene eseguito quando viene generato l'avviso.

Aggiunta di avvisi per eventi relativi alle performance

È possibile configurare gli avvisi per singoli eventi relativi alle performance esattamente come qualsiasi altro evento ricevuto da Unified Manager. Inoltre, se si desidera trattare tutti gli eventi relativi alle performance allo stesso modo e inviare un'e-mail alla stessa persona, è possibile creare un singolo avviso per notificare l'attivazione di eventi critici o di avviso relativi alle performance.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

L'esempio seguente mostra come creare un evento per tutti gli eventi critici di latenza, IOPS e Mbps. È possibile utilizzare questa stessa metodologia per selezionare gli eventi da tutti i contatori delle prestazioni e per tutti gli eventi di avviso.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina **Alert Setup**, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo **Aggiungi avviso**, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.
4. Non selezionare alcuna risorsa nella pagina **risorse**.

   Poiché non sono selezionate risorse, l'avviso viene applicato a tutti i cluster, aggregati, volumi e così via, per i quali vengono ricevuti questi eventi.

5. Fare clic su **Eventi** ed eseguire le seguenti operazioni:
   a. Nell'elenco gravità evento, selezionare **critico**.
   b. Nel campo Nome evento contiene, immettere **`latency`**, quindi fare clic sulla freccia per selezionare tutti gli eventi corrispondenti.
   c. Nel campo Nome evento contiene, immettere **`iops`**, quindi fare clic sulla freccia per selezionare tutti gli eventi corrispondenti.
   d. Nel campo Nome evento contiene, immettere **`mbps`**, quindi fare clic sulla freccia per selezionare tutti gli eventi corrispondenti.
6. Fare clic su **azioni**, quindi selezionare il nome dell'utente che riceverà l'e-mail di avviso nel campo **Avvisa questi utenti**.
7. Configurare tutte le altre opzioni di questa pagina per l'emissione di trap SNMP e l'esecuzione di uno script.
8. Fare clic su **Save** (Salva).

Test degli avvisi

È possibile verificare che un avviso sia stato configurato correttamente. Quando viene attivato un evento, viene generato un avviso e inviato un messaggio di posta elettronica ai destinatari configurati. È possibile verificare se la notifica viene inviata e se lo script viene eseguito utilizzando l'avviso di test.

Cosa ti serve

- È necessario aver configurato le impostazioni di notifica, ad esempio l'indirizzo e-mail dei destinatari, il server SMTP e il trap SNMP.

  Il server Unified Manager può utilizzare queste impostazioni per inviare notifiche agli utenti quando viene generato un evento.

- È necessario aver assegnato uno script e configurato lo script per l'esecuzione quando viene generato l'avviso.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina **Alert Setup**, selezionare l'avviso che si desidera sottoporre a test, quindi fare clic su **Test**.

   Viene inviato un messaggio e-mail di avviso di test agli indirizzi e-mail specificati durante la creazione dell'avviso.

Attivazione e disattivazione degli avvisi per gli eventi risolti e obsoleti

Per tutti gli eventi configurati per l'invio di avvisi, viene inviato un messaggio di avviso quando tali eventi passano attraverso tutti gli stati disponibili: Nuovo, confermato, risolto e obsoleto. Se non si desidera ricevere avvisi per gli eventi quando si spostano negli stati Resolved (risolto) e obsoleto, è possibile configurare un'impostazione globale per eliminare tali avvisi.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Per impostazione predefinita, gli avvisi non vengono inviati per gli eventi quando si spostano negli stati Resolved (risolto) e obsoleto.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina **Alert Setup**, eseguire una delle seguenti operazioni utilizzando il dispositivo di scorrimento accanto alla voce **Alerts for Resolved and obsolete events** (Avvisi per eventi risolti e obsoleti):

Per…	Eseguire questa operazione…
Interrompere l'invio di avvisi in caso di risoluzione o obsoleto degli eventi	Spostare il dispositivo di scorrimento verso sinistra
Inizia a inviare avvisi quando gli eventi vengono risolti o resi obsoleti	Spostare il dispositivo di scorrimento verso destra

Esclusione dei volumi di destinazione per il disaster recovery dalla generazione di avvisi

Quando si configurano gli avvisi di volume, è possibile specificare una stringa nella finestra di dialogo Avviso che identifica un volume o un gruppo di volumi. Tuttavia, se è stato configurato il disaster recovery per le SVM, i volumi di origine e di destinazione hanno lo stesso nome, in modo da ricevere avvisi per entrambi i volumi.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile disattivare gli avvisi per i volumi di destinazione del disaster recovery escludendo i volumi che hanno il nome della SVM di destinazione. Ciò è possibile perché l'identificatore per gli eventi del volume contiene sia il nome SVM che il nome del volume nel formato "<svm_name>:/<volume_name>".

L’esempio seguente mostra come creare avvisi per il volume "vol1" sulla SVM primaria "vs1", ma esclude che l’avviso venga generato su un volume con lo stesso nome su SVM "vs1-dr".

Nella finestra di dialogo Aggiungi avviso, attenersi alla seguente procedura:

Fasi

1. Fare clic su **Nome** e immettere un nome e una descrizione per l’avviso.
2. Fare clic su **risorse**, quindi selezionare la scheda **Includi**.
   a. Selezionare **Volume** dall’elenco a discesa, quindi premere Invio `vol1` Nel campo **Nome contiene** per visualizzare i volumi il cui nome contiene "vol1".
   b. Selezionare **<<All Volumes whose name contains 'vol1'>>** dall’area **risorse disponibili** e spostarla nell’area **risorse selezionate**.
3. Selezionare la scheda **Escludi**, quindi **Volume** e premere Invio `vs1-dr` Nel campo **il nome contiene**, quindi fare clic su **Aggiungi**.

   Ciò esclude la generazione dell’avviso per il volume "vol1" su SVM "vs1-dr".
4. Fare clic su **Eventi** e selezionare l’evento o gli eventi che si desidera applicare al volume o ai volumi.
5. Fare clic su **azioni**, quindi selezionare il nome dell’utente che riceverà l’e-mail di avviso nel campo **Avvisa questi utenti**.
6. Configurare le altre opzioni di questa pagina per l’emissione di trap SNMP e l’esecuzione di uno script, quindi fare clic su **Salva**.

Visualizzazione degli avvisi

È possibile visualizzare l’elenco degli avvisi creati per diversi eventi dalla pagina Configurazione avvisi. È inoltre possibile visualizzare le proprietà degli avvisi, ad esempio la descrizione, il metodo e la frequenza di notifica, gli eventi che attivano l’avviso, i destinatari degli avvisi e le risorse interessate, ad esempio cluster, aggregati e volumi.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell’applicazione o amministratore dello storage.

Fase

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.

   L’elenco degli avvisi viene visualizzato nella pagina Configurazione avvisi.

Modifica degli avvisi

È possibile modificare le proprietà degli avvisi, ad esempio la risorsa a cui è associato l’avviso, gli eventi, i destinatari, le opzioni di notifica, la frequenza di notifica, e script associati.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell’applicazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina **Alert Setup**, selezionare l'avviso che si desidera modificare e fare clic su **Edit** (Modifica).
3. Nella finestra di dialogo **Edit Alert** (Modifica avviso), modificare le sezioni relative a nome, risorse, eventi e azioni, secondo necessità.

   È possibile modificare o rimuovere lo script associato all'avviso.

4. Fare clic su **Save** (Salva).

Eliminazione degli avvisi

È possibile eliminare un avviso quando non è più necessario. Ad esempio, è possibile eliminare un avviso creato per una determinata risorsa quando tale risorsa non viene più monitorata da Unified Manager.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina **Configurazione avviso**, selezionare gli avvisi che si desidera eliminare e fare clic su **Elimina**.
3. Fare clic su **Sì** per confermare la richiesta di eliminazione.

Descrizione delle finestre di avviso e delle finestre di dialogo

È necessario configurare gli avvisi in modo che ricevano le notifiche relative agli eventi utilizzando la finestra di dialogo Aggiungi avviso. È inoltre possibile visualizzare l'elenco degli avvisi dalla pagina Configurazione avvisi.

Pagina Alert Setup

La pagina Configurazione avvisi visualizza un elenco di avvisi e fornisce informazioni sul nome, lo stato, il metodo di notifica e la frequenza di notifica. Da questa pagina è inoltre possibile aggiungere, modificare, rimuovere, attivare o disattivare gli avvisi.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Pulsanti di comando

- **Aggiungi**

  Visualizza la finestra di dialogo Aggiungi avviso, che consente di aggiungere nuovi avvisi.

- **Modifica**

  Visualizza la finestra di dialogo Modifica avviso, che consente di modificare gli avvisi selezionati.

- **Elimina**

  Elimina gli avvisi selezionati.

- **Enable** (attiva)

  Consente agli avvisi selezionati di inviare notifiche.

- **Disattiva**

  Disattiva gli avvisi selezionati quando si desidera interrompere temporaneamente l'invio delle notifiche.

- **Test**

  Verifica gli avvisi selezionati per verificarne la configurazione dopo l'aggiunta o la modifica.

- **Avvisi per eventi risolti e obsoleti**

  Consente di attivare o disattivare l'invio di avvisi quando gli eventi vengono spostati negli stati risolti o obsoleti. Ciò può aiutare gli utenti a ricevere notifiche non necessarie.

Vista elenco

La vista elenco visualizza, in formato tabulare, le informazioni sugli avvisi creati. È possibile utilizzare i filtri di colonna per personalizzare i dati visualizzati. È inoltre possibile selezionare un avviso per visualizzare ulteriori informazioni nell'area dei dettagli.

- **Stato**

  Specifica se un avviso è attivato ( ) o disattivato ( ).

- **Avviso**

  Visualizza il nome dell'avviso.

- **Descrizione**

  Visualizza una descrizione dell'avviso.

- **Metodo di notifica**

  Visualizza il metodo di notifica selezionato per l'avviso. È possibile inviare notifiche agli utenti tramite messaggi e-mail o trap SNMP.

- **Frequenza di notifica**

  Specifica la frequenza (in minuti) con cui il server di gestione continua a inviare notifiche fino a quando l'evento non viene riconosciuto, risolto o spostato nello stato obsoleto.

Area dei dettagli

L'area dei dettagli fornisce ulteriori informazioni sull'avviso selezionato.

- **Nome avviso**

Visualizza il nome dell'avviso.

- **Descrizione avviso**

  Visualizza una descrizione dell'avviso.

- **Eventi**

  Visualizza gli eventi per i quali si desidera attivare l'avviso.

- **Risorse**

  Visualizza le risorse per le quali si desidera attivare l'avviso.

- **Include**

  Visualizza il gruppo di risorse per cui si desidera attivare l'avviso.

- **Esclusi**

  Visualizza il gruppo di risorse per cui non si desidera attivare l'avviso.

- **Metodo di notifica**

  Visualizza il metodo di notifica per l'avviso.

- **Frequenza di notifica**

  Visualizza la frequenza con cui il server di gestione continua a inviare notifiche di avviso fino a quando l'evento non viene riconosciuto, risolto o spostato nello stato obsoleto.

- **Nome script**

  Visualizza il nome dello script associato all'avviso selezionato. Questo script viene eseguito quando viene generato un avviso.

- **Destinatari email**

  Visualizza gli indirizzi e-mail degli utenti che ricevono la notifica di avviso.

Finestra di dialogo Add Alert (Aggiungi avviso)

È possibile creare avvisi per notificare quando viene generato un determinato evento, in modo da poter risolvere il problema rapidamente e ridurre al minimo l'impatto sull'ambiente. È possibile creare avvisi per una singola risorsa o un set di risorse e per eventi di un particolare tipo di severità. È inoltre possibile specificare il metodo di notifica e la frequenza degli avvisi.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Nome

Questa area consente di specificare un nome e una descrizione per l'avviso:

- **Nome avviso**

  Consente di specificare un nome di avviso.

- **Descrizione avviso**

  Consente di specificare una descrizione per l'avviso.

Risorse

Quest'area consente di selezionare una singola risorsa o di raggruppare le risorse in base a una regola dinamica per la quale si desidera attivare l'avviso. Una *regola dinamica* è l'insieme di risorse filtrate in base alla stringa di testo specificata. È possibile cercare le risorse selezionando un tipo di risorsa dall'elenco a discesa oppure specificare il nome esatto della risorsa per visualizzare una risorsa specifica.

Se si crea un avviso da una qualsiasi delle pagine dei dettagli dell'oggetto di storage, l'oggetto di storage viene automaticamente incluso nell'avviso.

- **Include**

  Consente di includere le risorse per le quali si desidera attivare gli avvisi. È possibile specificare una stringa di testo per raggruppare le risorse che corrispondono alla stringa e selezionare questo gruppo da includere nell'avviso. Ad esempio, è possibile raggruppare tutti i volumi il cui nome contiene la stringa "abc".

- **Escludi**

  Consente di escludere le risorse per le quali non si desidera attivare avvisi. Ad esempio, è possibile escludere tutti i volumi il cui nome contiene la stringa "xyz".

  La scheda Escludi viene visualizzata solo quando si selezionano tutte le risorse di un particolare tipo di risorsa, ad esempio <<All Volumes>> oppure <<All Volumes whose name contains 'xyz'>>.

  Se una risorsa è conforme alle regole di inclusione ed esclusione specificate, la regola di esclusione ha la precedenza sulla regola di inclusione e l'avviso non viene generato per l'evento.

Eventi

Quest'area consente di selezionare gli eventi per i quali si desidera creare gli avvisi. È possibile creare avvisi per gli eventi in base a una determinata severità o a una serie di eventi.

Per selezionare più eventi, tenere premuto il tasto Ctrl mentre si effettuano le selezioni.

- **Severità evento**

  Consente di selezionare gli eventi in base al tipo di severità, che può essere critico, errore o Avviso.

- **Il nome dell'evento contiene**

  Consente di selezionare eventi il cui nome contiene caratteri specifici.

Azioni

Questa area consente di specificare gli utenti che si desidera notificare quando viene attivato un avviso. È

inoltre possibile specificare il metodo di notifica e la frequenza di notifica.

- **Avvisa questi utenti**

  Consente di specificare l'indirizzo e-mail o il nome utente dell'utente per ricevere le notifiche.

  Se si modifica l'indirizzo di posta elettronica specificato per l'utente e si riapre l'avviso per la modifica, il campo Nome appare vuoto perché l'indirizzo di posta elettronica modificato non è più associato all'utente precedentemente selezionato. Inoltre, se l'indirizzo e-mail dell'utente selezionato è stato modificato dalla pagina utenti, l'indirizzo e-mail modificato non viene aggiornato per l'utente selezionato.

- **Frequenza di notifica**

  Consente di specificare la frequenza con cui il server di gestione invia le notifiche fino a quando l'evento non viene riconosciuto, risolto o spostato nello stato obsoleto.

  È possibile scegliere i seguenti metodi di notifica:

  - Notifica solo una volta
  - Notifica a una frequenza specificata
  - Notifica a una frequenza specificata entro l'intervallo di tempo specificato

- **Problema trap SNMP**

  La selezione di questa casella consente di specificare se inviare trap SNMP all'host SNMP configurato a livello globale.

- **Esegui script**

  Consente di aggiungere lo script personalizzato all'avviso. Questo script viene eseguito quando viene generato un avviso.

  Se questa funzionalità non viene visualizzata nell'interfaccia utente, è perché è stata disattivata dall'amministratore. Se necessario, è possibile attivare questa funzionalità da **Storage Management** > **Feature Settings**.

Pulsanti di comando

- **Salva**

  Crea un avviso e chiude la finestra di dialogo.

- **Annulla**

  Elimina le modifiche e chiude la finestra di dialogo.

Finestra di dialogo Edit Alert (Modifica avviso)

È possibile modificare le proprietà degli avvisi, ad esempio la risorsa a cui è associato l'avviso, gli eventi, gli script e le opzioni di notifica.

Nome

Quest'area consente di modificare il nome e la descrizione dell'avviso.

- **Nome avviso**

  Consente di modificare il nome dell'avviso.

- **Descrizione avviso**

  Consente di specificare una descrizione per l'avviso.

- **Stato avviso**

  Consente di attivare o disattivare l'avviso.

Risorse

Quest'area consente di selezionare una singola risorsa o di raggruppare le risorse in base a una regola dinamica per la quale si desidera attivare l'avviso. È possibile cercare le risorse selezionando un tipo di risorsa dall'elenco a discesa oppure specificare il nome esatto della risorsa per visualizzare una risorsa specifica.

- **Include**

  Consente di includere le risorse per le quali si desidera attivare gli avvisi. È possibile specificare una stringa di testo per raggruppare le risorse che corrispondono alla stringa e selezionare questo gruppo da includere nell'avviso. Ad esempio, è possibile raggruppare tutti i volumi il cui nome contiene la stringa "vol0".

- **Escludi**

  Consente di escludere le risorse per le quali non si desidera attivare avvisi. Ad esempio, è possibile escludere tutti i volumi il cui nome contiene la stringa "xyz".

> La scheda Escludi viene visualizzata solo quando si selezionano tutte le risorse di un particolare tipo di risorsa, ad esempio <<All Volumes>> o <<All Volumes whose name contains 'xyz'>>.

Eventi

Quest'area consente di selezionare gli eventi per i quali si desidera attivare gli avvisi. È possibile attivare un avviso per gli eventi in base a una determinata severità o a una serie di eventi.

- **Severità evento**

  Consente di selezionare gli eventi in base al tipo di severità, che può essere critico, errore o Avviso.

- **Il nome dell'evento contiene**

  Consente di selezionare gli eventi il cui nome contiene i caratteri specificati.

Azioni

Questa area consente di specificare il metodo di notifica e la frequenza di notifica.

- **Avvisa questi utenti**

  Consente di modificare l'indirizzo e-mail o il nome utente oppure di specificare un nuovo indirizzo e-mail o nome utente per ricevere le notifiche.

- **Frequenza di notifica**

  Consente di modificare la frequenza con cui il server di gestione invia le notifiche fino a quando l'evento non viene riconosciuto, risolto o spostato nello stato obsoleto.

  È possibile scegliere i seguenti metodi di notifica:

  - Notifica solo una volta
  - Notifica a una frequenza specificata
  - Notifica a una frequenza specificata entro l'intervallo di tempo specificato

- **Problema trap SNMP**

  Consente di specificare se inviare trap SNMP all'host SNMP configurato a livello globale.

- **Esegui script**

  Consente di associare uno script all'avviso. Questo script viene eseguito quando viene generato un avviso.

Pulsanti di comando

- **Salva**

  Salva le modifiche e chiude la finestra di dialogo.

- **Annulla**

  Elimina le modifiche e chiude la finestra di dialogo.

Gestione degli script

È possibile utilizzare gli script per modificare o aggiornare automaticamente più oggetti di storage in Unified Manager. Lo script è associato a un avviso. Quando un evento attiva un avviso, lo script viene eseguito. È possibile caricare script personalizzati e testarne l'esecuzione quando viene generato un avviso.

Per impostazione predefinita, è attivata la possibilità di caricare gli script in Unified Manager ed eseguirli. Se l'organizzazione non desidera consentire questa funzionalità per motivi di sicurezza, è possibile disattivarla da **Storage Management** > **Feature Settings**.

Informazioni correlate

"Abilitazione e disabilitazione della capacità di caricare gli script"

Come funzionano gli script con gli avvisi

È possibile associare un avviso allo script in modo che venga eseguito quando viene

generato un avviso per un evento in Unified Manager. È possibile utilizzare gli script per risolvere i problemi relativi agli oggetti di storage o identificare gli oggetti di storage che generano gli eventi.

Quando viene generato un avviso per un evento in Unified Manager, viene inviata un'email di avviso ai destinatari specificati. Se è stato associato un avviso a uno script, lo script viene eseguito. È possibile ottenere i dettagli degli argomenti passati allo script dall'e-mail di avviso.

> Se è stato creato uno script personalizzato e lo si è associato a un avviso per un tipo di evento specifico, le azioni vengono eseguite in base allo script personalizzato per quel tipo di evento e le azioni **Fix it** non sono disponibili per impostazione predefinita nella pagina delle azioni di gestione o nella dashboard di Unified Manager.

Lo script utilizza i seguenti argomenti per l'esecuzione:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

È possibile utilizzare gli argomenti negli script e raccogliere informazioni relative agli eventi o modificare gli oggetti di storage.

Esempio per ottenere argomenti dagli script

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

Quando viene generato un avviso, questo script viene eseguito e viene visualizzato il seguente output:

```
-`eventID : 290`
-`eventSourceID : 4138`
```

Aggiunta di script

È possibile aggiungere script in Unified Manager e associarli agli avvisi. Questi script vengono eseguiti automaticamente quando viene generato un avviso e consentono di ottenere informazioni sugli oggetti di storage per i quali viene generato l'evento.

Cosa ti serve

- È necessario aver creato e salvato gli script che si desidera aggiungere al server Unified Manager.
- I formati di file supportati per gli script sono Perl, Shell, PowerShell, Python e. `.bat` file.

Piattaforma su cui è installato Unified Manager	Lingue supportate
VMware	Script Perl e Shell
Linux	Script Perl, Python e Shell
Windows	Script PowerShell, Perl, Python e .bat

  - Per gli script Perl, Perl deve essere installato sul server Unified Manager. Per le installazioni VMware, Perl 5 viene installato per impostazione predefinita e gli script supportano solo ciò che Perl 5 supporta. Se Perl è stato installato dopo Unified Manager, è necessario riavviare il server Unified Manager.
  - Per gli script PowerShell, è necessario impostare il criterio di esecuzione PowerShell appropriato sul server Windows in modo che gli script possano essere eseguiti.

> Se lo script crea file di log per tenere traccia dell'avanzamento dello script di avviso, è necessario assicurarsi che i file di log non vengano creati in alcun punto della cartella di installazione di Unified Manager.

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile caricare script personalizzati e raccogliere i dettagli dell'evento relativi all'avviso.

> Se questa funzionalità non viene visualizzata nell'interfaccia utente, è perché è stata disattivata dall'amministratore. Se necessario, è possibile attivare questa funzionalità da **Storage Management** > **Feature Settings**.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage Management** > **Scripts**.
2. Nella pagina **script**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi script**, fare clic su **Sfoglia** per selezionare il file script.
4. Inserire una descrizione per lo script selezionato.
5. Fare clic su **Aggiungi**.

Informazioni correlate

"Abilitazione e disabilitazione della capacità di caricare gli script"

Eliminazione degli script

È possibile eliminare uno script da Unified Manager quando lo script non è più necessario o valido.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

- Lo script non deve essere associato a un avviso.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage Management** > **Scripts**.
2. Nella pagina **script**, selezionare lo script che si desidera eliminare, quindi fare clic su **Elimina**.
3. Nella finestra di dialogo **Avviso**, confermare l'eliminazione facendo clic su **Sì**.

Esecuzione di test dello script

È possibile verificare che lo script venga eseguito correttamente quando viene generato un avviso per un oggetto di storage.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver caricato uno script nel formato di file supportato in Unified Manager.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage Management** > **Scripts**.
2. Nella pagina **script**, aggiungere lo script di test.
3. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
4. Nella pagina **Alert Setup**, eseguire una delle seguenti operazioni:

Per…	Eseguire questa operazione…
Aggiungere un avviso	a. Fare clic su **Aggiungi**. b. Nella sezione Actions (azioni), associare l'avviso allo script di test.
Modificare un avviso	a. Selezionare un avviso, quindi fare clic su **Modifica**. b. Nella sezione Actions (azioni), associare l'avviso allo script di test.

5. Fare clic su **Save** (Salva).
6. Nella pagina **Alert Setup**, selezionare l'avviso aggiunto o modificato, quindi fare clic su **Test**.

   Lo script viene eseguito con l'argomento "-test" e viene inviato un avviso di notifica agli indirizzi e-mail specificati al momento della creazione dell'avviso.

Comandi CLI di Unified Manager supportati

In qualità di amministratore dello storage, è possibile utilizzare i comandi CLI per eseguire query sugli oggetti storage, ad esempio su cluster, aggregati, volumi, Qtree e LUN. È possibile utilizzare i comandi CLI per eseguire query nel database interno di Unified Manager e nel database ONTAP. È inoltre possibile utilizzare i comandi CLI negli

script eseguiti all'inizio o alla fine di un'operazione o quando viene attivato un avviso.

Tutti i comandi devono essere preceduti dal comando `um cli login` e un nome utente e una password validi per l'autenticazione.

Per eseguire il comando *um run*, assicurarsi che l'account disponga dell'accesso all'applicazione *console*.

Comando CLI	Descrizione	Output
`um cli login -u <username> [-p <password>]`	Effettua l'accesso alla CLI. A causa delle implicazioni legate alla sicurezza, inserire solo il nome utente dopo l'opzione "-u". Quando viene utilizzata in questo modo, viene richiesta la password e la password non viene acquisita nella tabella della cronologia o del processo. La sessione scade dopo tre ore dal momento dell'accesso, dopodiché l'utente deve effettuare nuovamente l'accesso.	Visualizza il messaggio corrispondente.
`um cli logout`	Disconnette dalla CLI.	Visualizza il messaggio corrispondente.
`um help`	Visualizza tutti i sottocomandi di primo livello.	Visualizza tutti i sottocomandi di primo livello.
`um run cmd [ -t <timeout> ] <cluster> <command>`	Il modo più semplice per eseguire un comando su uno o più host. Utilizzato principalmente per lo scripting degli avvisi per ottenere o eseguire un'operazione su ONTAP. L'argomento opzionale timeout imposta un limite di tempo massimo (in secondi) per il completamento del comando sul client. Il valore predefinito è 0 (attendere per sempre).	Come ricevuto da ONTAP.
`um run query <sql command>`	Esegue una query SQL. Sono consentite solo le query lette dal database. Le operazioni di aggiornamento, inserimento o eliminazione non sono supportate.	I risultati vengono visualizzati in formato tabulare. Se viene restituito un set vuoto o se si verificano errori di sintassi o richieste errate, viene visualizzato il messaggio di errore appropriato.

Comando CLI	Descrizione	Output
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Aggiunge un'origine dati all'elenco dei sistemi di storage gestiti. Un'origine dati descrive le modalità di connessione ai sistemi storage. Quando si aggiunge un'origine dati, è necessario specificare le opzioni -u (nome utente) e -P (password). L'opzione -t (protocollo) specifica il protocollo utilizzato per comunicare con il cluster (http o https). Se il protocollo non viene specificato, si tenteranno entrambi i protocolli. L'opzione -p (porta) specifica la porta utilizzata per comunicare con il cluster. Se la porta non viene specificata, viene tentato di utilizzare il valore predefinito del protocollo appropriato. Questo comando può essere eseguito solo dall'amministratore dello storage.	Richiede all'utente di accettare il certificato e stampa il messaggio corrispondente.
`um datasource list [ <datasource-id>]`	Visualizza le origini dati per i sistemi storage gestiti.	Visualizza i seguenti valori in formato tabulare: `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>`	Modifica una o più opzioni di origine dati. Può essere eseguito solo dall'amministratore dello storage.	Visualizza il messaggio corrispondente.
`um datasource remove <datasource-id>`	Rimuove l'origine dati (cluster) da Unified Manager.	Visualizza il messaggio corrispondente.
`um option list [ <option> .. ]`	Elenca tutte le opzioni che è possibile configurare utilizzando il comando set.	Visualizza i seguenti valori in formato tabulare: `Name, Value, Default Value, and Requires Restart.`
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	Imposta una o più opzioni. Il comando può essere eseguito solo dall'amministratore dello storage.	Visualizza il messaggio corrispondente.

Comando CLI	Descrizione	Output
`um version`	Visualizza la versione del software Unified Manager.	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	Elenca i LUN dopo il filtraggio sull'oggetto specificato. -q è applicabile a tutti i comandi per non visualizzare alcuna intestazione. ObjectType può essere lun, qtree, cluster, volume, quota, o svm. Ad esempio: **`um lun list -cluster 1`** In questo esempio, "-cluster" è objectType e "1" è objectID. Il comando elenca tutte le LUN all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabulare: `ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	Elenca le VM di storage dopo il filtraggio sull'oggetto specificato. ObjectType può essere lun, qtree, cluster, volume, quota, o svm. Ad esempio: **`um svm list -cluster 1`** In questo esempio, "-cluster" è objectType e "1" è objectID. Il comando elenca tutte le VM di storage all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabulare: `Name and Cluster ID.`
`um qtree list [-q] [ -ObjectType <object-id>]`	Elenca i qtree dopo il filtraggio sull'oggetto specificato. -q è applicabile a tutti i comandi per non visualizzare alcuna intestazione. ObjectType può essere lun, qtree, cluster, volume, quota, o svm. Ad esempio: **`um qtree list -cluster 1`** In questo esempio, "-cluster" è objectType e "1" è objectID. Il comando elenca tutti i qtree all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabulare: `Qtree ID and Qtree Name.`

Comando CLI	Descrizione	Output
`um disk list [-q] [-ObjectType <object-id>]`	Elenca i dischi dopo il filtraggio sull'oggetto specificato. ObjectType può essere disco, aggr, nodo o cluster. Ad esempio: **`um disk list -cluster 1`** In questo esempio, "-cluster" è objectType e "1" è objectID. Il comando elenca tutti i dischi all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabulare `ObjectType and object-id`.
`um cluster list [-q] [-ObjectType <object-id>]`	Elenca i cluster dopo il filtraggio sull'oggetto specificato. ObjectType può essere disco, aggr, nodo, cluster, lun, qtree, volume, quota o svm. Ad esempio: **`um cluster list -aggr 1`** In questo esempio, "-aggr" è objectType e "1" è objectID. Il comando elenca il cluster a cui appartiene l'aggregato con ID 1.	Visualizza i seguenti valori in formato tabulare: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key`.
`um cluster node list [-q] [-ObjectType <object-id>]`	Elenca i nodi del cluster dopo il filtraggio sull'oggetto specificato. ObjectType può essere disco, aggr, nodo o cluster. Ad esempio: **`um cluster node list -cluster 1`** In questo esempio, "-cluster" è objectType e "1" è objectID. Il comando elenca tutti i nodi all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabulare `Name and Cluster ID`.

Comando CLI	Descrizione	Output
`um volume list [-q] [-ObjectType <object-id>]`	Elenca i volumi dopo il filtraggio sull'oggetto specificato. ObjectType può essere lun, qtree, cluster, volume, quota, svm o aggregato. Ad esempio: **`um volume list -cluster 1`** In questo esempio, "-cluster" è objectType e "1" è objectID. Il comando elenca tutti i volumi all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabulare `Volume ID and Volume Name`.
`um quota user list [-q] [-ObjectType <object-id>]`	Elenca gli utenti di quota dopo il filtraggio sull'oggetto specificato. ObjectType può essere qtree, cluster, volume, quota o svm. Ad esempio: **`um quota user list -cluster 1`** In questo esempio, "-cluster" è objectType e "1" è objectID. Il comando elenca tutti gli utenti di quota all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabulare `ID, Name, SID and Email`.
`um aggr list [-q] [-ObjectType <object-id>]`	Elenca gli aggregati dopo il filtraggio sull'oggetto specificato. ObjectType può essere disco, aggr, nodo, cluster o volume. Ad esempio: **`um aggr list -cluster 1`** In questo esempio, "-cluster" è objectType e "1" è objectID. Il comando elenca tutti gli aggregati all'interno del cluster con ID 1.	Visualizza i seguenti valori in formato tabulare `Aggr ID, and Aggr Name`.
`um event ack <event-ids>`	Riconosce uno o più eventi.	Visualizza il messaggio corrispondente.
`um event resolve <event-ids>`	Risolve uno o più eventi.	Visualizza il messaggio corrispondente.

Comando CLI	Descrizione	Output
`um event assign -u <username> <event-id>`	Assegna un evento a un utente.	Visualizza il messaggio corrispondente.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Elenca gli eventi generati dal sistema o dall'utente. Filtra gli eventi in base all'origine, allo stato e agli ID.	Visualizza i seguenti valori in formato tabulare `Source, Source type, Name, Severity, State, User and Timestamp`.
`um backup restore -f <backup_file_path_and_name>`	Ripristina un backup del database MySQL utilizzando file .7z.	Visualizza il messaggio corrispondente.

Descrizione delle finestre di script e delle finestre di dialogo

La pagina script consente di aggiungere script a Unified Manager.

Pagina degli script

La pagina script consente di aggiungere gli script personalizzati a Unified Manager. È possibile associare questi script agli avvisi per consentire la riconfigurazione automatica degli oggetti di storage.

La pagina script consente di aggiungere o eliminare script da Unified Manager.

Pulsanti di comando

- **Aggiungi**

  Visualizza la finestra di dialogo Aggiungi script, che consente di aggiungere script.

- **Elimina**

  Elimina lo script selezionato.

Vista elenco

La vista elenco visualizza, in formato tabulare, gli script aggiunti a Unified Manager.

- **Nome**

  Visualizza il nome dello script.

- **Descrizione**

  Visualizza la descrizione dello script.

Finestra di dialogo Add script (Aggiungi script)

La finestra di dialogo Aggiungi script consente di aggiungere script a Unified Manager. È possibile configurare gli avvisi con gli script per risolvere automaticamente gli eventi generati per gli oggetti di storage.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

- **Selezionare file script**

  Consente di selezionare uno script per l'avviso.

- **Descrizione**

  Consente di specificare una descrizione per lo script.

Monitorare e gestire le performance del cluster

Introduzione al monitoraggio delle performance di Active IQ Unified Manager

Active IQ Unified Manager (in precedenza Unified Manager di OnCommand) offre funzionalità di monitoraggio delle performance e analisi delle cause principali degli eventi per i sistemi che eseguono il software NetApp ONTAP.

Unified Manager ti aiuta a identificare i carichi di lavoro che stanno utilizzando in eccesso i componenti del cluster e a ridurre le performance di altri carichi di lavoro sul cluster. La definizione dei criteri di soglia delle performance consente inoltre di specificare i valori massimi per determinati contatori delle performance in modo che gli eventi vengano generati quando la soglia viene superata. Unified Manager avvisa l'utente in merito a questi eventi di performance in modo da poter intraprendere azioni correttive e riportare le performance ai normali livelli operativi. È possibile visualizzare e analizzare gli eventi nell'interfaccia utente di Unified Manager.

Unified Manager monitora le performance di due tipi di carichi di lavoro:

- Carichi di lavoro definiti dall'utente

  Questi carichi di lavoro sono costituiti da volumi FlexVol e volumi FlexGroup creati nel cluster.

- Carichi di lavoro definiti dal sistema

  Questi carichi di lavoro sono costituiti da attività di sistema interne.

Funzionalità di monitoraggio delle performance di Unified Manager

Unified Manager raccoglie e analizza le statistiche delle performance dai sistemi che eseguono il software ONTAP. Utilizza soglie di performance dinamiche e soglie di performance definite dall'utente per monitorare una varietà di contatori di performance su molti componenti del cluster.

Un tempo di risposta elevato (latenza) indica che le prestazioni dell'oggetto storage, ad esempio un volume, sono più lente del normale. Questo problema indica anche che le performance sono diminuite per le applicazioni client che utilizzano il volume. Unified Manager identifica il componente di storage in cui si trova il problema delle performance e fornisce un elenco di azioni consigliate che è possibile intraprendere per risolvere il problema delle performance.

Unified Manager include le seguenti funzionalità:

- Monitora e analizza le statistiche delle performance dei carichi di lavoro da un sistema che esegue il software ONTAP.
- Tiene traccia dei contatori delle performance per cluster, nodi, aggregati, porte, SVM, Volumi, LUN, spazi dei nomi NVMe e interfacce di rete (LIFF).
- Visualizza grafici dettagliati che rappresentano l'attività dei carichi di lavoro nel tempo, inclusi IOPS (operazioni), MB/s (throughput), latenza (tempo di risposta), utilizzo, capacità delle performance e rapporto cache.

- Consente di creare criteri di soglia delle performance definiti dall'utente che attivano gli eventi e inviano avvisi via email quando le soglie vengono superate.
- Utilizza soglie definite dal sistema e soglie di performance dinamiche che consentono di conoscere l'attività del carico di lavoro per identificare e avvisare l'utente in caso di problemi di performance.
- Identifica le policy di qualità del servizio (QoS) e le policy di performance del livello di servizio (PSL) applicate ai volumi e alle LUN.
- Identifica chiaramente il componente del cluster in conflitto.
- Identifica i carichi di lavoro che stanno utilizzando in eccesso i componenti del cluster e i carichi di lavoro le cui performance sono influenzate dall'aumento dell'attività.

Interfacce di Unified Manager utilizzate per gestire le performance del sistema storage

Queste sezioni contengono informazioni sulle due interfacce utente fornite da Active IQ Unified Manager per la risoluzione dei problemi di capacità, disponibilità e protezione dello storage dei dati. Le due interfacce utente sono l'interfaccia utente Web di Unified Manager e la console di manutenzione.

Se si desidera utilizzare le funzioni di protezione di Unified Manager, è necessario installare e configurare anche OnCommand Workflow Automation (Wfa).

UI Web di Unified Manager

L'interfaccia utente Web di Unified Manager consente a un amministratore di monitorare e risolvere i problemi del cluster relativi a capacità, disponibilità e protezione dello storage dei dati.

Queste sezioni descrivono alcuni flussi di lavoro comuni che un amministratore può seguire per risolvere i problemi di capacità dello storage, disponibilità dei dati o protezione visualizzati nell'interfaccia utente Web di Unified Manager.

Console di manutenzione

La console di manutenzione di Unified Manager consente a un amministratore di monitorare, diagnosticare e risolvere i problemi del sistema operativo, i problemi di aggiornamento della versione, i problemi di accesso degli utenti e i problemi di rete relativi al server Unified Manager stesso. Se l'interfaccia utente Web di Unified Manager non è disponibile, la console di manutenzione è l'unica forma di accesso a Unified Manager.

È possibile utilizzare queste informazioni per accedere alla console di manutenzione e utilizzarla per risolvere i problemi relativi al funzionamento del server Unified Manager.

Attività di raccolta dei dati relativi alla configurazione e alle performance del cluster

L'intervallo di raccolta per *dati di configurazione del cluster* è di 15 minuti. Ad esempio, dopo aver aggiunto un cluster, sono necessari 15 minuti per visualizzare i dettagli del cluster nell'interfaccia utente di Unified Manager. Questo intervallo si applica anche quando si apportano modifiche a un cluster.

Ad esempio, se si aggiungono due nuovi volumi a una SVM in un cluster, i nuovi oggetti vengono visualizzati nell'interfaccia utente dopo il successivo intervallo di polling, che potrebbe arrivare fino a 15 minuti.

Unified Manager raccoglie le *statistiche sulle performance* correnti da tutti i cluster monitorati ogni cinque minuti. Analizza questi dati per identificare gli eventi relativi alle performance e i potenziali problemi. Conserva 30 giorni di dati storici delle performance di cinque minuti e 180 giorni di dati storici delle performance di un'ora. Ciò consente di visualizzare dettagli granulari sulle performance per il mese corrente e trend generali delle performance fino a un anno.

I sondaggi di raccolta vengono sfalsati di alcuni minuti in modo che i dati provenienti da ogni cluster non vengano inviati contemporaneamente, il che potrebbe influire sulle performance.

La seguente tabella descrive le attività di raccolta eseguite da Unified Manager:

Attività	Intervallo di tempo	Descrizione
Polling delle statistiche delle performance	Ogni 5 minuti	Raccoglie i dati delle performance in tempo reale da ciascun cluster.
Analisi statistica	Ogni 5 minuti	Dopo ogni polling delle statistiche, Unified Manager confronta i dati raccolti con le soglie definite dall'utente, definite dal sistema e dinamiche. In caso di superamento di qualsiasi soglia di performance, Unified Manager genera eventi e invia messaggi di posta elettronica agli utenti specificati, se configurati per farlo.
Polling della configurazione	Ogni 15 minuti	Raccoglie informazioni dettagliate sull'inventario da ciascun cluster per identificare tutti gli oggetti storage (nodi, SVM, volumi e così via).
Riepilogo	Ogni ora	Riepiloga le ultime 12 raccolte di dati delle performance di cinque minuti in medie orarie. I valori medi orari vengono utilizzati in alcune pagine dell'interfaccia utente e vengono conservati per 180 giorni.
Analisi delle previsioni e eliminazione dei dati	Tutti i giorni dopo la mezzanotte	Analizza i dati del cluster per stabilire soglie dinamiche per la latenza del volume e gli IOPS per le 24 ore successive. Elimina dal database tutti i dati relativi alle performance di cinque minuti precedenti a 30 giorni.

Attività	Intervallo di tempo	Descrizione
Eliminazione dei dati	Tutti i giorni dopo le 2 del mattino	Elimina dal database tutti gli eventi più vecchi di 180 giorni e le soglie dinamiche più vecchie di 180 giorni.
Eliminazione dei dati	Tutti i giorni dopo le 3:30	Elimina dal database tutti i dati relativi alle performance di un'ora precedenti a 180 giorni.

Che cos'è un ciclo di raccolta di continuità dei dati

Un ciclo di raccolta della continuità dei dati recupera i dati delle performance al di fuori del ciclo di raccolta delle performance del cluster in tempo reale che viene eseguito, per impostazione predefinita, ogni cinque minuti. Le raccolte di continuità dei dati consentono a Unified Manager di colmare le lacune dei dati statistici che si verificano quando non è stato in grado di raccogliere dati in tempo reale.

Unified Manager esegue il polling della raccolta di continuità dei dati storici delle performance quando si verificano i seguenti eventi:

- Un cluster viene inizialmente aggiunto a Unified Manager.

  Unified Manager raccoglie i dati storici delle performance dei 15 giorni precedenti. In questo modo, è possibile visualizzare due settimane di informazioni cronologiche sulle performance di un cluster poche ore dopo l'aggiunta.

  Inoltre, gli eventi di soglia definiti dal sistema vengono riportati per il periodo precedente, se presenti.

- Il ciclo corrente di raccolta dei dati sulle performance non termina in tempo.

  Se il sondaggio sulle performance in tempo reale supera il periodo di raccolta di cinque minuti, viene avviato un ciclo di raccolta della continuità dei dati per raccogliere le informazioni mancanti. Senza la raccolta di continuità dei dati, il successivo periodo di raccolta viene ignorato.

- Unified Manager è rimasto inaccessibile per un certo periodo di tempo e poi torna online, come nelle seguenti situazioni:
  - È stato riavviato.
  - È stato arrestato durante un aggiornamento del software o durante la creazione di un file di backup.
  - Un'interruzione di rete viene riparata.
- Un cluster è stato inaccessibile per un certo periodo di tempo e quindi torna online, come nelle seguenti situazioni:
  - Un'interruzione di rete viene riparata.
  - Una connessione di rete wide-area lenta ha ritardato la normale raccolta di dati sulle prestazioni.

Un ciclo di raccolta della continuità dei dati può raccogliere un massimo di 24 ore di dati storici. Se Unified Manager rimane inattivo per più di 24 ore, nelle pagine dell'interfaccia utente viene visualizzato un divario nei dati relativi alle prestazioni.

Non è possibile eseguire contemporaneamente un ciclo di raccolta della continuità dei dati e un ciclo di raccolta dati in tempo reale. Il ciclo di raccolta della continuità dei dati deve terminare prima di iniziare la raccolta dei dati delle performance in tempo reale. Quando la raccolta di continuità dei dati è necessaria per raccogliere più di un'ora di dati storici, nella parte superiore del riquadro Notifiche viene visualizzato un messaggio banner per quel cluster.

Cosa significa il timestamp nei dati e negli eventi raccolti

L'indicatore data e ora visualizzato nei dati di salute e performance raccolti o visualizzato come ora di rilevamento di un evento si basa sull'ora del cluster ONTAP, regolata in base al fuso orario impostato nel browser Web.

Si consiglia vivamente di utilizzare un server NTP (Network Time Protocol) per sincronizzare l'ora sui server Unified Manager, sui cluster ONTAP e sui browser Web.

Se vengono visualizzati indicatori di data e ora non corretti per un determinato cluster, controllare che l'ora del cluster sia stata impostata correttamente.

Navigazione nei flussi di lavoro delle performance nella GUI di Unified Manager

L'interfaccia di Unified Manager fornisce molte pagine per la raccolta e la visualizzazione delle informazioni sulle performance. Il pannello di navigazione sinistro consente di accedere alle pagine della GUI e di visualizzare e configurare le informazioni utilizzando le schede e i collegamenti presenti nelle pagine.

Per monitorare e risolvere i problemi relativi alle prestazioni del cluster, utilizzare tutte le pagine seguenti:

- pagina del dashboard
- pagine di inventario degli oggetti di storage e di rete
- pagine dei dettagli dell'oggetto storage (incluso performance explorer)
- pagine di configurazione e configurazione
- pagine di eventi

Accesso all'interfaccia utente

È possibile accedere all'interfaccia utente di Unified Manager utilizzando un browser Web supportato.

Cosa ti serve

- Il browser Web deve soddisfare i requisiti minimi.

  Consultare la matrice di interoperabilità all'indirizzo "mysupport.netapp.com/matrix" per l'elenco completo delle versioni del browser supportate.

- È necessario disporre dell'indirizzo IP o dell'URL del server Unified Manager.

L'utente viene disconnesso automaticamente dalla sessione dopo 1 ora di inattività. Questo intervallo di tempo

può essere configurato in **Generale** > **Impostazioni delle funzioni**.

Fasi

1. Inserire l'URL nel browser Web, dove URL è l'indirizzo IP o FQDN (Fully Qualified Domain Name) del server Unified Manager:
   - Per IPv4: `https://URL/`
   - Per IPv6: `https://[URL]/`

Se il server utilizza un certificato digitale autofirmato, il browser potrebbe visualizzare un avviso che indica che il certificato non è attendibile. È possibile riconoscere il rischio di continuare l'accesso o installare un certificato digitale firmato dall'autorità di certificazione (CA) per l'autenticazione del server. . Nella schermata di accesso, inserire il nome utente e la password.

Se l'accesso all'interfaccia utente di Unified Manager è protetto mediante l'autenticazione SAML, inserire le credenziali nella pagina di accesso del provider di identità (IdP) invece che nella pagina di accesso di Unified Manager.

Viene visualizzata la pagina Dashboard.

Se il server Unified Manager non viene inizializzato, viene visualizzata una nuova finestra del browser con la procedura guidata per la prima esperienza. Immettere un destinatario e-mail iniziale a cui verranno inviati gli avvisi e-mail, il server SMTP che gestirà le comunicazioni e-mail e se AutoSupport è abilitato per inviare informazioni sull'installazione di Unified Manager al supporto tecnico. L'interfaccia utente di Unified Manager viene visualizzata dopo aver completato queste informazioni.

Interfaccia grafica e percorsi di navigazione

Unified Manager offre una grande flessibilità e consente di eseguire più attività in vari modi. Ci sono molti percorsi di navigazione che scoprirete mentre lavorate in Unified Manager. Anche se non tutte le possibili combinazioni di navigazione possono essere mostrate, dovresti avere familiarità con alcuni degli scenari più comuni.

Monitorare la navigazione degli oggetti del cluster

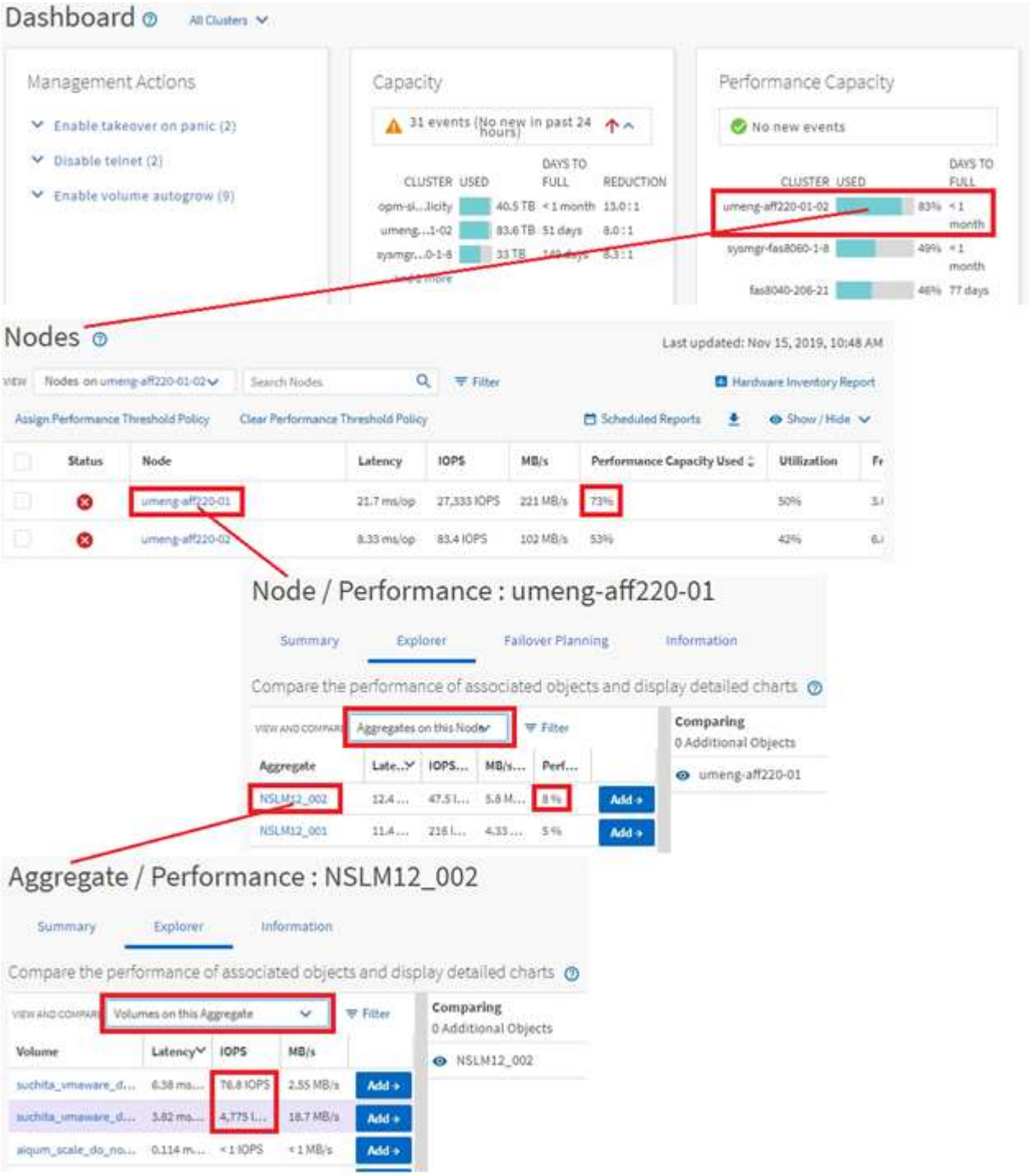
È possibile monitorare le performance di tutti gli oggetti in qualsiasi cluster gestito da Unified Manager. Il monitoraggio degli oggetti storage offre una panoramica delle performance di cluster e oggetti e include il monitoraggio degli eventi delle performance. È possibile visualizzare performance ed eventi a un livello elevato oppure esaminare ulteriormente i dettagli delle performance degli oggetti e degli eventi delle performance.

Questo è un esempio di molte possibili esplorazioni degli oggetti del cluster:

1. Dalla pagina Dashboard, esaminare i dettagli nel pannello Performance Capacity (capacità delle performance) per identificare il cluster che utilizza la capacità di performance più elevata e fare clic sul grafico a barre per accedere all'elenco dei nodi per il cluster.
2. Identificare il nodo con il valore più elevato utilizzato per la capacità delle performance e fare clic su tale nodo.
3. Dalla pagina Node / Performance Explorer (Esplora nodi/prestazioni), fare clic su **Aggregates on this Node** (aggregati su questo nodo) dal menu View and compare (Visualizza e confronta).

4. Identificare l'aggregato che utilizza la capacità di performance più elevata e fare clic su tale aggregato.
5. Dalla pagina aggregate / Performance Explorer, fare clic su **Volumes on this aggregate** (volumi su questo aggregato) dal menu View and compare (Visualizza e confronta).
6. Identificare i volumi che utilizzano il maggior numero di IOPS.

È necessario esaminare questi volumi per verificare se è necessario applicare una policy di QoS o una policy di Performance Service Level o modificare le impostazioni della policy, in modo che tali volumi non utilizzino una percentuale così elevata di IOPS sul cluster.



Monitorare la navigazione delle performance del cluster

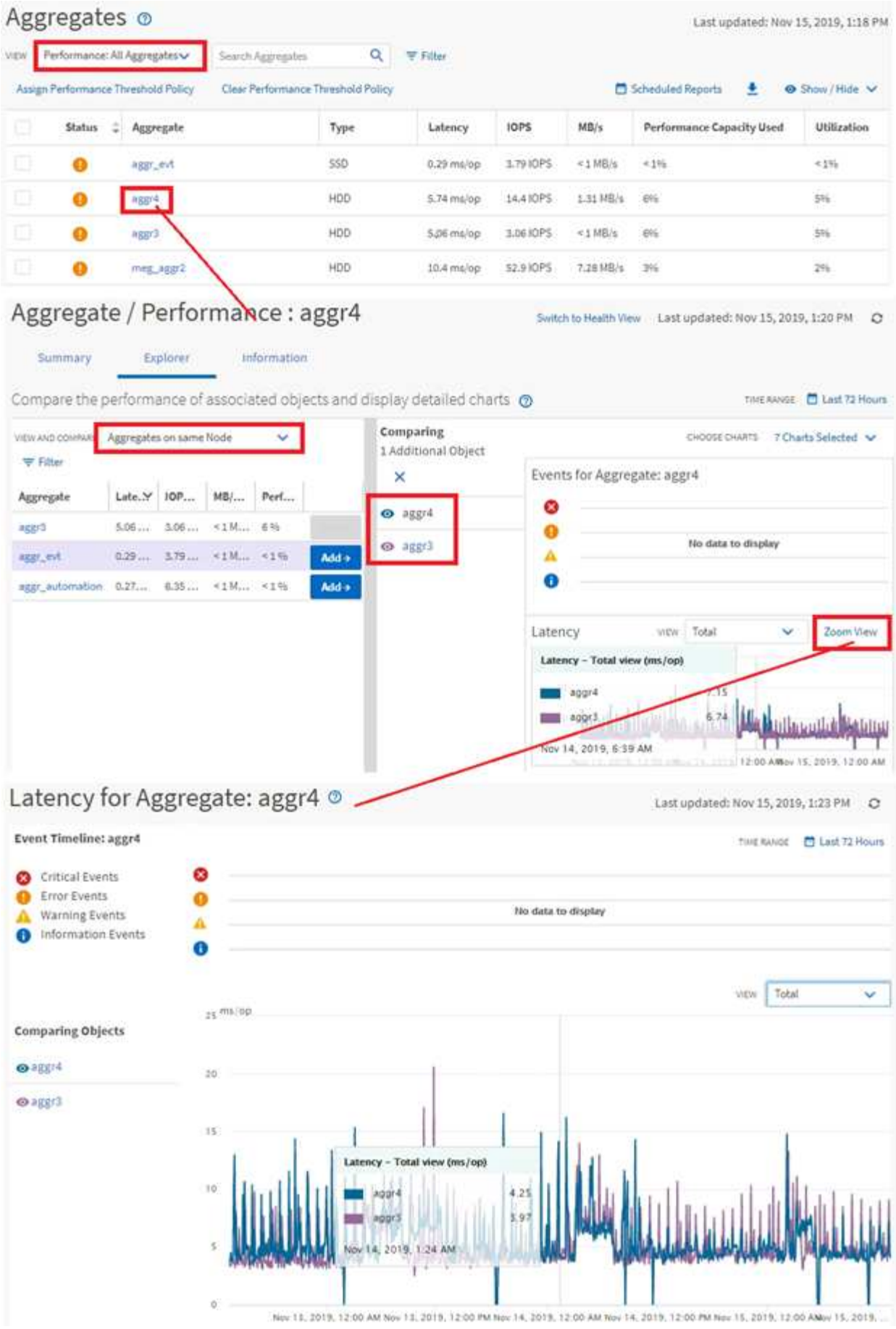
È possibile monitorare le performance di tutti i cluster gestiti da Unified Manager. Il monitoraggio dei cluster offre una panoramica delle performance di cluster e oggetti e include il monitoraggio degli eventi delle performance. È possibile visualizzare performance ed eventi a un livello elevato, oppure esaminare ulteriormente eventuali dettagli relativi alle performance di cluster e oggetti e agli eventi relativi alle performance.

Questo è un esempio di molti possibili percorsi di navigazione delle performance del cluster:

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates**.
2. Per visualizzare le informazioni sulle performance in questi aggregati, selezionare la vista Performance: All aggregates (prestazioni: Tutti gli aggregati).
3. Identificare l'aggregato che si desidera analizzare e fare clic sul nome dell'aggregato per accedere alla pagina aggregato/Esplora prestazioni.
4. Se si desidera, selezionare altri oggetti da confrontare con questo aggregato nel menu Visualizza e confronta, quindi aggiungere uno degli oggetti al riquadro di confronto.

   Le statistiche per entrambi gli oggetti verranno visualizzate nei diagrammi dei contatori per il confronto.

5. Nel riquadro di confronto a destra della pagina Explorer, fare clic su **Zoom View** in uno dei diagrammi dei contatori per visualizzare i dettagli sulla cronologia delle performance per quell'aggregato.


Aggregates
Last updated: Nov 15, 2019, 1:18 PM
VIEW
Performance: All Aggregates
Search Aggregates
Filter
Assign Performance Threshold Policy
Clear Performance Threshold Policy
Scheduled Reports
Show / Hide
Status
Aggregate
Type
Latency
IOPS
MB/s
Performance Capacity Used
Utilization
aggr_evt
SSD
0.29 ms/op
3.79 IOPS
< 1 MB/s
< 1%
aggr4
HDD
5.74 ms/op
14.4 IOPS
1.31 MB/s
6%
5%
aggr3
HDD
5.06 ms/op
3.06 IOPS
< 1 MB/s
6%
5%
meg_aggr2
HDD
10.4 ms/op
52.9 IOPS
7.28 MB/s
3%
2%
Aggregate / Performance : aggr4
Switch to Health View
Last updated: Nov 15, 2019, 1:20 PM
Summary
Explorer
Information
Compare the performance of associated objects and display detailed charts
TIME RANGE
Last 72 Hours
VIEW AND COMPARE
Aggregates on same Node
Filter
Aggregate
Late...
IOP...
MB/...
Perf...
aggr3
5.06 ...
3.06 ...
< 1 M...
6 %
aggr_evt
0.29 ...
3.79 ...
< 1 M...
< 1 %
Add
aggr_automation
0.27...
6.35 ...
< 1 M...
< 1 %
Add
Comparing
1 Additional Object
CHOOSE CHARTS
7 Charts Selected
aggr4
aggr3
Events for Aggregate: aggr4
No data to display
Latency
VIEW
Total
Zoom View
Latency – Total view (ms/op)
aggr4
7.15
aggr3
6.74
Nov 14, 2019, 6:39 AM
12:00 AM
Nov 15, 2019, 12:00 AM
Latency for Aggregate: aggr4
Last updated: Nov 15, 2019, 1:23 PM
Event Timeline: aggr4
TIME RANGE
Last 72 Hours
Critical Events
Error Events
Warning Events
Information Events
No data to display
VIEW
Total
Comparing Objects
aggr4
aggr3
ms/op
25
20
15
10
5
0
Latency – Total view (ms/op)
aggr4
4.25
aggr3
3.97
Nov 14, 2019, 1:24 AM
Nov 13, 2019, 12:00 AM
Nov 13, 2019, 12:00 PM
Nov 14, 2019, 12:00 AM
Nov 14, 2019, 12:00 PM
Nov 15, 2019, 12:00 AM
Nov 15, 2019,

Navigazione nell’analisi degli eventi

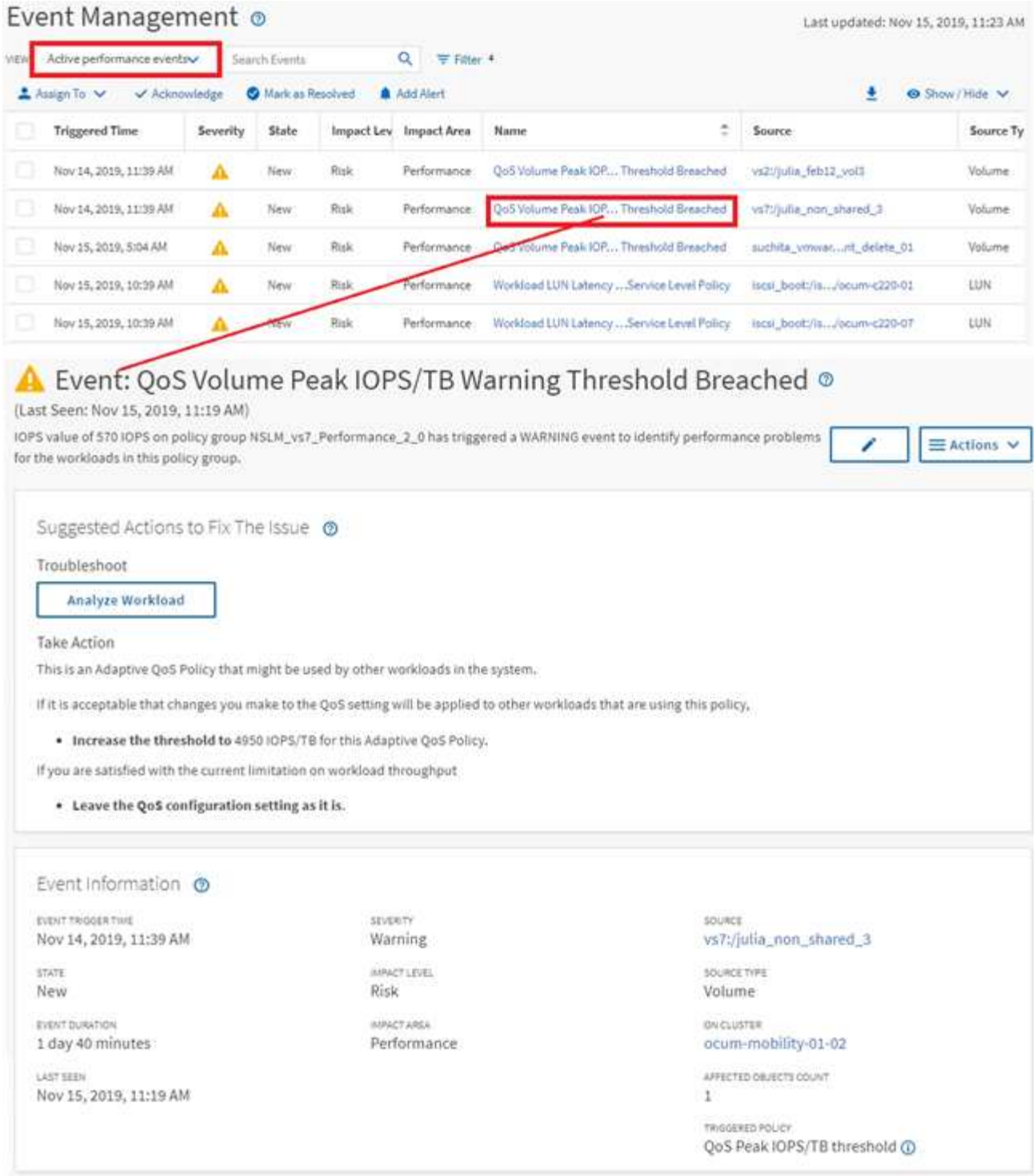
Le pagine dei dettagli degli eventi di Unified Manager offrono uno sguardo approfondito a qualsiasi evento relativo alle performance. Ciò è utile quando si esaminano gli eventi relativi alle performance, quando si esegue la risoluzione dei problemi e quando si ottimizzano le performance del sistema.

A seconda del tipo di evento relativo alle performance, è possibile visualizzare uno dei due tipi di pagine dei dettagli dell’evento:

- Pagina dei dettagli degli eventi per gli eventi definiti dall’utente e dal sistema
- Pagina dei dettagli dell’evento per gli eventi del criterio di soglia dinamico

Questo è un esempio di navigazione nell’analisi degli eventi.

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**.
2. Dal menu View (Visualizza), fare clic su **Active performance events** (Eventi performance attivi).
3. Fare clic sul nome dell’evento che si desidera esaminare e viene visualizzata la pagina Dettagli evento.
4. Visualizzare la descrizione dell’evento e consultare le azioni consigliate (se disponibili) per visualizzare ulteriori dettagli sull’evento che potrebbero essere utili per risolvere il problema. È possibile fare clic sul pulsante **Analyze workload** (analizza carico di lavoro) per visualizzare grafici dettagliati delle performance e analizzare ulteriormente il problema.



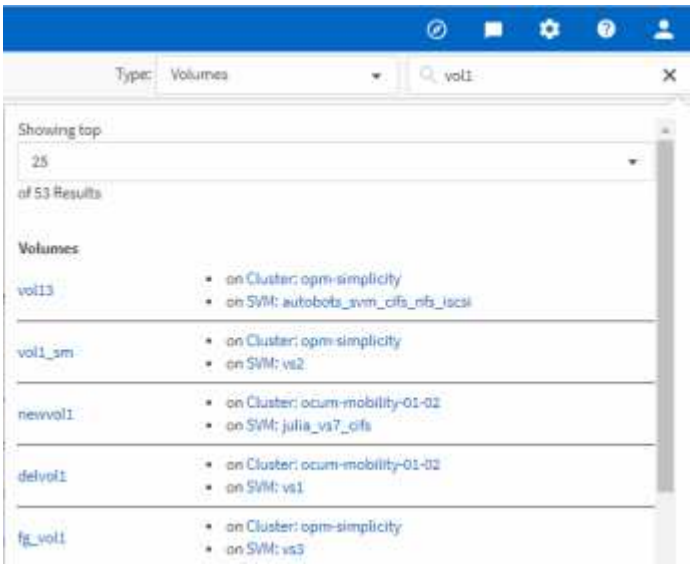
Ricerca di oggetti storage

Per accedere rapidamente a un oggetto specifico, è possibile utilizzare il campo **Search All Storage Objects** (Cerca tutti gli oggetti di storage) nella parte superiore della barra dei menu. Questo metodo di ricerca globale in tutti gli oggetti consente di individuare rapidamente oggetti specifici in base al tipo. I risultati della ricerca sono ordinati in base al tipo di oggetto di storage ed è possibile filtrarli utilizzando il menu a discesa. Una ricerca valida deve contenere almeno tre caratteri.

La ricerca globale visualizza il numero totale di risultati, ma solo i primi 25 risultati sono accessibili. Per questo motivo, la funzionalità di ricerca globale può essere considerata come uno strumento di scelta rapida per trovare elementi specifici se si conoscono gli elementi che si desidera individuare rapidamente. Per risultati di ricerca completi, è possibile utilizzare la ricerca nelle pagine di inventario degli oggetti e la relativa funzionalità di filtraggio associata.

È possibile fare clic sulla casella a discesa e selezionare **tutti** per eseguire contemporaneamente la ricerca in tutti gli oggetti e gli eventi. In alternativa, fare clic sulla casella a discesa per specificare il tipo di oggetto. Digitare un minimo di tre caratteri del nome dell'oggetto o dell'evento nel campo **Cerca tutti gli oggetti di storage**, quindi premere **Invio** per visualizzare i risultati della ricerca, ad esempio:

- Cluster: Nomi dei cluster
- Nodi: Nomi dei nodi
- Aggregati: Nomi di aggregati
- SVM: Nomi SVM
- Volumi: Nomi dei volumi
- LUN: Percorsi LUN



Le LIF e le porte non sono ricercabili nella barra di ricerca globale.

In questo esempio, nella casella a discesa è selezionato il tipo di oggetto Volume. Digitando "vol" nel campo **Search All Storage Objects** viene visualizzato un elenco di tutti i volumi i cui nomi contengono questi caratteri. Per le ricerche di oggetti, è possibile fare clic su qualsiasi risultato di ricerca per accedere alla pagina Performance Explorer dell'oggetto. Per la ricerca degli eventi, facendo clic su un elemento nel risultato della ricerca si accede alla pagina Dettagli evento.

Filtraggio del contenuto della pagina di inventario

È possibile filtrare i dati delle pagine di inventario in Unified Manager per individuare rapidamente i dati in base a criteri specifici. È possibile utilizzare il filtraggio per restringere il contenuto delle pagine di Unified Manager e visualizzare solo i risultati desiderati. Questo offre un metodo molto efficiente per visualizzare solo i dati che ti interessano.

Utilizzare **Filtering** per personalizzare la vista griglia in base alle proprie preferenze. Le opzioni di filtro disponibili si basano sul tipo di oggetto visualizzato nella griglia. Se i filtri sono attualmente applicati, il numero di filtri applicati viene visualizzato a destra del pulsante Filter (filtro).

Sono supportati tre tipi di parametri di filtro.

Parametro	Convalida
Stringa (testo)	Gli operatori sono **contains**, **inizia con**, **termina con** e **non contiene**.
Numero	Gli operatori sono **maggiori di**, **minori di**, **negli ultimi** e **tra**.
Enum (testo)	Gli operatori sono **IS** e **non**.

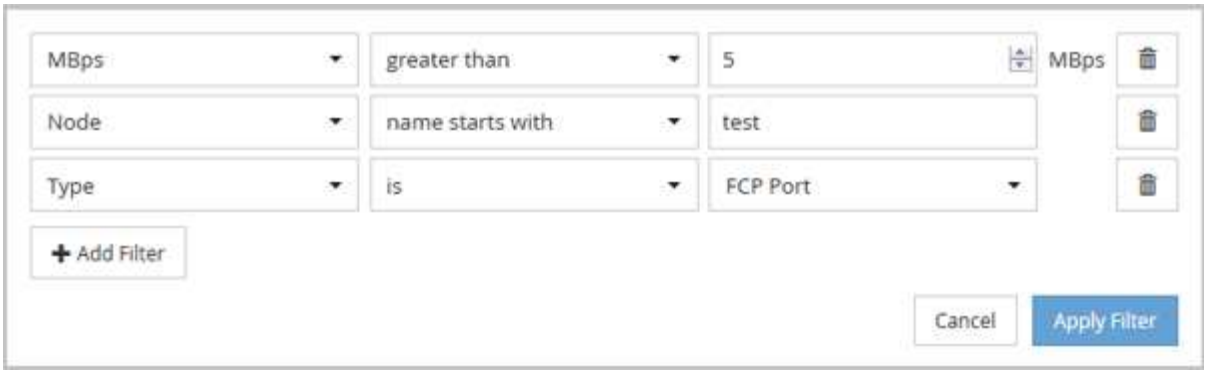
I campi Column (colonna), Operator (operatore) e Value (valore) sono obbligatori per ciascun filtro; i filtri disponibili riflettono le colonne filtrabili nella pagina corrente. Il numero massimo di filtri che è possibile applicare è quattro. I risultati filtrati si basano su parametri di filtro combinati. I risultati filtrati si applicano a tutte le pagine della ricerca filtrata, non solo alla pagina attualmente visualizzata.

È possibile aggiungere filtri utilizzando il pannello di filtraggio.

1. Nella parte superiore della pagina, fare clic sul pulsante **Filter** (filtro). Viene visualizzato il pannello Filtering (filtraggio).
2. Fare clic sull'elenco a discesa a sinistra e selezionare un oggetto, ad esempio *Cluster* o un contatore delle prestazioni.
3. Fare clic sull'elenco a discesa centrale e selezionare l'operatore che si desidera utilizzare.
4. Nell'ultimo elenco, selezionare o inserire un valore per completare il filtro per l'oggetto.
5. Per aggiungere un altro filtro, fare clic su **+Aggiungi filtro**. Viene visualizzato un campo di filtro aggiuntivo. Completare questo filtro seguendo la procedura descritta nei passaggi precedenti. Si noti che quando si aggiunge il quarto filtro, il pulsante **+Aggiungi filtro** non viene più visualizzato.
6. Fare clic su **Applica filtro**. Le opzioni di filtro vengono applicate alla griglia e il numero di filtri viene visualizzato a destra del pulsante Filter (filtro).
7. Utilizzare il pannello di filtraggio per rimuovere i singoli filtri facendo clic sull'icona del cestino a destra del filtro da rimuovere.
8. Per rimuovere tutti i filtri, fare clic su **Reset** nella parte inferiore del pannello di filtraggio.

Esempio di filtraggio

La figura mostra il pannello di filtraggio con tre filtri. Il pulsante **+Aggiungi filtro** viene visualizzato quando si dispone di un numero inferiore al massimo di quattro filtri.



Dopo aver fatto clic su **Apply Filter** (Applica filtro), il pannello Filtering (filtraggio) si chiude, applica i filtri e mostra il numero di filtri applicati (3).

Monitoraggio delle performance del cluster dalla dashboard

Unified Manager Dashboard offre alcuni pannelli che visualizzano lo stato delle performance di alto livello di tutti i cluster monitorati da questa istanza di Unified Manager. Consente di valutare le performance generali dei cluster gestiti e di annotare, individuare o assegnare rapidamente per la risoluzione eventuali eventi specifici identificati.

Informazioni sui pannelli delle performance della dashboard

Unified Manager Dashboard offre alcuni pannelli che visualizzano lo stato delle performance di alto livello per tutti i cluster monitorati nell'ambiente. È possibile scegliere di visualizzare lo stato di tutti i cluster o di un singolo cluster.

Oltre a mostrare le informazioni sulle performance, la maggior parte dei pannelli visualizza anche il numero di eventi attivi in quella categoria e il numero di nuovi eventi aggiunti nelle 24 ore precedenti. Queste informazioni consentono di decidere quali cluster analizzare ulteriormente per risolvere gli eventi segnalati. Facendo clic sugli eventi, vengono visualizzati i primi eventi e viene fornito un collegamento alla pagina dell'inventario Gestione eventi filtrata per visualizzare gli eventi di tale categoria.

I seguenti pannelli forniscono lo stato delle prestazioni.

- **Pannello Performance Capacity**

  Durante la visualizzazione di tutti i cluster, questo pannello visualizza il valore della capacità delle performance per ciascun cluster (media nell'ora precedente) e il numero di giorni fino a quando la capacità delle performance non raggiunge il limite massimo (in base al tasso di crescita giornaliero). Facendo clic sul grafico a barre si accede alla pagina di inventario dei nodi per quel cluster. Si noti che la pagina di inventario dei nodi visualizza la capacità di performance media nelle 72 ore precedenti, pertanto questo valore potrebbe non corrispondere al valore del Dashboard.

  Durante la visualizzazione di un singolo cluster, questo pannello visualizza la capacità delle performance del cluster, gli IOPS totali e i valori di throughput totale.

- **Pannello workload IOPS**

  Quando la gestione attiva del carico di lavoro è attivata e quando si visualizza un singolo cluster, questo

pannello visualizza il numero totale di carichi di lavoro attualmente in esecuzione in un determinato intervallo di IOPS.

- **Pannello workload Performance**

  Quando la gestione attiva del carico di lavoro è attivata, questo pannello visualizza il numero totale di carichi di lavoro conformi e non conformi assegnati a ciascun livello di servizio Performance definito. Facendo clic su un grafico a barre, è possibile accedere ai carichi di lavoro assegnati a tale policy nella pagina carichi di lavoro.

- **Pannello Usage Overview (Panoramica utilizzo)**

  Durante la visualizzazione di tutti i cluster, è possibile scegliere di visualizzare i cluster in base agli IOPS o al throughput più elevati (MB/s).

  Durante la visualizzazione di un singolo cluster, è possibile scegliere di visualizzare i carichi di lavoro del cluster in base agli IOPS o al throughput più elevati (MB/s).

Messaggi e descrizioni dei banner delle performance

Unified Manager può visualizzare i messaggi banner nella pagina Notifiche (dal campanello di notifica) per avvisare l'utente in caso di problemi di stato per un determinato cluster.

Messaggio banner	Descrizione	Risoluzione
`No performance data is being collected from cluster cluster_name. Restart Unified Manager to correct this issue.`	Il servizio di raccolta di Unified Manager si è arrestato e non vengono raccolti dati relativi alle performance da nessun cluster.	Riavviare Unified Manager per risolvere il problema. Se il problema persiste, contattare il supporto tecnico.
`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.`	Attualmente è in esecuzione un ciclo di raccolta della continuità dei dati per recuperare i dati delle performance al di fuori del ciclo di raccolta delle performance del cluster in tempo reale.	Non è richiesta alcuna azione. I dati sulle performance correnti verranno raccolti al termine del ciclo di raccolta della continuità dei dati. Un ciclo di raccolta della continuità dei dati viene eseguito quando viene aggiunto un nuovo cluster o quando Unified Manager non è stato in grado di raccogliere dati sulle performance correnti per qualche motivo.

Modifica dell'intervallo di raccolta delle statistiche delle performance

L'intervallo di raccolta predefinito per le statistiche delle performance è di 5 minuti. È possibile modificare questo intervallo in 10 o 15 minuti se si rileva che le raccolte di cluster di grandi dimensioni non vengono terminate entro il tempo predefinito. Questa

impostazione influisce sulla raccolta di statistiche di tutti i cluster monitorati da questa istanza di Unified Manager.

Cosa ti serve

Per accedere alla console di manutenzione del server Unified Manager, è necessario disporre di un ID utente e di una password autorizzati.

Il problema delle raccolte di statistiche delle performance che non terminano in tempo è indicato dai messaggi banner `Unable to consistently collect from cluster <cluster_name>` oppure `Data collection is taking too long on cluster <cluster_name>`.

È necessario modificare l'intervallo di raccolta solo quando richiesto a causa di un problema di raccolta di statistiche. Non modificare questa impostazione per altri motivi.

> La modifica di questo valore dall'impostazione predefinita di 5 minuti può influire sul numero e sulla frequenza degli eventi relativi alle performance segnalati da Unified Manager. Ad esempio, le soglie di performance definite dal sistema attivano eventi quando il criterio viene superato per 30 minuti. Quando si utilizzano raccolte di 5 minuti, la policy deve essere superata per sei raccolte consecutive. Per le raccolte di 15 minuti, la policy deve essere superata solo per due periodi di raccolta.

Un messaggio nella parte inferiore della pagina Cluster Setup indica l'intervallo corrente di raccolta dei dati statistici.

Fasi

1. Accedere utilizzando SSH come utente di manutenzione all'host di Unified Manager.

   Vengono visualizzati i prompt della console di manutenzione di Unified Manager.

2. Digitare il numero dell'opzione di menu **Performance polling Interval Configuration** (Configurazione intervallo di polling delle prestazioni), quindi premere Invio.
3. Se richiesto, inserire nuovamente la password utente per la manutenzione.
4. Digitare il numero del nuovo intervallo di polling che si desidera impostare, quindi premere Invio.

Se l'intervallo di raccolta di Unified Manager è stato modificato su 10 o 15 minuti e si dispone di una connessione corrente a un provider di dati esterno (ad esempio Graphite), è necessario modificare l'intervallo di trasmissione del provider di dati in modo che sia uguale o superiore all'intervallo di raccolta di Unified Manager.

Risoluzione dei problemi dei carichi di lavoro utilizzando l'analizzatore dei carichi di lavoro

L'analizzatore del carico di lavoro consente di visualizzare importanti criteri di salute e performance per un singolo carico di lavoro su una singola pagina per agevolare la risoluzione dei problemi. Visualizzando tutti gli eventi attuali e passati per un workload, è possibile capire meglio perché il workload potrebbe avere un problema di performance o capacità.

L'utilizzo di questo tool può anche aiutare a determinare se lo storage è la causa di eventuali problemi di performance per un'applicazione o se il problema è causato da un problema di rete o da altri problemi correlati.

È possibile avviare questa funzionalità da diversi punti dell'interfaccia utente:

- Dalla selezione Workload Analysis (analisi carico di lavoro) nel menu di navigazione a sinistra
- Dalla pagina Dettagli evento, fare clic sul pulsante **Analyze workload** (analizza carico di lavoro)
- Da qualsiasi pagina di inventario dei workload (volume, LUN, carico di lavoro, condivisione NFS o condivisione SMB/CIFS), facendo clic sull'icona altro , Quindi **Analyze workload**
- Dalla pagina macchine virtuali, fare clic sul pulsante **Analyze workload** (analizza carico di lavoro) da qualsiasi oggetto Datastore

Quando si avvia lo strumento dal menu di navigazione a sinistra, è possibile immettere il nome di qualsiasi carico di lavoro che si desidera analizzare e selezionare l'intervallo di tempo per il quale si desidera risolvere il problema. Quando si avvia lo strumento da una qualsiasi delle pagine di inventario del carico di lavoro o delle macchine virtuali, il nome del carico di lavoro viene compilato automaticamente e i dati del carico di lavoro vengono visualizzati con l'intervallo di tempo predefinito di 2 ore. Quando si avvia lo strumento dalla pagina Dettagli evento, il nome del carico di lavoro viene compilato automaticamente e vengono visualizzati i dati di 10 giorni.

Quali dati vengono visualizzati dall'analizzatore del carico di lavoro

La pagina dell'analizzatore del carico di lavoro visualizza informazioni sugli eventi correnti che potrebbero influire sul carico di lavoro, consigli per risolvere il problema che causa l'evento e grafici per l'analisi della cronologia delle performance e della capacità.

Nella parte superiore della pagina, specificare il nome del carico di lavoro (volume o LUN) che si desidera analizzare e il periodo di tempo in cui si desidera visualizzare le statistiche. È possibile modificare l'intervallo di tempo in qualsiasi momento se si desidera visualizzare un periodo di tempo più breve o più lungo.

Le altre aree della pagina visualizzano i risultati dell'analisi e i grafici delle prestazioni e della capacità.

> I grafici dei carichi di lavoro per le LUN non forniscono lo stesso livello di statistiche dei grafici per i volumi, quindi noterai delle differenze durante l'analisi di questi due tipi di carichi di lavoro.

- **Area di riepilogo eventi**

  Visualizza una breve panoramica del numero e dei tipi di eventi che si sono verificati nel periodo di tempo. Quando sono presenti eventi provenienti da diverse aree di impatto (ad esempio, performance e capacità), queste informazioni vengono visualizzate in modo da poter selezionare i dettagli per il tipo di evento a cui si è interessati. Fare clic sul tipo di evento per visualizzare un elenco dei nomi degli eventi.

  Se si verifica un solo evento durante il periodo di tempo, viene visualizzato un elenco di suggerimenti per risolvere il problema per alcuni eventi.

- **Cronologia eventi**

  Mostra tutte le occorrenze degli eventi durante l'intervallo di tempo specificato. Posizionare il cursore su ciascun evento per visualizzarne il nome.

  Se si è arrivati a questa pagina facendo clic sul pulsante **Analyze Workload** (analizza carico di lavoro) dalla pagina Event Details (Dettagli evento), l'icona dell'evento selezionato appare più grande in modo da poter identificare l'evento.

- **Area grafici delle performance**

  Visualizza i grafici relativi a latenza, throughput (IOPS e MB/s) e utilizzo (sia per il nodo che per l'aggregato) in base al periodo di tempo selezionato. È possibile fare clic sul collegamento View performance details (Visualizza dettagli sulle prestazioni) per visualizzare la pagina Performance Explorer (Esplora prestazioni) per il carico di lavoro nel caso si desideri eseguire ulteriori analisi.

  - **Latency** Visualizza la latenza per il carico di lavoro nel periodo di tempo selezionato. Il grafico dispone di tre viste che consentono di visualizzare:
    - Latenza **totale**
    - Latenza **breakdown** (suddivisa per letture, scritture e altri processi)
    - **Componenti del cluster** latenza (interrotta per componente del cluster)

Vedere "Componenti del cluster e perché possono essere in conflitto" per una descrizione dei componenti del cluster visualizzati qui. **Throughput Visualizza il throughput IOPS e MB/s per il carico di lavoro nel periodo di tempo selezionato. Il grafico presenta quattro viste che consentono di visualizzare:** * **Throughput totale * throughput ridotto (suddiviso per letture, scritture e altri processi)** * **throughput del cloud** (i MB/s utilizzati per scrivere e leggere i dati dal cloud; Per i carichi di lavoro che stanno tiering della capacità nel cloud) *** IOPS con previsione (una previsione dei valori di throughput IOPS superiori e inferiori previsti per il periodo di tempo), questo grafico mostra anche le impostazioni di soglia massima e minima di throughput della qualità del servizio (QoS), se configurate, In questo modo, è possibile vedere dove il sistema potrebbe limitare intenzionalmente il throughput con le policy di QoS. Utilization** Visualizza l'utilizzo dell'aggregato e del nodo su cui il carico di lavoro viene eseguito nel periodo di tempo selezionato. Da qui è possibile vedere se l'aggregato o il nodo sono utilizzati in modo eccessivo, causando una latenza elevata. Quando si analizzano i volumi FlexGroup, nei grafici di utilizzo sono elencati più nodi e più aggregati.

- **Area del grafico della capacità**

  Visualizza i grafici relativi alla capacità dei dati e alla capacità Snapshot degli ultimi un mese per il carico di lavoro.

  Per i volumi, fare clic sul collegamento View Capacity Details (Visualizza dettagli capacità) per visualizzare la pagina Health Details (Dettagli stato) del carico di lavoro nel caso si desideri eseguire ulteriori analisi. I LUN non forniscono questo collegamento perché non esiste una pagina Health Details per le LUN.

  - **Capacity View** visualizza lo spazio totale disponibile allocato per il carico di lavoro e lo spazio logico utilizzato (dopo tutte le ottimizzazioni NetApp).
  - **Snapshot View** visualizza lo spazio totale riservato per le copie Snapshot e la quantità di spazio attualmente in uso. Tenere presente che i LUN non forniscono una vista Snapshot.
  - **Cloud Tier View** visualizza la capacità utilizzata nel Tier di performance locale e la quantità utilizzata nel Tier di cloud. Questi grafici includono una stima del tempo rimanente prima che la capacità sia piena per questo carico di lavoro. Queste informazioni si basano sull'utilizzo storico e richiedono un minimo di 10 giorni di dati. Quando rimangono meno di 30 giorni di capacità, Unified Manager identifica lo storage come "quasi pieno".

Quando dovrei utilizzare l'analizzatore del carico di lavoro

In genere, si utilizza l'analizzatore del carico di lavoro per risolvere un problema di latenza segnalato da un utente, per analizzare più a fondo un evento o un avviso segnalato o per esplorare un carico di lavoro che si vede funzionare in modo anomalo.

Nel caso in cui gli utenti vi abbiano contattati per affermare che l'applicazione in uso è in esecuzione molto lentamente, è possibile controllare i grafici di latenza, throughput e utilizzo per il carico di lavoro su cui l'applicazione è in esecuzione per verificare se lo storage è la causa del problema di performance. È possibile utilizzare anche il grafico della capacità per vedere se la capacità è bassa perché un sistema ONTAP in cui la capacità è utilizzata oltre il 85% può causare problemi di performance. Questi grafici consentono di determinare se il problema è causato dallo storage, da un problema di rete o da altri problemi correlati.

Nel caso in cui Unified Manager abbia generato un evento relativo alle performance e si desideri esaminare la causa del problema in modo più approfondito, è possibile avviare l'analizzatore del carico di lavoro dalla pagina Dettagli evento facendo clic sul pulsante **Analyze workload** per ricercare la latenza, il throughput, e le tendenze della capacità per il carico di lavoro.

Nel caso in cui si noti un workload che sembra funzionare in modo anomalo durante la visualizzazione di qualsiasi pagina di inventario dei workload (volume, LUN, carico di lavoro, condivisione NFS o condivisione SMB/CIFS), è possibile fare clic sull'icona altro , Quindi **Analyze workload** per aprire la pagina workload Analysis (analisi del carico di lavoro) per esaminare ulteriormente il carico di lavoro.

Utilizzo dell'analizzatore del carico di lavoro

Esistono diversi modi per avviare l'analizzatore del carico di lavoro dall'interfaccia utente. Di seguito viene descritto l'avvio dello strumento dal riquadro di navigazione a sinistra.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **analisi del carico di lavoro**.

   Viene visualizzata la pagina workload Analysis (analisi del carico di lavoro).

2. Se si conosce il nome del carico di lavoro, immetterlo. Se non si è sicuri del nome completo, immettere un minimo di 3 caratteri e il sistema visualizza un elenco di carichi di lavoro corrispondenti alla stringa.
3. Selezionare l'intervallo di tempo se si desidera visualizzare le statistiche per un periodo superiore alle 2 ore predefinite e fare clic su **Apply** (Applica).
4. Visualizzare l'area Summary (Riepilogo) per visualizzare gli eventi che si sono verificati durante l'intervallo di tempo.
5. Visualizza i grafici delle performance e della capacità per vedere quando una qualsiasi delle metriche è anomala e vedere se gli eventi sono allineati con la voce anomala.

Monitoraggio delle performance del cluster dalla pagina di destinazione del cluster di performance

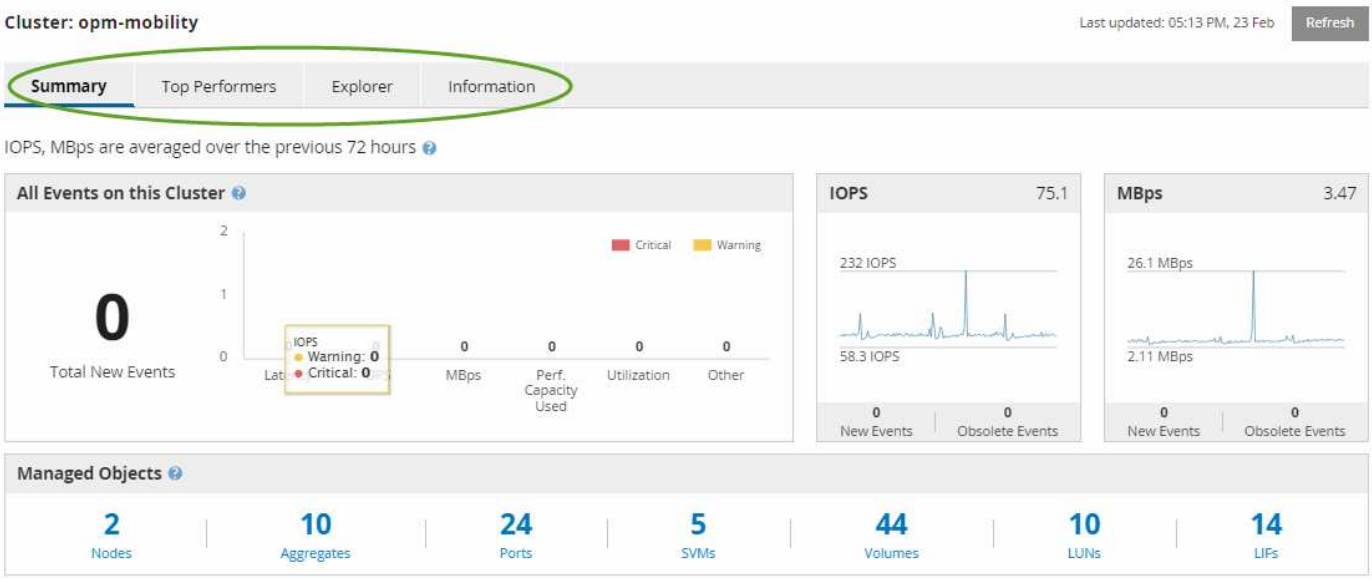
La pagina Landing di Performance Cluster visualizza lo stato delle performance di alto livello di un cluster selezionato che viene monitorato da un'istanza di Unified Manager. Questa pagina consente di valutare le performance generali di un cluster specifico e di annotare, individuare o assegnare rapidamente per la risoluzione gli eventi specifici del cluster identificati.

Informazioni sulla pagina di destinazione del cluster di performance

La landing page Performance Cluster offre una panoramica delle performance di alto livello di un cluster selezionato, con particolare attenzione allo stato delle performance

dei primi 10 oggetti all'interno del cluster. I problemi di performance vengono visualizzati nella parte superiore della pagina, nel pannello tutti gli eventi di questo cluster.

La landing page Performance Cluster fornisce una panoramica di alto livello di ogni cluster gestito da un'istanza di Unified Manager. Questa pagina fornisce informazioni su eventi e performance e consente di monitorare e risolvere i problemi dei cluster. L'immagine seguente mostra un esempio della pagina di destinazione del cluster Performance Cluster per il cluster chiamato opm-mobility:



Il numero di eventi nella pagina Cluster Summary (Riepilogo cluster) potrebbe non corrispondere al numero di eventi nella pagina Performance Event Inventory (inventario eventi performance). Questo perché la pagina Cluster Summary (Riepilogo cluster) può mostrare un evento ciascuno nelle barre di latenza e utilizzo quando le policy di soglia della combinazione sono state violate, mentre la pagina Performance Event Inventory (inventario eventi performance) mostra un solo evento quando una policy di combinazione è stata violata.

Se un cluster è stato rimosso dalla gestione da Unified Manager, lo stato **removed** viene visualizzato a destra del nome del cluster nella parte superiore della pagina.

Pagina di destinazione del cluster di performance

La pagina Landing di Performance Cluster visualizza lo stato delle performance di alto livello di un cluster selezionato. La pagina consente di accedere ai dettagli completi di ciascun contatore di performance per gli oggetti di storage nel cluster selezionato.

La landing page del cluster di performance include quattro schede che separano i dettagli del cluster in quattro aree di informazioni:

- Pagina di riepilogo
  - Pannello Cluster Events (Eventi cluster)
  - Grafici delle performance di MB/s e IOPS
  - Pannello Managed Objects (oggetti gestiti)
- Pagina Top Performers
- Pagina Explorer

- Pagina informativa

Pagina Performance Cluster Summary

La pagina Performance Cluster Summary (Riepilogo cluster di prestazioni) fornisce un riepilogo degli eventi attivi, delle performance IOPS e delle performance MB/s per un cluster. Questa pagina include anche il conteggio totale degli oggetti di storage nel cluster.

Pannello degli eventi relativi alle performance del cluster

Il pannello Cluster performance events (Eventi delle performance del cluster) visualizza le statistiche delle performance e tutti gli eventi attivi per il cluster. Ciò risulta particolarmente utile quando si monitorano i cluster e tutte le performance e gli eventi correlati al cluster.

Tutti gli eventi in questo pannello del cluster

Il riquadro tutti gli eventi di questo cluster visualizza tutti gli eventi attivi relativi alle prestazioni del cluster per le 72 ore precedenti. Il totale degli eventi attivi viene visualizzato all'estrema sinistra; questo numero rappresenta il totale di tutti gli eventi nuovi e riconosciuti per tutti gli oggetti di storage in questo cluster. È possibile fare clic sul collegamento Total Active Events (Eventi attivi totali) per accedere alla pagina Events Inventory (inventario eventi), che viene filtrata per visualizzare questi eventi.

Il grafico a barre Total Active Events (Eventi attivi totali) del cluster visualizza il numero totale di eventi critici e di avviso attivi:

- Latenza (totale per nodi, aggregati, SVM, volumi, LUN, e spazi dei nomi)
- IOPS (totale per cluster, nodi, aggregati, SVM, volumi, LUN e spazi dei nomi)
- MB/s (totale per cluster, nodi, aggregati, SVM, volumi, LUN, namespace, porte e LIFF)
- Capacità di performance utilizzata (totale per nodi e aggregati)
- Utilizzo (totale per nodi, aggregati e porte)
- Altro (rapporto di perdita della cache per i volumi)

L'elenco contiene eventi attivi relativi alle performance attivati da criteri di soglia definiti dall'utente, criteri di soglia definiti dal sistema e soglie dinamiche.

I dati del grafico (barre dei contatori verticali) vengono visualizzati in rosso ( ) per gli eventi critici e giallo ( ) per gli eventi di avviso. Posizionare il cursore su ciascuna barra verticale del contatore per visualizzare il tipo e il numero di eventi effettivi. È possibile fare clic su **Refresh** (Aggiorna) per aggiornare i dati del pannello del contatore.

È possibile visualizzare o nascondere gli eventi critici e di avviso nel grafico delle prestazioni degli eventi attivi totali facendo clic sulle icone **critico** e **Avviso** nella legenda. Se si nascondono determinati tipi di eventi, le icone della legenda vengono visualizzate in grigio.

Pannelli dei contatori

I pannelli dei contatori visualizzano gli eventi relativi alle prestazioni e all'attività del cluster per le 72 ore precedenti e includono i seguenti contatori:

- **Pannello contatore IOPS**

  IOPS indica la velocità operativa del cluster in numero di operazioni di input/output al secondo. Questo pannello del contatore fornisce una panoramica di alto livello dello stato degli IOPS del cluster per il periodo di 72 ore precedente. È possibile posizionare il cursore sulla linea di trend del grafico per visualizzare il valore IOPS per un tempo specifico.

- **Pannello contatore MB/s**

  MB/s indica la quantità di dati trasferiti da e verso il cluster in megabyte al secondo. Questo pannello del contatore fornisce una panoramica di alto livello dello stato dei MB/s del cluster per il periodo di 72 ore precedente. È possibile posizionare il cursore sulla linea di trend del grafico per visualizzare il valore in MB/s per un tempo specifico.

Il numero in alto a destra del grafico nella barra grigia è il valore medio delle ultime 72 ore. I numeri visualizzati nella parte inferiore e superiore del grafico a linee di trend sono i valori minimi e massimi per le ultime 72 ore. La barra grigia sotto il grafico contiene il numero di eventi attivi (nuovi e riconosciuti) e obsoleti degli ultimi 72 ore.

I pannelli dei contatori contengono due tipi di eventi:

- **Attivo**

  Indica che l'evento di performance è attualmente attivo (nuovo o confermato). Il problema che causa l'evento non è stato risolto o non è stato risolto. Il contatore delle performance per l'oggetto storage rimane al di sopra della soglia di performance.

- **Obsoleto**

  Indica che l'evento non è più attivo. Il problema che ha causato l'evento è stato risolto o risolto. Il contatore delle performance per l'oggetto storage non è più al di sopra della soglia di performance.

Per **Eventi attivi**, se è presente un evento, è possibile posizionare il cursore sull'icona dell'evento e fare clic sul numero dell'evento per accedere alla pagina Dettagli evento appropriata. Se sono presenti più eventi, è possibile fare clic su **View All Events** (Visualizza tutti gli eventi) per visualizzare la pagina Events Inventory (inventario eventi), che viene filtrata per visualizzare tutti gli eventi per il tipo di contatore a oggetti selezionato.

Pannello Managed Objects (oggetti gestiti)

Il riquadro Managed Objects della scheda Performance Summary fornisce una panoramica di primo livello dei tipi di oggetti di storage e dei conteggi per il cluster. Questo riquadro consente di tenere traccia dello stato degli oggetti in ciascun cluster.

Il numero di oggetti gestiti è dato point-in-time dell'ultimo periodo di raccolta. I nuovi oggetti vengono rilevati a intervalli di 15 minuti.

Facendo clic sul numero collegato per qualsiasi tipo di oggetto viene visualizzata la pagina di inventario delle performance degli oggetti per quel tipo di oggetto. La pagina dell'inventario degli oggetti viene filtrata per visualizzare solo gli oggetti di questo cluster.

Gli oggetti gestiti sono:

- **Nodi**

Un sistema fisico in un cluster.

- **Aggregati**

  Un set di più gruppi RAID (Redundant Array of Independent Disks) che possono essere gestiti come una singola unità per la protezione e il provisioning.

- **Porte**

  Punto di connessione fisico sui nodi utilizzato per la connessione ad altri dispositivi in una rete.

- **Storage VM**

  Una macchina virtuale che fornisce l'accesso alla rete attraverso indirizzi di rete univoci. Una SVM potrebbe servire i dati da uno spazio dei nomi distinto ed è amministrabile separatamente dal resto del cluster.

- **Volumi**

  Entità logica che contiene dati utente accessibili attraverso uno o più protocolli di accesso supportati. Il conteggio include sia volumi FlexVol che volumi FlexGroup; non include i componenti FlexGroup.

- **LUN**

  L'identificatore di un'unità logica Fibre Channel (FC) o di un'unità logica iSCSI. Un'unità logica corrisponde in genere a un volume di storage ed è rappresentata all'interno di un sistema operativo del computer come dispositivo.

- **Interfacce di rete**

  Interfaccia di rete logica che rappresenta un access point di rete per un nodo. Il numero include tutti i tipi di interfaccia.

Pagina Top Performers

La pagina Top Performer visualizza gli oggetti storage con le performance più elevate o più basse, in base al contatore delle performance selezionato. Ad esempio, nella categoria Storage VM, è possibile visualizzare le SVM con IOPS più elevati, latenza più elevata o MB/s più bassi Questa pagina mostra anche se uno qualsiasi dei migliori esecutori ha eventi di performance attivi (nuovi o riconosciuti).

La pagina Top Performer visualizza un massimo di 10 oggetti. Si noti che l'oggetto Volume include volumi FlexVol e volumi FlexGroup.

- **Intervallo di tempo**

  È possibile selezionare un intervallo di tempo per visualizzare le prestazioni principali; l'intervallo di tempo selezionato si applica a tutti gli oggetti di storage. Intervalli di tempo disponibili:

  - Ultima ora
  - Ultime 24 ore
  - Ultime 72 ore (impostazione predefinita)

- Ultimi 7 giorni

- **Metrico**

  Fare clic sul menu **Metrico** per selezionare un contatore diverso. Le opzioni del contatore sono univoche per il tipo di oggetto. Ad esempio, i contatori disponibili per l'oggetto **Volumes** sono **Latency**, **IOPS** e **MB/s**. La modifica del contatore consente di ricaricare i dati del pannello con i principali performer in base al contatore selezionato.

  Contatori disponibili:

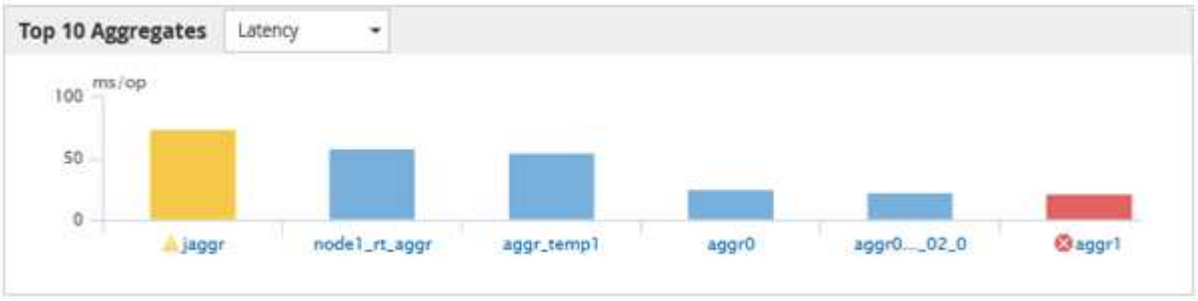
  - Latenza
  - IOPS
  - MB/s.
  - Capacità di performance utilizzata (per nodi e aggregati)
  - Utilizzo (per nodi e aggregati)

- **Ordina**

  Fare clic sul menu **Ordina** per selezionare un ordine crescente o decrescente per l'oggetto e il contatore selezionati. Le opzioni disponibili sono: Da **massimo a minimo** e da **minimo a massimo**. Queste opzioni consentono di visualizzare gli oggetti con le performance più elevate o più basse.

- **Barra del contatore**

  La barra del contatore nel grafico mostra le statistiche delle performance per ciascun oggetto, rappresentato come una barra per quell'elemento. I grafici a barre sono codificati a colori. Se il contatore non supera una soglia di performance, la barra del contatore viene visualizzata in blu. Se è attiva una violazione di soglia (un evento nuovo o confermato), la barra viene visualizzata a colori per l'evento: Gli eventi di avviso vengono visualizzati in giallo ( ) e gli eventi critici sono visualizzati in rosso ( ). Le violazioni di soglia sono inoltre indicate dalle icone degli indicatori degli eventi di severità per gli eventi critici e di avviso.



  Per ciascun grafico, l'asse X visualizza le prestazioni superiori per il tipo di oggetto selezionato. L'asse Y visualizza le unità applicabili al contatore selezionato. Facendo clic sul collegamento relativo al nome dell'oggetto sotto ciascun elemento del grafico a barre verticale, si accede alla pagina di destinazione delle prestazioni per l'oggetto selezionato.

- **Indicatore di evento di severità**

  L'icona dell'indicatore **evento di severità** viene visualizzata a sinistra del nome di un oggetto per Active Critical ( ) o avviso ( ) nei grafici con le migliori performance. Fare clic sull'icona dell'indicatore **evento di severità** per visualizzare:

- **Un evento**

  Consente di accedere alla pagina Dettagli evento relativa all'evento.

- **Due o più eventi**

  Consente di accedere alla pagina Event Inventory (inventario eventi), che viene filtrata per visualizzare tutti gli eventi per l'oggetto selezionato.

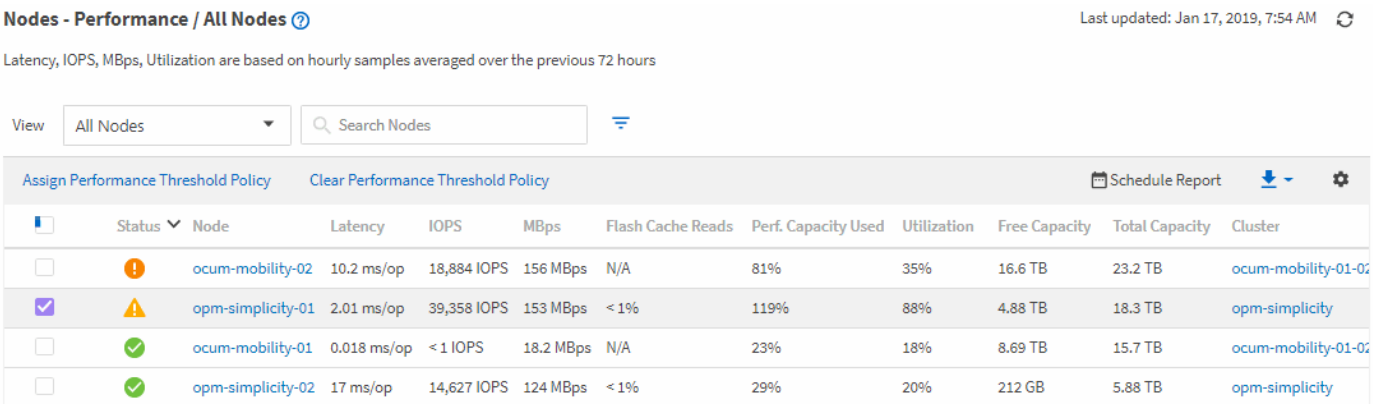
- **Pulsante Esporta**

  Crea un `.csv` file contenente i dati visualizzati nella barra del contatore. È possibile scegliere di creare il file per il singolo cluster visualizzato o per tutti i cluster del data center.

Monitoraggio delle performance tramite le pagine Performance Inventory

Le pagine delle performance dell'inventario degli oggetti visualizzano informazioni sulle performance, eventi delle performance e stato degli oggetti per tutti gli oggetti all'interno di una categoria di tipi di oggetti. In questo modo viene fornita una panoramica immediata dello stato delle performance di ciascun oggetto all'interno di un cluster, ad esempio per tutti i nodi o tutti i volumi.

Le pagine sulle performance dell'inventario degli oggetti offrono una panoramica di alto livello dello stato degli oggetti, consentendo di valutare le performance complessive di tutti gli oggetti e di confrontare i dati sulle performance degli oggetti. Puoi perfezionare il contenuto delle pagine di inventario degli oggetti ricercando, ordinando e filtrando. Ciò risulta vantaggioso quando si monitorano e si gestiscono le performance degli oggetti, in quanto consente di individuare rapidamente gli oggetti con problemi di performance e di avviare il processo di troubleshooting.



Per impostazione predefinita, gli oggetti nelle pagine di inventario delle performance vengono ordinati in base alla criticità delle performance degli oggetti. Gli oggetti con nuovi eventi critici relativi alle performance vengono elencati per primi e gli oggetti con eventi di avviso vengono elencati per secondi. Ciò fornisce un'indicazione visiva immediata dei problemi che devono essere risolti. Tutti i dati relativi alle performance si basano su una media di 72 ore.

È possibile navigare facilmente dalla pagina delle prestazioni dell'inventario degli oggetti alla pagina dei dettagli di un oggetto facendo clic sul nome dell'oggetto nella colonna Nome oggetto. Ad esempio, nella pagina di inventario Performance/All Nodes, fare clic su un oggetto nodo nella colonna **Nodes**. La pagina dei dettagli dell'oggetto fornisce informazioni e dettagli approfonditi sull'oggetto selezionato, incluso il confronto affiancato

degli eventi attivi.

Visualizzazione delle pagine di inventario delle performance per tutti gli oggetti di storage

Le pagine dell'inventario delle performance consentono di visualizzare un riepilogo delle informazioni sulle performance relative a ciascuno degli oggetti di storage disponibili, ad esempio cluster, aggregati, volumi e così via. È possibile collegarsi alle pagine Dettagli oggetto Performance per visualizzare informazioni dettagliate relative a un particolare oggetto.

Per impostazione predefinita, gli oggetti nelle pagine di visualizzazione vengono ordinati in base alla criticità degli eventi. Gli oggetti con eventi critici vengono elencati per primi e gli oggetti con eventi di avviso vengono elencati per secondi. Ciò fornisce un'indicazione visiva immediata dei problemi che devono essere risolti.

È possibile esportare i dati da queste pagine in valori separati da virgole (`.csv`), file Microsoft Excel (`.xlsx`), o. (`.pdf`) Utilizzando il pulsante **Report**, quindi utilizzare i dati esportati per creare i report. Inoltre, è possibile personalizzare la pagina e pianificare la creazione e l'invio di un report tramite e-mail utilizzando il pulsante **Report pianificati**.

Tutti i campi di queste pagine possono essere utilizzati nelle visualizzazioni personalizzate e nei report. Alcuni campi sono collegati a pagine correlate per una visualizzazione più dettagliata.

Performance: Vista di tutti i cluster

La vista Performance: All Clusters (prestazioni: Tutti i cluster) visualizza una panoramica degli eventi di performance, dei dati e delle informazioni di configurazione per ciascun cluster monitorato da un'istanza di Unified Manager. Questa pagina consente di monitorare le performance dei cluster e di risolvere i problemi relativi alle performance e agli eventi di soglia.

È possibile assegnare criteri di soglia delle performance a qualsiasi oggetto presente nelle pagine di inventario degli oggetti o cancellare i criteri di soglia utilizzando i pulsanti **Assign Performance Threshold Policy** e **Clear Performance Threshold Policy**.

Di seguito sono riportati alcuni campi importanti della vista Performance: All Clusters (prestazioni: Tutti i cluster).

- Cluster FQDN (FQDN, Fully Qualified Domain Name): Il nome di dominio completo (FQDN, Fully Qualified Domain Name) del cluster.
- IOPS: Le operazioni di input/output al secondo sul cluster.
- MB/s: Il throughput sul cluster, misurato in MIB al secondo.
- Capacità: Capacità libera e totale in GiB.
- Host Name (Nome host) o IP Address (Indirizzo IP): Nome host o indirizzo IP (IPv4 o IPv6) della LIF di gestione del cluster.
- Versione del sistema operativo: La versione del software ONTAP installata nel cluster.

> Se nei nodi del cluster sono installate versioni diverse del software ONTAP, viene visualizzato il numero di versione più basso. È possibile visualizzare la versione di ONTAP installata su ciascun nodo dalla vista prestazioni: Tutti i nodi.

- Threshold Policy (criterio di soglia): Il criterio o i criteri di soglia delle performance definiti dall'utente che sono attivi su questo oggetto di storage. È possibile posizionare il cursore sui nomi dei criteri contenenti i puntini di sospensione (…) per visualizzare il nome completo del criterio o l'elenco dei nomi dei criteri assegnati. I pulsanti Assign Performance Threshold Policy (Assegna policy soglia prestazioni) e Clear Performance Threshold Policy (Cancella policy soglia prestazioni) rimangono disattivati finché non si selezionano uno o più oggetti facendo clic sulle caselle di controllo situate all'estrema sinistra.

Performance (prestazioni): Vista di tutti i volumi

La vista performance: All Volumes (prestazioni: Tutti i volumi) visualizza una panoramica degli eventi relativi alle performance, dei dati dei contatori e delle informazioni di configurazione per ciascun volume FlexVol e FlexGroup monitorato da un'istanza di Unified Manager. In questo modo è possibile monitorare rapidamente le performance dei volumi e risolvere i problemi di performance e gli eventi di soglia.

Se si desidera analizzare la latenza e il throughput di un oggetto specifico, fare clic sul pulsante altre opzioni ⋮ Quindi, **Analyze workload** ed è possibile visualizzare i grafici relativi a performance e capacità nella pagina workload Analysis. È possibile visualizzare i dettagli in System Manager, se si dispone di credenziali valide per System Manager.

ⓘ Per i volumi di data Protection (DP), vengono visualizzati solo i valori dei contatori per il traffico generato dall'utente. I volumi root non vengono visualizzati in questa pagina.

Di seguito sono riportati alcuni campi importanti della vista Performance: All Volumes (prestazioni: Tutti i volumi).

- Stile: FlexVol o FlexGroup.
- Latenza: Per i volumi FlexVol, si tratta del tempo di risposta medio del volume per tutte le richieste di i/o, espresso in millisecondi per operazione. Per i volumi FlexGroup, si tratta della latenza media di tutti i volumi costituenti.
- IOPS/TB: Il numero di operazioni di input/output elaborate al secondo in base allo spazio totale consumato dal carico di lavoro, in terabyte. Questo contatore misura la quantità di performance che può essere erogata da una determinata quantità di capacità di storage.
- IOPS: Per i volumi FlexVol, indica il numero di operazioni di input/output al secondo per il volume. Per i volumi FlexGroup, si tratta della somma degli IOPS per tutti i volumi costituenti.
- MB/s: Per i volumi FlexVol, si tratta del throughput sul volume, misurato in megabyte al secondo. Per i volumi FlexGroup, si tratta della somma di MB/s per tutti i volumi costituenti.
- Capacità: Capacità libera e totale in GiB.

Per ulteriori informazioni, consultare i seguenti collegamenti:

- "Assegnazione di criteri di soglia delle performance agli oggetti di storage"
- "Rimozione dei criteri di soglia delle performance dagli oggetti storage"
- "Tipi di workload monitorati da Unified Manager"
- "Visualizzazione delle impostazioni del gruppo di criteri QoS applicate a volumi o LUN specifici"
- "Comprendere le raccomandazioni di Unified Manager per il Tier dei dati nel cloud"
- "Visualizzazione dei grafici delle performance per confrontare volumi o LUN che si trovano nello stesso gruppo di criteri QoS"

Performance: Vista di tutti gli aggregati

La vista Performance: All aggregates (prestazioni: Tutti gli aggregati) visualizza una panoramica degli eventi di performance, dei dati e delle informazioni di configurazione per ciascun aggregato monitorato da un'istanza di Unified Manager. Questa pagina consente di monitorare le performance degli aggregati e di risolvere i problemi relativi alle performance e agli eventi di soglia.

Di seguito sono riportati alcuni campi importanti della vista Performance: All aggregates (prestazioni: Tutti gli aggregati).

- Tipo: Il tipo di aggregato:
  - DISCO RIGIDO
  - Ibrido. Combina HDD e SSD, ma Flash Pool non è stato attivato.
  - Ibrido (Flash Pool). Combina HDD e SSD ed è stato attivato Flash Pool.
  - SSD
  - SSD (FabricPool). Combina SSD e un Tier cloud
  - Disco rigido (FabricPool). Combina HDD e un Tier cloud
  - VMDisk (SDS). Dischi virtuali all'interno di una macchina virtuale
  - VMDisk (FabricPool). Combina dischi virtuali e un Tier cloud
  - LUN (FlexArray)
- Inactive Data Reporting (Report dati inattivi): Indica se la funzionalità di reporting dei dati inattivi è attivata o disattivata su questo aggregato. Quando questa opzione è attivata, i volumi di questo aggregato visualizzano la quantità di dati cold nella vista Performance: All Volumes (prestazioni: Tutti i volumi). Il valore in questo campo è "N/A" quando la versione di ONTAP non supporta il reporting dei dati inattivi.
- Threshold Policy (criterio di soglia): Il criterio o i criteri di soglia delle performance definiti dall'utente che sono attivi su questo oggetto di storage. È possibile posizionare il cursore sui nomi dei criteri contenenti i puntini di sospensione (…) per visualizzare il nome completo del criterio o l'elenco dei nomi dei criteri assegnati. I pulsanti Assign Performance Threshold Policy (Assegna policy soglia prestazioni) e Clear Performance Threshold Policy (Cancella policy soglia prestazioni) rimangono disattivati finché non si selezionano uno o più oggetti facendo clic sulle caselle di controllo situate all'estrema sinistra. Per ulteriori informazioni, consultare i seguenti collegamenti:
- "Assegnazione di criteri di soglia delle performance agli oggetti di storage"
- "Rimozione dei criteri di soglia delle performance dagli oggetti storage"

Performance: Vista di tutti i nodi

La vista Performance: All Nodes (prestazioni: Tutti i nodi) visualizza una panoramica degli eventi di performance, dei dati e delle informazioni di configurazione per ciascun nodo monitorato da un'istanza di Unified Manager. In questo modo è possibile monitorare rapidamente le performance dei nodi e risolvere i problemi di performance e gli eventi di soglia.

> Flash cache Read restituisce la percentuale di operazioni di lettura sul nodo che sono soddisfatte dalla cache, invece di essere restituite dal disco. I dati di Flash cache vengono visualizzati solo per i nodi e solo quando nel nodo è installato un modulo Flash cache.

Nel menu **Report**, l'opzione **hardware Inventory Report** viene fornita quando Unified Manager e i cluster gestiti vengono installati in un sito senza connettività di rete esterna. Questo pulsante genera un file .csv che contiene un elenco completo di informazioni su cluster e nodi, ad esempio numeri di modello e di serie

dell'hardware, tipi e conteggi di dischi, licenze installate e altro ancora. Questa funzionalità di reporting è utile per il rinnovo del contratto all'interno di siti sicuri non connessi alla piattaforma NetApp Active IQ. È possibile assegnare criteri di soglia delle performance a qualsiasi oggetto presente nelle pagine di inventario degli oggetti o cancellare i criteri di soglia utilizzando i pulsanti **Assign Performance Threshold Policy** e **Clear Performance Threshold Policy**.

Per ulteriori informazioni, consultare i seguenti collegamenti:

- "Assegnazione di criteri di soglia delle performance agli oggetti di storage"
- "Rimozione dei criteri di soglia delle performance dagli oggetti storage"
- "Generazione di un report sull'inventario hardware per il rinnovo del contratto"

Performance: Vista di tutte le VM di storage

La vista Performance: All Storage VM (prestazioni: Tutte le macchine virtuali dello storage) visualizza una panoramica degli eventi di performance, dei dati e delle informazioni di configurazione per ciascuna macchina virtuale dello storage (SVM) monitorata da un'istanza di Unified Manager. In questo modo è possibile monitorare rapidamente le performance delle SVM e risolvere i problemi di performance e gli eventi di soglia. Il campo latenza in questa pagina riporta il tempo di risposta medio per tutte le richieste di i/o, espresso in millisecondi per operazione.

Le SVM elencate in questa pagina includono solo SVM di dati e cluster. Unified Manager non utilizza o visualizza le SVM di amministrazione o nodo.

Per ulteriori informazioni, consultare i seguenti collegamenti:

- "Assegnazione di criteri di soglia delle performance agli oggetti di storage"
- "Rimozione dei criteri di soglia delle performance dagli oggetti storage"

Performance: Vista di tutti i LUN

La vista Performance: All LUN visualizza una panoramica degli eventi delle performance, dei dati e delle informazioni di configurazione per ogni LUN monitorato da un'istanza di Unified Manager. In questo modo è possibile monitorare rapidamente le performance dei LUN e risolvere i problemi di performance e gli eventi di soglia.

Se si desidera analizzare la latenza e il throughput di un oggetto specifico, fare clic sull'icona Altro ⋮, Quindi **Analyze workload** ed è possibile visualizzare i grafici relativi a performance e capacità nella pagina **workload Analysis**.

Per ulteriori informazioni, consultare i seguenti collegamenti:

- "Monitoraggio delle LUN in una relazione Consistency Group"
- "Provisioning dei LUN"
- "Assegnazione di criteri di soglia delle performance agli oggetti di storage"
- "Rimozione dei criteri di soglia delle performance dagli oggetti storage"
- "Visualizzazione di volumi o LUN che si trovano nello stesso gruppo di criteri QoS".
- "Visualizzazione delle impostazioni del gruppo di criteri QoS applicate a volumi o LUN specifici"
- "Provisioning delle LUN tramite API"

Performance (prestazioni): Visualizzazione di tutti gli spazi dei nomi NVMe

La vista Performance: All NVMe Namespaces (prestazioni: Tutti gli spazi dei nomi NVMe) visualizza una panoramica degli eventi di performance, dei dati e delle informazioni di configurazione per ogni spazio dei nomi NVMe monitorato da un'istanza di Unified Manager. Ciò consente di monitorare rapidamente le performance e lo stato dei namespace e di risolvere i problemi e gli eventi di soglia.

Vengono riportate, tra le altre, le seguenti informazioni: Lo stato corrente dello spazio dei nomi. * Offline - non è consentito l'accesso in lettura o scrittura allo spazio dei nomi. * Online - è consentito l'accesso in lettura e scrittura allo spazio dei nomi. * NVFail - lo spazio dei nomi è stato automaticamente disattivato a causa di un errore della NVRAM. * Errore di spazio - lo spazio dello spazio dei nomi è esaurito.

Per ulteriori informazioni, consultare i seguenti collegamenti:

- "Assegnazione di criteri di soglia delle performance agli oggetti di storage"
- "Rimozione dei criteri di soglia delle performance dagli oggetti storage"

Performance (prestazioni): Vista All Network Interface (tutte le interfacce di rete)

La vista Performance: All Network Interfaces (prestazioni: Tutte le interfacce di rete) visualizza una panoramica degli eventi relativi alle performance, dei dati e delle informazioni di configurazione per ciascuna interfaccia di rete (LIF) monitorata da questa istanza di Unified Manager. Questa pagina consente di monitorare rapidamente le performance delle interfacce e di risolvere i problemi di performance e gli eventi di soglia. Di seguito sono riportati alcuni campi importanti della vista Performance: All Network Interfaces (prestazioni: Tutte le interfacce di rete).

- IOPS: Le operazioni di input/output al secondo. IOPS non è applicabile a LIF NFS e LIF CIFS e viene visualizzato come N/D per questi tipi.
- Latency (latenza): Tempo di risposta medio per tutte le richieste di i/o, espresso in millisecondi per operazione. La latenza non è applicabile a LIF NFS e LIF CIFS e viene visualizzata come N/A per questi tipi.
- Home Location (posizione iniziale): La posizione iniziale dell'interfaccia, visualizzata come nome del nodo e nome della porta, separata dai due punti (:). Se la posizione viene visualizzata con i puntini di sospensione (…), è possibile posizionare il cursore sul nome della posizione per visualizzare l'intera posizione.
- Current Location (posizione corrente): La posizione corrente dell'interfaccia, visualizzata come nome del nodo e nome della porta, separata dai due punti (:). Se la posizione viene visualizzata con i puntini di sospensione (…), è possibile posizionare il cursore sul nome della posizione per visualizzare l'intera posizione.
- Ruolo: Ruolo dell'interfaccia: Dati, cluster, gestione dei nodi o Intercluster.

Le interfacce elencate in questa pagina includono Data LIF, Cluster LIF, Node Management LIF e Intercluster LIF. Unified Manager non utilizza o visualizza le LIF di sistema.

Performance: Vista All Ports (prestazioni: Tutte le porte

La vista Performance: All Ports (prestazioni: Tutte le porte) visualizza una panoramica degli eventi di performance, dei dati e delle informazioni di configurazione per ciascuna porta monitorata da un'istanza di Unified Manager. In questo modo è possibile monitorare rapidamente le performance delle porte e risolvere i problemi di performance e gli eventi di soglia. Per un ruolo di porta, viene visualizzata la funzione della porta di rete, Data (dati) o Cluster (cluster). Le porte FCP non possono avere un ruolo e il ruolo viene visualizzato come N/A.

I valori dei contatori delle prestazioni vengono visualizzati solo per le porte fisiche. I valori dei contatori non vengono visualizzati per VLAN o gruppi di interfacce.

Per ulteriori informazioni, consultare i seguenti collegamenti:

- "Assegnazione di criteri di soglia delle performance agli oggetti di storage"
- "Rimozione dei criteri di soglia delle performance dagli oggetti storage"

Performance (prestazioni): Vista QoS Policy Groups (gruppi di policy

La vista QoS Policy Groups (gruppi policy QoS) visualizza i gruppi di policy QoS disponibili sui cluster monitorati da Unified Manager. Ciò include policy QoS tradizionali, policy QoS adattive e policy QoS assegnate utilizzando i livelli di servizio Performance.

Di seguito sono riportati alcuni campi importanti della vista Performance: QoS Policy Groups (prestazioni: Gruppi policy QoS).

- QoS Policy Group (Gruppo criteri QoS): Il nome del gruppo di criteri QoS. Per le policy di NetApp Service Level Manager (NSLM) 1.3 che sono state importate in Unified Manager 9.7 o versione successiva, il nome visualizzato qui include il nome SVM e altre informazioni che non si trovano nel nome quando il livello del servizio Performance è stato definito in NSLM. Ad esempio, il nome "NSLM_vs6_Performance_2_0" indica che si tratta del criterio PSL "Performance" definito dal sistema NSLM creato su SVM "vs6" con una latenza prevista di "2 ms/op".
- SVM: La VM di storage (SVM) a cui appartiene il gruppo di criteri QoS. È possibile fare clic sul nome della VM di storage per accedere alla pagina dei dettagli della VM di storage. Si noti che questo campo è vuoto se il criterio QoS è stato creato sulla VM di storage amministrativa, poiché questo tipo di VM di storage rappresenta il cluster.
- Throughput minimo: Il throughput minimo, in IOPS, garantito dal gruppo di policy. Per le policy adattive, si tratta degli IOPS minimi previsti per TB allocati al volume o al LUN, in base alla dimensione allocata dell'oggetto di storage.
- Throughput massimo: Il throughput, in IOPS e/o MB/s, che il gruppo di criteri non deve superare. Quando questo campo è vuoto, significa che il massimo definito in ONTAP è infinito. Per le policy adattive, si tratta del massimo (picco) di IOPS possibili per TB allocati al volume o al LUN, in base alla dimensione allocata dell'oggetto di storage o alla dimensione utilizzata dell'oggetto di storage.
- IOPS minimi assoluti: Per le policy adattive, questo è il valore IOPS minimo assoluto che viene utilizzato come override quando gli IOPS previsti sono inferiori a questo valore.
- Block Size (dimensione blocco): La dimensione del blocco specificata per il criterio adattivo QoS.
- Allocazione minima: Se viene utilizzato "spazio allocato" o "spazio utilizzato" per determinare gli IOPS di throughput massimo (picco).
- Latenza prevista: La latenza media prevista per le operazioni di input/output dello storage.
- Shared (condiviso): Per le policy QoS tradizionali, se i valori di throughput definiti nel gruppo di policy sono condivisi tra più oggetti.
- Associated Objects (oggetti associati): Il numero di carichi di lavoro assegnati al gruppo di criteri QoS. È possibile fare clic sul pulsante Expand (Espandi) ( ) Accanto a QoS Policy Group Name (Nome gruppo policy QoS) per visualizzare ulteriori dettagli sul gruppo di policy.
- Allocated Capacity (capacità allocata): Quantità di spazio attualmente utilizzato dagli oggetti del gruppo di criteri QoS.
- Associated Objects (oggetti associati): Il numero di workload assegnati al gruppo di policy QoS, separati in

volumi e LUN. È possibile fare clic sul numero per accedere a una pagina che fornisce ulteriori dettagli sui volumi o sui LUN selezionati.

Per ulteriori informazioni, consultare gli argomenti della sezione "Gestione delle performance utilizzando le informazioni del gruppo di policy QoS".

Perfezionare il contenuto della pagina dell'inventario delle performance

Le pagine di inventario per gli oggetti performance contengono strumenti che consentono di perfezionare il contenuto dei dati di inventario degli oggetti, consentendo di individuare dati specifici in modo rapido e semplice.

Le informazioni contenute nelle pagine di inventario degli oggetti Performance possono essere estese, spesso estendendosi su più pagine. Questo tipo di dati completi è eccellente per il monitoraggio, il monitoraggio e il miglioramento delle performance; tuttavia, l'individuazione di dati specifici richiede strumenti che consentono di individuare rapidamente i dati desiderati. Pertanto, le pagine di inventario degli oggetti Performance contengono funzionalità per la ricerca, l'ordinamento e il filtraggio. Inoltre, la ricerca e il filtraggio possono lavorare insieme per restringere ulteriormente i risultati.

Ricerca nelle pagine Object Inventory Performance

È possibile cercare le stringhe nelle pagine Object Inventory Performance (prestazioni inventario oggetti). Utilizzare il campo **Search** situato nella parte superiore destra della pagina per individuare rapidamente i dati in base al nome dell'oggetto o del criterio. In questo modo è possibile individuare rapidamente oggetti specifici e i relativi dati associati oppure individuare rapidamente le policy e visualizzare i dati degli oggetti policy associati.

Fase

1. Eseguire una delle seguenti opzioni in base ai requisiti di ricerca:

Per individuare…	Digitare questo…
Un oggetto specifico	Il nome dell'oggetto nel campo **Search** e fare clic su **Search**. Viene visualizzato l'oggetto per il quale è stata eseguita la ricerca e i relativi dati.
Una policy di soglia delle performance definita dall'utente	Nome completo o parziale del criterio nel campo **Cerca** e fare clic su **Cerca**. Vengono visualizzati gli oggetti assegnati al criterio per il quale si è eseguita la ricerca.

Ordinamento nelle pagine Object Inventory Performance (prestazioni inventario oggetti)

È possibile ordinare tutti i dati nelle pagine Object Inventory Performance in base a qualsiasi colonna in ordine crescente o decrescente. Ciò consente di individuare rapidamente i dati di inventario degli oggetti, cosa utile quando si esaminano le prestazioni o si avvia un processo di risoluzione dei problemi.

La colonna selezionata per l'ordinamento è indicata da un nome di intestazione di colonna evidenziato e da un'icona a forma di freccia che indica la direzione di ordinamento a destra del nome. Una freccia rivolta verso

l'alto indica l'ordine crescente, mentre una freccia rivolta verso il basso indica l'ordine decrescente. Il criterio di ordinamento predefinito è per **Status** (criticità evento) in ordine decrescente, con gli eventi di performance più critici elencati per primi.

Fase

1. È possibile fare clic sul nome di una colonna per alternare l'ordinamento della colonna in ordine crescente o decrescente.

   I contenuti della pagina Object Inventory Performance sono ordinati in ordine crescente o decrescente, in base alla colonna selezionata.

Filtraggio dei dati nelle pagine Object Inventory Performance

È possibile filtrare i dati nelle pagine Object Inventory Performance per individuare rapidamente i dati in base a criteri specifici. È possibile utilizzare il filtraggio per restringere il contenuto delle pagine Object Inventory Performance e visualizzare solo i risultati specificati. In questo modo si ottiene un metodo molto efficiente per visualizzare solo i dati relativi alle performance di cui si è interessati.

È possibile utilizzare il pannello di filtraggio per personalizzare la vista a griglia in base alle proprie preferenze. Le opzioni di filtro disponibili si basano sul tipo di oggetto visualizzato nella griglia. Se i filtri sono attualmente applicati, il numero di filtri applicati viene visualizzato a destra del pulsante Filter (filtro).

Sono supportati tre tipi di parametri di filtro.

Parametro	Convalida
Stringa (testo)	Gli operatori sono **contains**, **inizia con**, **termina con** e **non contiene**.
Numero	Gli operatori sono **maggiori di**, **minori di**, **negli ultimi** e **tra**.
Enum (testo)	Gli operatori sono **IS** e **non**.

I campi Column (colonna), Operator (operatore) e Value (valore) sono obbligatori per ciascun filtro; i filtri disponibili riflettono le colonne filtrabili nella pagina corrente. Il numero massimo di filtri che è possibile applicare è quattro. I risultati filtrati si basano su parametri di filtro combinati. I risultati filtrati si applicano a tutte le pagine della ricerca filtrata, non solo alla pagina attualmente visualizzata.

È possibile aggiungere filtri utilizzando il pannello di filtraggio.

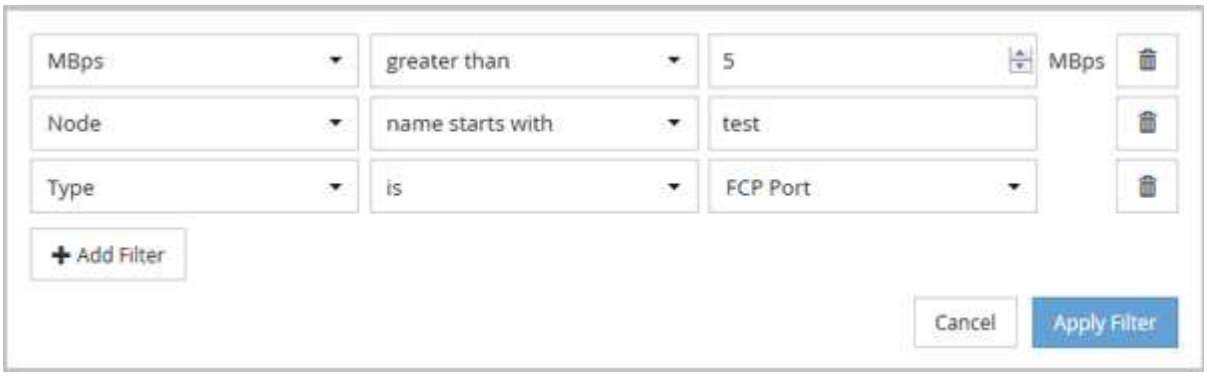
1. Nella parte superiore della pagina, fare clic sul pulsante **Filter** (filtro). Viene visualizzato il pannello Filtering (filtraggio).
2. Fare clic sull'elenco a discesa a sinistra e selezionare un oggetto, ad esempio *Cluster* o un contatore delle prestazioni.
3. Fare clic sull'elenco a discesa centrale e selezionare l'operatore che si desidera utilizzare.
4. Nell'ultimo elenco, selezionare o inserire un valore per completare il filtro per l'oggetto.
5. Per aggiungere un altro filtro, fare clic su **+Aggiungi filtro**. Viene visualizzato un campo di filtro aggiuntivo. Completare questo filtro seguendo la procedura descritta nei passaggi precedenti. Si noti che quando si

aggiunge il quarto filtro, il pulsante **+Aggiungi filtro** non viene più visualizzato.

6. Fare clic su **Applica filtro**. Le opzioni di filtro vengono applicate alla griglia e il numero di filtri viene visualizzato a destra del pulsante Filter (filtro).
7. Utilizzare il pannello di filtraggio per rimuovere i singoli filtri facendo clic sull'icona del cestino a destra del filtro da rimuovere.
8. Per rimuovere tutti i filtri, fare clic su **Reset** nella parte inferiore del pannello di filtraggio.

Esempio di filtraggio

La figura mostra il pannello di filtraggio con tre filtri. Il pulsante **+Aggiungi filtro** viene visualizzato quando si dispone di un numero inferiore al massimo di quattro filtri.



Dopo aver fatto clic su **Apply Filter** (Applica filtro), il pannello Filtering (filtraggio) si chiude, applica i filtri e mostra il numero di filtri applicati (3).

Comprendere le raccomandazioni di Unified Manager per il Tier dei dati nel cloud

La vista Performance: All Volumes (prestazioni: Tutti i volumi) visualizza le informazioni relative alle dimensioni dei dati utente memorizzati nel volume inattivo (freddo). In alcuni casi, Unified Manager identifica alcuni volumi che trarrebbero beneficio dal tiering dei dati inattivi nel Tier cloud (cloud provider o StorageGRID) di un aggregato abilitato a FabricPool.

FabricPool è stato introdotto in ONTAP 9.2, quindi se si utilizza una versione del software ONTAP precedente alla 9.2, la raccomandazione di Unified Manager per i dati di Tier richiede l'aggiornamento del software ONTAP. Inoltre, il `auto` La policy di tiering è stata introdotta in ONTAP 9.4 e in `all` La policy di tiering è stata introdotta in ONTAP 9.6, quindi se si consiglia di utilizzare la policy di tiering automatico, è necessario eseguire l'aggiornamento a ONTAP 9.4 o superiore.

I tre campi seguenti relativi alle performance: All Volumes view (visualizzazione di tutti i volumi) forniscono informazioni sulla possibilità di migliorare l'utilizzo del disco del sistema storage e di risparmiare spazio sul Tier di performance spostando i dati inattivi sul Tier cloud.

- **Policy di tiering**

  La policy di tiering determina se i dati sul volume rimangono nel Tier di performance o se alcuni dei dati vengono spostati dal Tier di performance al Tier cloud.

Il valore in questo campo indica il criterio di tiering impostato sul volume, anche se il volume non risiede attualmente in un aggregato FabricPool. La policy di tiering ha effetto solo quando il volume si trova su un aggregato FabricPool.

- **Dati a freddo**

  I dati cold visualizzano le dimensioni dei dati utente memorizzati nel volume inattivo (freddo).

  Un valore viene visualizzato solo quando si utilizza ONTAP 9.4 o un software superiore, perché richiede che l'aggregato su cui viene distribuito il volume disponga di **`inactive data reporting parameter`** impostare su **`enabled`**`e che sia stata raggiunta la soglia minima di giorni di raffreddamento (per i volumi che utilizzano `**`snapshot-only`** oppure **`auto`** policy di tiering). In caso contrario, il valore viene elencato come "N/A".

- **Cloud Recommendation**

  Una volta acquisita una quantità sufficiente di informazioni sull'attività dei dati sul volume, Unified Manager può determinare che non è richiesta alcuna azione o che è possibile risparmiare spazio sul Tier delle performance eseguendo il tiering dei dati inattivi sul Tier del cloud.

> Il campo Cold Data viene aggiornato ogni 15 minuti, ma il campo Cloud Recommendation viene aggiornato ogni 7 giorni quando l'analisi dei dati cold viene eseguita sul volume. Pertanto, la quantità esatta di dati cold può differire tra i campi. Il campo Cloud Recommendation visualizza la data in cui è stata eseguita l'analisi.

Quando Inactive Data Reporting è attivato, il campo Cold Data (dati a freddo) visualizza la quantità esatta di dati inattivi. Senza la funzionalità di reporting dei dati inattiva, Unified Manager utilizza le statistiche delle performance per determinare se i dati sono inattivi su un volume. In questo caso, la quantità di dati inattivi non viene visualizzata nel campo dati a freddo, ma viene visualizzata quando si sposta il cursore sulla parola **Tier** per visualizzare la raccomandazione cloud.

I consigli sul cloud che vedrai sono:

- **Formazione**. Non sono stati raccolti dati sufficienti per fornire consigli.
- **Tier**. L'analisi ha determinato che il volume contiene dati inattivi (cold) e che è necessario configurare il volume per spostare tali dati nel Tier cloud. In alcuni casi, potrebbe essere necessario spostare prima il volume in un aggregato abilitato a FabricPool. In altri casi in cui il volume si trova già su un aggregato FabricPool, è sufficiente modificare la policy di tiering.
- **Nessuna azione**. Il volume contiene pochissimi dati inattivi, il volume è già impostato sul criterio di tiering "auto" su un aggregato FabricPool oppure il volume è un volume di protezione dei dati. Questo valore viene visualizzato anche quando il volume è offline o quando viene utilizzato in una configurazione MetroCluster.

Per spostare un volume o modificare il criterio di tiering del volume o le impostazioni di reporting dei dati inattivi aggregati, utilizzare Gestione di sistema di ONTAP, i comandi dell'interfaccia utente di ONTAP o una combinazione di questi strumenti.

Se si è connessi a Unified Manager con il ruolo di amministratore dell'applicazione o di amministratore dello storage, il collegamento **Configure Volume** (Configura volume) è disponibile nella raccomandazione cloud quando si sposta il cursore sulla parola **Tier**. Fare clic su questo pulsante per aprire la pagina Volumes (volumi) in System Manager (Gestione sistema) e apportare le modifiche consigliate.

Monitoraggio delle performance tramite le pagine Performance Explorer

Le pagine Performance Explorer (Esplora prestazioni) visualizzano informazioni dettagliate sulle prestazioni di ciascun oggetto in un cluster. La pagina fornisce una vista dettagliata delle performance di tutti gli oggetti del cluster, consentendo di selezionare e confrontare i dati delle performance di oggetti specifici in diversi periodi di tempo.

È inoltre possibile valutare le performance complessive di tutti gli oggetti e confrontare i dati delle performance degli oggetti in un formato affiancato.

Comprensione dell'oggetto root

L'oggetto root è la base rispetto alla quale vengono effettuati altri confronti tra oggetti. Ciò consente di visualizzare e confrontare i dati di altri oggetti con l'oggetto root, fornendo un'analisi dei dati delle performance che consente di risolvere i problemi e migliorare le performance degli oggetti.

Il nome dell'oggetto root viene visualizzato nella parte superiore del pannello di confronto. Gli oggetti aggiuntivi vengono visualizzati sotto l'oggetto root. Sebbene non vi sia alcun limite al numero di oggetti aggiuntivi che è possibile aggiungere al pannello di confronto, è consentito un solo oggetto root. I dati dell'oggetto root vengono visualizzati automaticamente nei grafici nel riquadro Counter Chart.

Non è possibile modificare l'oggetto root, che viene sempre impostato sulla pagina oggetto visualizzata. Ad esempio, se si apre la pagina Volume Performance Explorer di Volume1, Volume1 è l'oggetto root e non può essere modificato. Se si desidera eseguire un confronto con un oggetto root diverso, fare clic sul collegamento di un oggetto e aprire la relativa landing page.

Gli eventi e le soglie vengono visualizzati solo per gli oggetti root.

Applicare il filtraggio per ridurre l'elenco degli oggetti correlati nella griglia

Il filtraggio consente di visualizzare un sottoinsieme di oggetti più piccolo e ben definito nella griglia. Ad esempio, se nella griglia sono presenti 25 volumi, il filtraggio consente di visualizzare solo i volumi con throughput inferiore a 90 Mbps o latenza superiore a 1 ms/op.

Specifica di un intervallo di tempo per gli oggetti correlati

Il selettore Time Range (intervallo di tempo) nella pagina Performance Explorer (Esplora prestazioni) consente di specificare l'intervallo di tempo per il confronto dei dati a oggetti. Specificando un intervallo di tempo, il contenuto delle pagine di Performance Explorer viene ridefinito in modo da visualizzare solo i dati dell'oggetto entro l'intervallo di tempo specificato.

La rifinitura dell'intervallo di tempo offre un metodo efficiente per visualizzare solo i dati relativi alle performance di cui si è interessati. È possibile selezionare un intervallo di tempo predefinito o specificare un intervallo di tempo personalizzato. L'intervallo di tempo predefinito è quello delle 72 ore precedenti.

Selezione di un intervallo di tempo predefinito

La selezione di un intervallo di tempo predefinito è un modo rapido ed efficiente per personalizzare e concentrare l'output dei dati durante la visualizzazione dei dati relativi alle performance degli oggetti del cluster. Quando si seleziona un intervallo di tempo predefinito, sono disponibili dati per un massimo di 13 mesi.

Fasi

1. Nella parte superiore destra della pagina **Performance Explorer**, fare clic su **Time Range**.
2. Nella parte destra del pannello **Time Range Selection** (selezione intervallo di tempo), selezionare un intervallo di tempo predefinito.
3. Fare clic su **Apply Range** (Applica intervallo).

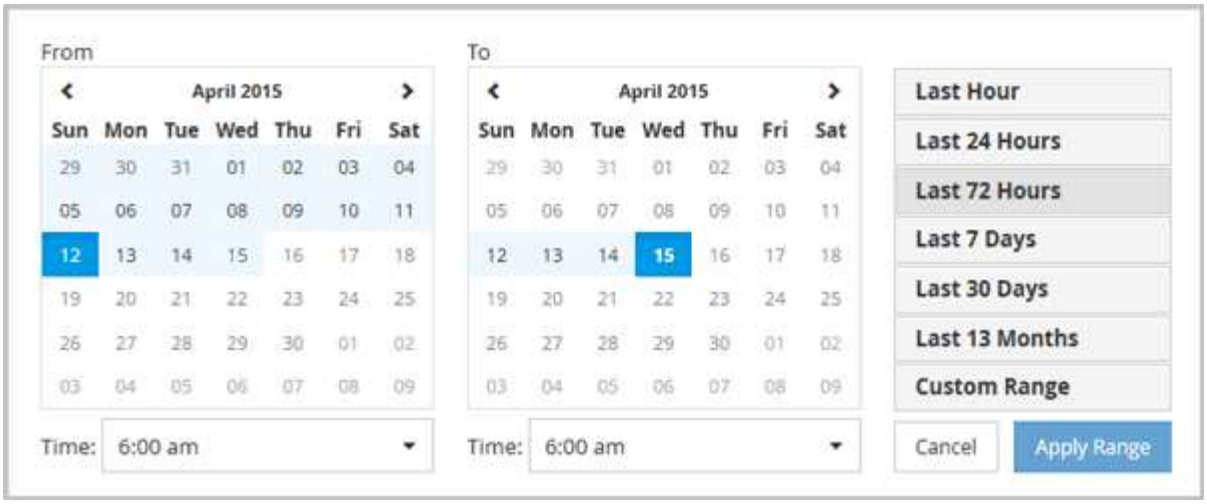
Specifica di un intervallo di tempo personalizzato

La pagina Performance Explorer (Esplora prestazioni) consente di specificare la data e l'intervallo di tempo per i dati relativi alle performance. La specifica di un intervallo di tempo personalizzato offre una maggiore flessibilità rispetto all'utilizzo di intervalli di tempo predefiniti durante la raffinazione dei dati degli oggetti del cluster.

È possibile selezionare un intervallo di tempo compreso tra un'ora e 390 giorni. 13 mesi equivale a 390 giorni perché ogni mese viene conteggiato come 30 giorni. La specifica di un intervallo di data e ora fornisce maggiori dettagli e consente di eseguire lo zoom su eventi specifici relativi alle performance o a serie di eventi. La specifica di un intervallo di tempo consente inoltre di risolvere potenziali problemi di performance, poiché specificando un intervallo di date e di ore vengono visualizzati i dati relativi all'evento di performance in modo più dettagliato. Utilizzare il controllo **Time Range** per selezionare intervalli di data e ora predefiniti oppure specificare un intervallo di data e ora personalizzato fino a 390 giorni. I pulsanti per intervalli di tempo predefiniti variano da **ultima ora** a **ultimi 13 mesi**.

Selezionando l'opzione **ultimi 13 mesi** o specificando un intervallo di date personalizzato superiore a 30 giorni, viene visualizzata una finestra di dialogo in cui viene segnalato che i dati relativi alle performance visualizzati per un periodo superiore a 30 giorni vengono inseriti utilizzando medie orarie e non il polling dei dati di 5 minuti. Pertanto, potrebbe verificarsi una perdita di granularità visiva della timeline. Se si fa clic sull'opzione **non mostrare più** nella finestra di dialogo, il messaggio non viene visualizzato quando si seleziona l'opzione **ultimi 13 mesi** o si specifica un intervallo di date personalizzato superiore a 30 giorni. I dati di riepilogo si applicano anche a un intervallo di tempo inferiore, se l'intervallo di tempo include un'ora/data che è più di 30 giorni da oggi.

Quando si seleziona un intervallo di tempo (personalizzato o predefinito), gli intervalli di tempo di 30 giorni o meno si basano su campioni di dati a intervalli di 5 minuti. Gli intervalli di tempo superiori a 30 giorni si basano su campioni di dati a intervalli di un'ora.



1. Fare clic sulla casella a discesa **intervallo di tempo** per visualizzare il pannello intervallo di tempo.
2. Per selezionare un intervallo di tempo predefinito, fare clic su uno dei pulsanti **ultimo…** a destra del pannello **intervallo di tempo**. Quando si seleziona un intervallo di tempo predefinito, sono disponibili dati per un massimo di 13 mesi. Il pulsante dell'intervallo di tempo predefinito selezionato viene evidenziato e i giorni e l'ora corrispondenti vengono visualizzati nei calendari e nei selettori dell'ora.
3. Per selezionare un intervallo di date personalizzato, fare clic sulla data di inizio nel calendario **da** a sinistra. Fare clic su **<** o **>** per spostarsi in avanti o indietro nel calendario. Per specificare la data di fine, fare clic su una data nel calendario **a** a destra. Si noti che la data di fine predefinita è oggi, a meno che non si specifichi una data di fine diversa. Il pulsante **Custom Range** (intervallo personalizzato) a destra del pannello Time Range (intervallo di tempo) è evidenziato, a indicare che è stato selezionato un intervallo di date personalizzato.
4. Per selezionare un intervallo di tempo personalizzato, fare clic sul controllo **Time** sotto il calendario **From** e selezionare l'ora di inizio. Per specificare l'ora di fine, fare clic sul controllo **Time** sotto il calendario **To** a destra e selezionare l'ora di fine. Il pulsante **Custom Range** (intervallo personalizzato) a destra del pannello Time Range (intervallo di tempo) è evidenziato, a indicare che è stato selezionato un intervallo di tempo personalizzato.
5. Facoltativamente, è possibile specificare l'ora di inizio e di fine quando si seleziona un intervallo di date predefinito. Selezionare l'intervallo di date predefinito come descritto in precedenza, quindi selezionare l'ora di inizio e di fine come descritto in precedenza. Le date selezionate vengono evidenziate nei calendari, gli orari di inizio e di fine specificati vengono visualizzati nei controlli **Time** e il pulsante **Custom Range** viene evidenziato.
6. Dopo aver selezionato l'intervallo di data e ora, fare clic su **Apply Range** (Applica intervallo). Le statistiche delle performance per quell'intervallo di tempo vengono visualizzate nei grafici e nella timeline degli eventi.

Definizione dell'elenco degli oggetti correlati per il grafico di confronto

È possibile definire un elenco di oggetti correlati per il confronto di dati e performance nel riquadro Counter Chart. Ad esempio, se la macchina virtuale di storage (SVM) presenta un problema di performance, è possibile confrontare tutti i volumi nella SVM per identificare il volume che potrebbe causare il problema.

È possibile aggiungere qualsiasi oggetto nella griglia oggetti correlati ai riquadri confronto e grafico contatore. In questo modo è possibile visualizzare e confrontare i dati di più oggetti e con l'oggetto root. È possibile aggiungere e rimuovere oggetti da e verso la griglia degli oggetti correlati; tuttavia, l'oggetto root nel pannello di confronto non è rimovibile.

L’aggiunta di molti oggetti al pannello di confronto può avere un impatto negativo sulle performance. Per mantenere le performance, è necessario selezionare un numero limitato di grafici per il confronto dei dati.

Fasi

1. Nella griglia oggetti, individuare l’oggetto che si desidera aggiungere e fare clic sul pulsante **Aggiungi**.

   Il pulsante **Add** diventa grigio e l’oggetto viene aggiunto all’elenco degli oggetti aggiuntivi nel riquadro di confronto. I dati dell’oggetto vengono aggiunti ai grafici nei riquadri Counter Chart. Il colore dell’icona dell’occhio dell’oggetto ( ) corrisponde al colore della linea di trend dei dati dell’oggetto nei grafici.

2. **Opzionale:** Nascondi o mostra i dati per gli oggetti selezionati:

A tal fine…	Eseguire questa azione…
Nascondere un oggetto selezionato	Fare clic sull’icona dell’occhio dell’oggetto selezionato ( ) Nel riquadro di confronto. I dati dell’oggetto vengono nascosti e l’icona dell’occhio per l’oggetto diventa grigia.
Mostra un oggetto nascosto	Fare clic sull’icona a occhio grigio dell’oggetto selezionato nel riquadro di confronto. L’icona occhio torna al colore originale e i dati dell’oggetto vengono aggiunti di nuovo ai grafici nel riquadro Counter Chart.

3. **Opzionale:** Rimuovi gli oggetti selezionati dal pannello **confronto**:

A tal fine…	Eseguire questa azione…
Rimuovere un oggetto selezionato	Passare il mouse sul nome dell’oggetto selezionato nel pannello di confronto per visualizzare il pulsante Remove Object (**X**), quindi fare clic sul pulsante. L’oggetto viene rimosso dal riquadro di confronto e i relativi dati vengono cancellati dai diagrammi dei contatori.
Rimuovi tutti gli oggetti selezionati	Fare clic sul pulsante Remove all object’s (**X**) nella parte superiore del pannello di confronto. Tutti gli oggetti selezionati e i relativi dati vengono rimossi, lasciando solo l’oggetto root.

Comprensione dei diagrammi di contatore

I grafici nel riquadro Counter Chart consentono di visualizzare e confrontare i dati delle performance per l’oggetto root e per gli oggetti aggiunti dalla griglia Correlated Objects. Ciò può aiutarti a comprendere le tendenze delle performance e a isolare e risolvere i problemi di performance.

I grafici dei contatori visualizzati per impostazione predefinita sono Eventi, latenza, IOPS e Mbps. I grafici opzionali che è possibile scegliere di visualizzare sono Utilization (utilizzo), Performance Capacity used (capacità di performance utilizzata), Available IOPS (IOPS disponibili), IOPS/TB (IOPS/TB) e cache Miss Ratio (rapporto errori cache). Inoltre, è possibile scegliere di visualizzare i valori totali o i valori di dettaglio per i grafici latenza, IOPS, Mbps e capacità di performance utilizzata.

Per impostazione predefinita, Performance Explorer visualizza alcuni contatori, indipendentemente dal fatto che l'oggetto di storage li supporti tutti o meno. Quando un contatore non è supportato, il contatore è vuoto e il messaggio `Not applicable for <object>` viene visualizzato.

I grafici mostrano i trend delle performance per l'oggetto root e per tutti gli oggetti selezionati nel pannello di confronto. I dati di ciascun grafico sono disposti come segue:

- **Asse X**

  Visualizza il periodo di tempo specificato. Se non è stato specificato un intervallo di tempo, l'impostazione predefinita è il periodo di 72 ore precedente.

- **Asse Y**

  Visualizza le unità del contatore univoche per l'oggetto o gli oggetti selezionati.

I colori delle linee di tendenza corrispondono al colore del nome dell'oggetto visualizzato nel riquadro di confronto. È possibile posizionare il cursore su un punto di qualsiasi linea di trend per visualizzare i dettagli relativi all'ora e al valore di tale punto.

Se si desidera esaminare un periodo di tempo specifico all'interno di un grafico, è possibile utilizzare uno dei seguenti metodi:

- Utilizzare il pulsante **<** per espandere il riquadro Counter Charts (grafici contatore) per estendere la larghezza della pagina.
- Utilizzare il cursore (quando passa a una lente di ingrandimento) per selezionare una parte dell'intervallo di tempo nel grafico per mettere a fuoco e ingrandire l'area. È possibile fare clic su Reset Chart Zoom (Ripristina zoom grafico) per riportare il grafico all'intervallo di tempo predefinito.
- Utilizzare il pulsante **Zoom View** (Vista zoom) per visualizzare un singolo contatore grande che contiene dettagli ampliati e indicatori di soglia.

Occasionalmente, vengono visualizzate delle lacune nelle linee di trend. Le lacune indicano che Unified Manager non è riuscito a raccogliere dati sulle performance dal sistema storage o che Unified Manager potrebbe essere stato inattivo.

Tipi di tabelle dei contatori delle performance

Sono disponibili grafici delle prestazioni standard che visualizzano i valori del contatore per l'oggetto di storage selezionato. Ciascuno dei diagrammi dei contatori dei guasti visualizza i valori totali separati in lettura, scrittura e altre categorie. Inoltre, alcuni grafici dei contatori dettagliati visualizzano ulteriori dettagli quando il grafico viene visualizzato nella vista Zoom.

La seguente tabella mostra i grafici dei contatori delle prestazioni disponibili.

Grafici disponibili	Descrizione del grafico
Eventi	Visualizza eventi critici, di errore, di avviso e di informazione in correlazione con i grafici statistici dell'oggetto root. Oltre agli eventi relativi alle performance, vengono visualizzati eventi relativi allo stato di salute per fornire un quadro completo dei motivi per cui le performance potrebbero risentirne.
Latenza - totale	Numero di millisecondi necessari per rispondere alle richieste dell'applicazione. Si noti che i valori medi di latenza sono ponderati in i/O.
Latenza - analisi	Le stesse informazioni mostrate in latenza totale, ma con i dati delle performance separati in latenza di lettura, scrittura e di altro tipo. Questa opzione di grafico si applica solo quando l'oggetto selezionato è SVM, nodo, aggregato, volume, LUN, o namespace.
Latenza - componenti del cluster	Le stesse informazioni visualizzate in Latency Total (latenza totale), ma con i dati delle performance separati in latenza per componente del cluster. Questa opzione di grafico si applica solo quando l'oggetto selezionato è un volume.
IOPS - totale	Numero di operazioni di input/output elaborate al secondo. Quando viene visualizzato per un nodo, selezionando "Total" (totale) vengono visualizzati gli IOPS per i dati che si spostano attraverso questo nodo che può risiedere sul nodo locale o remoto e selezionando "Total (Local)" (totale (locale)) vengono visualizzati gli IOPS per i dati che risiedono solo sul nodo corrente.
IOPS - guasto	Le stesse informazioni mostrate in IOPS Total, ma con i dati delle performance separati in lettura, scrittura e altri IOPS. Questa opzione di grafico si applica solo quando l'oggetto selezionato è SVM, nodo, aggregato, volume, LUN, o namespace. Quando viene visualizzato nella vista Zoom, il grafico dei volumi visualizza i valori di throughput minimo e massimo di QoS, se configurato in ONTAP. Quando viene visualizzato per un nodo, selezionando "Breakdown" viene visualizzata la suddivisione IOPS per i dati che si spostano attraverso questo nodo che potrebbe risiedere sul nodo locale o remoto e selezionando "Breakdown (Local)" viene visualizzata la suddivisione IOPS per i dati che risiedono solo sul nodo corrente.

Grafici disponibili	Descrizione del grafico
IOPS - protocolli	Le stesse informazioni mostrate in IOPS Total, ma i dati delle performance sono separati in singoli grafici per il traffico dei protocolli CIFS, NFS, FCP, NVMe e iSCSI. Questa opzione di grafico si applica solo quando l'oggetto selezionato è una SVM.
IOPS/TB - totale	Numero di operazioni di input/output elaborate al secondo in base allo spazio totale consumato dal carico di lavoro, in terabyte. Detto anche densità di i/o, questo contatore misura la quantità di performance che possono essere fornite da una determinata quantità di capacità di storage. Se visualizzato nella vista Zoom, il grafico dei volumi visualizza i valori di QoS previsti e di picco di throughput, se configurato in ONTAP. Questa opzione di grafico si applica solo quando l'oggetto selezionato è un volume.
MB/s - totale	Numero di megabyte di dati trasferiti da e verso l'oggetto al secondo.
MB/s - Dettagli	Le stesse informazioni mostrate nel grafico MB/s, ma con i dati di throughput separati in letture di dischi, letture di Flash cache, scritture e altro. Quando viene visualizzato nella vista Zoom, il grafico dei volumi visualizza i valori massimi di throughput QoS, se configurati in ONTAP. Questa opzione di grafico si applica solo quando l'oggetto selezionato è SVM, nodo, aggregato, volume, LUN, o namespace. I dati di Flash cache vengono visualizzati solo per i nodi e solo quando nel nodo è installato un modulo Flash cache.
Capacità di performance utilizzata - totale	Percentuale di capacità di performance consumata dal nodo o dall'aggregato.
Capacità di performance utilizzata - ripartizione	Performance Capacity utilizza i dati separati nei protocolli utente e nei processi di background del sistema. Inoltre, viene mostrata la quantità di capacità di performance libera.

Grafici disponibili	Descrizione del grafico
IOPS disponibili - totale	Numero di operazioni di input/output al secondo attualmente disponibili (libere) su questo oggetto. Questo numero è il risultato della sottrazione degli IOPS attualmente utilizzati dai IOPS totali che Unified Manager calcola che l'oggetto può eseguire. Questa opzione di grafico si applica solo quando l'oggetto selezionato è un nodo o aggregato.
Utilizzo - totale	Percentuale di risorse disponibili dell'oggetto in uso. L'utilizzo indica l'utilizzo del nodo per i nodi, l'utilizzo del disco per gli aggregati e l'utilizzo della larghezza di banda per le porte. Questa opzione di grafico si applica solo quando l'oggetto selezionato è un nodo, un aggregato o una porta.
Cache Miss Ratio - Total (rapporto errori cache - totale)	Percentuale di richieste di lettura provenienti dalle applicazioni client restituite dal disco invece di essere restituite dalla cache. Questa opzione di grafico si applica solo quando l'oggetto selezionato è un volume.

Selezione dei grafici delle prestazioni da visualizzare

L'elenco a discesa Scegli grafici consente di selezionare i tipi di grafici dei contatori delle prestazioni da visualizzare nel riquadro Counter Chart. In questo modo è possibile visualizzare dati e contatori specifici in base ai requisiti di performance.

Fasi

1. Nel riquadro **Counter Chart**, fare clic sull'elenco a discesa **Choose Chart** (Scegli grafici).
2. Aggiungere o rimuovere grafici:

Per…	Eseguire questa operazione…
Aggiungere o rimuovere singoli grafici	Fare clic sulle caselle di controllo accanto ai grafici che si desidera visualizzare o nascondere
Aggiungere tutti i grafici	Fare clic su **Select All** (Seleziona tutto)
Rimuovere tutti i grafici	Fare clic su **Deseleziona tutto**

Le selezioni dei grafici vengono visualizzate nel riquadro Counter Chart. Quando si aggiungono i grafici, i nuovi grafici vengono inseriti nel riquadro Counter Chart in modo che corrispondano all'ordine dei grafici elencati nell'elenco a discesa Choose Chart (Scegli grafici). La selezione di grafici aggiuntivi potrebbe richiedere uno scorrimento aggiuntivo.

Espansione del riquadro Counter Chart

È possibile espandere il riquadro Counter Chart in modo che i grafici siano più grandi e leggibili.

Dopo aver definito gli oggetti di confronto e l'intervallo di tempo per i contatori, è possibile visualizzare un riquadro di Counter Chart più grande. Per espandere il riquadro, utilizzare il pulsante **<** al centro della finestra di Performance Explorer.

Fase

1. Espandere o ridurre il riquadro **Counter Chart**.

Per…	Eseguire questa operazione…
Espandere il riquadro Counter Chart per adattarlo alla larghezza della pagina	Fare clic sul pulsante **<**
Ridurre il riquadro Counter Chart alla metà destra della pagina	Fare clic sul pulsante **>**

Modifica della messa a fuoco dei Counter Chart in un periodo di tempo più breve

È possibile utilizzare il mouse per ridurre l'intervallo di tempo per concentrarsi su un periodo di tempo specifico nel riquadro Counter Chart (grafico contatore) o nella finestra Counter Chart Zoom View (Vista zoom grafici contatore). In questo modo è possibile visualizzare in modo più granulare e microscopico qualsiasi parte della tempistica dei dati, degli eventi e delle soglie relativi alle performance.

Cosa ti serve

Il cursore deve essere stato modificato in una lente di ingrandimento per indicare che questa funzionalità è attiva.

> Quando si utilizza questa funzione, che modifica la timeline per visualizzare i valori corrispondenti alla visualizzazione più granulare, l'intervallo di tempo e data sul selettore **intervallo di tempo** non cambia dai valori originali del grafico.

Fasi

1. Per ingrandire un periodo di tempo specifico, fare clic utilizzando la lente di ingrandimento e trascinare il mouse per evidenziare l'area che si desidera visualizzare nei dettagli.

   I valori del contatore per il periodo di tempo selezionato riempiono il grafico del contatore.

2. Per tornare al periodo di tempo originale impostato nel selettore **Time Range** (intervallo di tempo), fare clic sul pulsante **Reset Chart Zoom** (Ripristina zoom grafico).

   Il grafico del contatore viene visualizzato nello stato originale.

Visualizzazione dei dettagli dell'evento nella cronologia degli eventi

È possibile visualizzare tutti gli eventi e i relativi dettagli nel riquadro Cronologia eventi di Performance Explorer. Si tratta di un metodo rapido ed efficiente per visualizzare tutti gli eventi relativi allo stato di salute e alle prestazioni che si sono verificati sull'oggetto root durante un intervallo di tempo specificato, che può essere utile per la risoluzione dei problemi relativi alle prestazioni.

Il riquadro Cronologia eventi mostra eventi critici, di errore, di avviso e informativi che si sono verificati sull'oggetto root durante l'intervallo di tempo selezionato. Ogni severità di evento ha una propria tempistica. Gli eventi singoli e multipli sono rappresentati da un punto sulla timeline. Per visualizzare i dettagli dell'evento, posizionare il cursore su un punto dell'evento. Per aumentare la granularità visiva di più eventi, è possibile ridurre l'intervallo di tempo. In questo modo, è possibile distribuire più eventi in singoli eventi, in modo da visualizzare e analizzare separatamente ciascun evento.

Ogni punto dell'evento relativo alle performance sulla timeline degli eventi si allinea verticalmente con un picco corrispondente nelle linee di trend dei grafici dei contatori visualizzate sotto la timeline degli eventi. In questo modo si ottiene una correlazione visiva diretta tra gli eventi e le performance complessive. Anche gli eventi di salute vengono visualizzati sulla timeline, ma questi tipi di eventi non si allineano necessariamente con un picco in uno dei grafici delle performance.

Fasi

1. Nel riquadro **Timeline eventi**, posizionare il cursore su un punto dell'evento su una timeline per visualizzare un riepilogo dell'evento o degli eventi in quel punto.

   Una finestra di dialogo a comparsa visualizza informazioni sui tipi di evento, la data e l'ora in cui si sono verificati gli eventi, lo stato e la durata dell'evento.

2. Visualizza i dettagli completi dell'evento per uno o più eventi:

A tal fine…	Fare clic qui…
Visualizza i dettagli di un singolo evento	**Visualizza dettagli evento** nella finestra di dialogo a comparsa.
Visualizza i dettagli di più eventi	**Visualizza dettagli evento** nella finestra di dialogo a comparsa. Facendo clic su un singolo evento nella finestra di dialogo Multiple events (più eventi) viene visualizzata la pagina Event Details (Dettagli evento) appropriata.

Counter Chart Zoom View

I Counter Chart forniscono una vista Zoom che consente di ingrandire i dettagli delle performance nel periodo di tempo specificato. In questo modo è possibile visualizzare i dettagli delle performance e gli eventi con una granularità molto più elevata, il che è vantaggioso per la risoluzione dei problemi relativi alle performance.

Quando viene visualizzato in Zoom View, alcuni dei grafici di dettaglio forniscono informazioni aggiuntive rispetto a quelle visualizzate quando il grafico non è in Zoom View. Ad esempio, le pagine IOPS, IOPS/TB e visualizzazione zoom del grafico a discesa Mbps visualizzano i valori dei criteri QoS per volumi e LUN, se impostati in ONTAP.

Per le policy di soglia delle performance definite dal sistema, solo le policy “Node resources over-utilizzed” e “QoS throughput limit violed” sono disponibili nell’elenco **Policies**. Gli altri criteri di soglia definiti dal sistema non sono attualmente disponibili.

Visualizzazione della vista Zoom dei grafici contatori

La vista Zoom dei grafici dei contatori fornisce un livello di dettaglio più dettagliato per il grafico dei contatori selezionato e la relativa timeline associata. Ciò consente di ingrandire i dati del contatore, consentendo di avere una vista più nitida degli eventi relativi alle performance e delle relative cause.

È possibile visualizzare la vista Zoom Counter Chart per qualsiasi grafico contatore.

Fasi

1. Fare clic su **Zoom View** per aprire la mappa selezionata in una nuova finestra del browser.
2. Se si sta visualizzando un grafico a discesa e si fa clic su **Zoom View** (Vista zoom), il grafico a discesa viene visualizzato in Zoom View (Vista zoom). Se si desidera modificare l’opzione di visualizzazione, è possibile selezionare **Total** (totale) in Zoom View (Vista zoom).

Specifica dell’intervallo di tempo nella vista Zoom

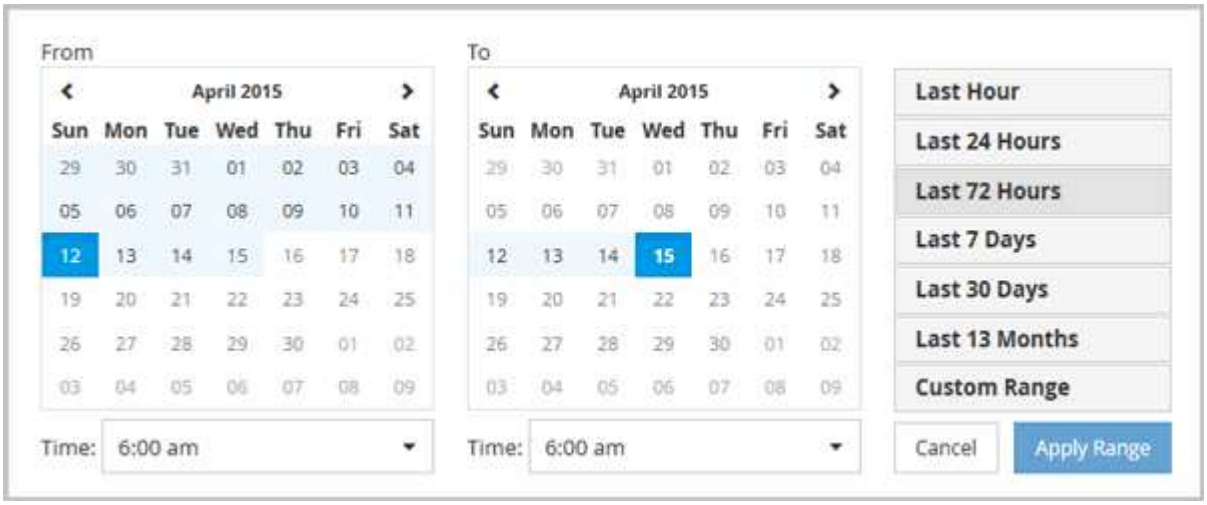
Il controllo **Time Range** nella finestra Counter Chart Zoom View consente di specificare una data e un intervallo di tempo per il grafico selezionato. In questo modo è possibile individuare rapidamente dati specifici in base a un intervallo di tempo preimpostato o a un intervallo di tempo personalizzato.

È possibile selezionare un intervallo di tempo compreso tra un’ora e 390 giorni. 13 mesi equivale a 390 giorni perché ogni mese viene conteggiato come 30 giorni. La specifica di un intervallo di data e ora fornisce maggiori dettagli e consente di eseguire lo zoom su eventi specifici relativi alle performance o a serie di eventi. La specifica di un intervallo di tempo consente inoltre di risolvere potenziali problemi di performance, poiché specificando un intervallo di date e di ore vengono visualizzati i dati relativi all’evento di performance in modo più dettagliato. Utilizzare il controllo **Time Range** per selezionare intervalli di data e ora predefiniti oppure specificare un intervallo di data e ora personalizzato fino a 390 giorni. I pulsanti per intervalli di tempo predefiniti variano da **ultima ora** a **ultimi 13 mesi**.

Selezionando l’opzione **ultimi 13 mesi** o specificando un intervallo di date personalizzato superiore a 30 giorni, viene visualizzata una finestra di dialogo in cui viene segnalato che i dati relativi alle performance visualizzati per un periodo superiore a 30 giorni vengono inseriti utilizzando medie orarie e non il polling dei dati di 5 minuti. Pertanto, potrebbe verificarsi una perdita di granularità visiva della timeline. Se si fa clic sull’opzione **non mostrare più** nella finestra di dialogo, il messaggio non viene visualizzato quando si seleziona l’opzione **ultimi 13 mesi** o si specifica un intervallo di date personalizzato superiore a 30 giorni. I dati di riepilogo si applicano anche a un intervallo di tempo inferiore, se l’intervallo di tempo include un’ora/data che è più di 30 giorni da oggi.

Quando si seleziona un intervallo di tempo (personalizzato o predefinito), gli intervalli di tempo di 30 giorni o meno si basano su campioni di dati a intervalli di 5 minuti. Gli intervalli di tempo superiori a 30 giorni si basano

su campioni di dati a intervalli di un'ora.



1. Fare clic sulla casella a discesa **intervallo di tempo** per visualizzare il pannello intervallo di tempo.
2. Per selezionare un intervallo di tempo predefinito, fare clic su uno dei pulsanti **ultimo…** a destra del pannello **intervallo di tempo**. Quando si seleziona un intervallo di tempo predefinito, sono disponibili dati per un massimo di 13 mesi. Il pulsante dell'intervallo di tempo predefinito selezionato viene evidenziato e i giorni e l'ora corrispondenti vengono visualizzati nei calendari e nei selettori dell'ora.
3. Per selezionare un intervallo di date personalizzato, fare clic sulla data di inizio nel calendario **da** a sinistra. Fare clic su **<** o **>** per spostarsi in avanti o indietro nel calendario. Per specificare la data di fine, fare clic su una data nel calendario **a** a destra. Si noti che la data di fine predefinita è oggi, a meno che non si specifichi una data di fine diversa. Il pulsante **Custom Range** (intervallo personalizzato) a destra del pannello Time Range (intervallo di tempo) è evidenziato, a indicare che è stato selezionato un intervallo di date personalizzato.
4. Per selezionare un intervallo di tempo personalizzato, fare clic sul controllo **Time** sotto il calendario **From** e selezionare l'ora di inizio. Per specificare l'ora di fine, fare clic sul controllo **Time** sotto il calendario **To** a destra e selezionare l'ora di fine. Il pulsante **Custom Range** (intervallo personalizzato) a destra del pannello Time Range (intervallo di tempo) è evidenziato, a indicare che è stato selezionato un intervallo di tempo personalizzato.
5. Facoltativamente, è possibile specificare l'ora di inizio e di fine quando si seleziona un intervallo di date predefinito. Selezionare l'intervallo di date predefinito come descritto in precedenza, quindi selezionare l'ora di inizio e di fine come descritto in precedenza. Le date selezionate vengono evidenziate nei calendari, gli orari di inizio e di fine specificati vengono visualizzati nei controlli **Time** e il pulsante **Custom Range** viene evidenziato.
6. Dopo aver selezionato l'intervallo di data e ora, fare clic su **Apply Range** (Applica intervallo). Le statistiche delle performance per quell'intervallo di tempo vengono visualizzate nei grafici e nella timeline degli eventi.

Selezione delle soglie di performance in Counter Chart Zoom View

Applicazione delle soglie nella visualizzazione Zoom dei grafici dei contatori fornisce una vista dettagliata delle occorrenze degli eventi delle soglie delle prestazioni. In questo modo è possibile applicare o rimuovere le soglie e visualizzare immediatamente i risultati, cosa che può essere utile per decidere se la risoluzione dei problemi deve essere la fase successiva.

La selezione delle soglie nella visualizzazione Zoom dei grafici dei contatori consente di visualizzare dati precisi sugli eventi delle soglie di performance. È possibile applicare qualsiasi soglia visualizzata nell'area

Policies della vista Zoom Counter Chart.

È possibile applicare un solo criterio alla volta all'oggetto nella vista Zoom Counter Chart.

Fase

1. Selezionare o deselezionare associato a una policy.

   La soglia selezionata viene applicata alla vista Zoom Counter Chart. Le soglie critiche vengono visualizzate sotto forma di linea rossa; le soglie di avviso vengono visualizzate sotto forma di linea gialla.

Visualizzazione della latenza del volume in base al componente del cluster

È possibile visualizzare informazioni dettagliate sulla latenza di un volume utilizzando la pagina Volume Performance Explorer (Esplora prestazioni volume). Il grafico del contatore latenza - totale mostra la latenza totale sul volume e il grafico del contatore latenza - suddivisione è utile per determinare l'impatto della latenza di lettura e scrittura sul volume.

Inoltre, il grafico latenza - componenti del cluster mostra un confronto dettagliato della latenza di ciascun componente del cluster per determinare il modo in cui ciascun componente contribuisce alla latenza totale sul volume. Vengono visualizzati i seguenti componenti del cluster:

- Rete
- Limite QoS max
- Limite QoS min
- Elaborazione di rete
- Interconnessione cluster
- Elaborazione dei dati
- Operazioni aggregate
- Attivazione del volume
- Risorse MetroCluster
- Latenza del cloud
- Sincronizza SnapMirror

Fasi

1. Nella pagina **Volume Performance Explorer** del volume selezionato, dal grafico della latenza, selezionare **Cluster Components** dal menu a discesa.

   Viene visualizzato il grafico latenza - componenti del cluster.

2. Per visualizzare una versione più grande della mappa, selezionare **Zoom View** (Vista zoom).

   Viene visualizzato il grafico comparativo dei componenti del cluster. È possibile limitare il confronto deselezionando o selezionando associato a ciascun componente del cluster.

3. Per visualizzare i valori specifici, spostare il cursore nell'area del grafico per visualizzare la finestra a comparsa.

Visualizzazione del traffico IOPS SVM in base al protocollo

È possibile visualizzare informazioni IOPS dettagliate per una SVM utilizzando la pagina Esplora prestazioni/SVM. Il grafico IOPS - Total counter mostra l'utilizzo totale degli IOPS sulla SVM, mentre il grafico IOPS - Breakdown counter è utile per determinare l'impatto degli IOPS di lettura, scrittura e altri IOPS sulla SVM.

Inoltre, il grafico IOPS - Protocols (IOPS - protocolli) mostra un confronto dettagliato del traffico IOPS per ciascun protocollo utilizzato sulla SVM. Sono disponibili i seguenti protocolli:

- CIFS
- NFS
- FCP
- ISCSI
- NVMe

Fasi

1. Nella pagina **Performance/SVM Explorer** (Esplora prestazioni/SVM) per la SVM selezionata, dal grafico IOPS, selezionare **Protocols** (protocolli) dal menu a discesa.

   Viene visualizzato il grafico IOPS - protocolli.

2. Per visualizzare una versione più grande della mappa, selezionare **Zoom View** (Vista zoom).

   Viene visualizzato il grafico comparativo del protocollo avanzato IOPS. È possibile limitare il confronto deselezionando o selezionando associato a un protocollo.

3. Per visualizzare i valori specifici, spostare il cursore nell'area del grafico per visualizzare la finestra a comparsa.

Visualizzazione dei diagrammi di latenza del volume e del LUN per verificare la garanzia delle performance

Puoi visualizzare i volumi e le LUN che hai sottoscritto al programma "Performance Guarantee" per verificare che la latenza non superi il livello garantito.

La garanzia delle performance di latenza è un valore di millisecondo per operazione che non deve essere superato. Si basa su una media oraria, non sul periodo predefinito di raccolta delle performance di cinque minuti.

Fasi

1. Nella vista **Performance: All Volumes** (prestazioni: Tutti i volumi) o **Performance: All LUN** (prestazioni: Tutti i LUN), selezionare il volume o il LUN desiderato.
2. Nella pagina **Performance Explorer** del volume o LUN selezionato, selezionare **Hourly Average** (Media oraria) dal selettore **View statistics in** (Visualizza statistiche in).

   La riga orizzontale nel grafico di latenza mostra una linea più uniforme quando le raccolte di cinque minuti vengono sostituite con la media oraria.

3. Se nello stesso aggregato sono presenti altri volumi che rientrano nella garanzia delle performance, è possibile aggiungere tali volumi per visualizzarne il valore di latenza nello stesso grafico.

Visualizzazione delle performance per tutti i cluster di array SAN

È possibile utilizzare la vista Performance: All Clusters (prestazioni: Tutti i cluster) per visualizzare lo stato delle performance di tutti i cluster di array SAN.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

È possibile visualizzare le informazioni generali per tutti i cluster di array SAN nella vista Performance: All Clusters (prestazioni: Tutti i cluster) e i dettagli nella pagina Cluster / Performance Explorer (Explorer cluster/prestazioni).

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Clusters**.
2. Assicurarsi che la colonna "Personality" sia visualizzata nella vista **Health: Tutti i cluster** oppure aggiungerla utilizzando il controllo **Show / Hide**.

   In questa colonna viene visualizzato "All SAN Array" (tutti gli array SAN) per tutti i cluster di array SAN.

3. Per visualizzare le informazioni sulle performance di questi cluster, selezionare la vista **Performance: All Clusters** (prestazioni: Tutti i cluster).

   Visualizzare le informazioni sulle performance per il cluster All SAN Array.

4. Per visualizzare informazioni dettagliate sulle performance di questi cluster, fare clic sul nome di un cluster All SAN Array.
5. Fare clic sulla scheda **Explorer**.
6. Nella pagina **Cluster / Performance Explorer**, selezionare **Nodes on this Cluster** (nodi su questo cluster) dal menu **View and compare** (Visualizza e confronta).

   È possibile confrontare le statistiche delle performance di entrambi i nodi di questo cluster per assicurarsi che il carico sia quasi identico su entrambi i nodi. In caso di grandi discrepanze tra i due nodi, è possibile aggiungere il secondo nodo ai grafici e confrontare i valori in un arco di tempo più lungo per identificare eventuali problemi di configurazione.

Visualizzazione degli IOPS dei nodi in base ai carichi di lavoro che risiedono solo sul nodo locale

Il contatore IOPS del nodo può evidenziare dove le operazioni passano solo attraverso il nodo locale utilizzando una LIF di rete per eseguire operazioni di lettura/scrittura sui volumi su un nodo remoto. I grafici IOPS - "Total (Local)" e "Breakdown (Local)" visualizzano gli IOPS per i dati che risiedono nei volumi locali solo sul nodo corrente.

Le versioni "Local" di questi counter chart sono simili ai diagrammi dei nodi per capacità e utilizzo delle performance, in quanto mostrano anche solo le statistiche dei dati che risiedono sui volumi locali.

Confrontando le versioni "Local" di questi counter chart con le normali versioni Total di questi counter chart, è possibile vedere se il traffico si sposta attraverso il nodo locale per accedere ai volumi sul nodo remoto. Questa situazione potrebbe causare problemi di performance, probabilmente indicati da un elevato utilizzo sul nodo, se sono presenti troppe operazioni che passano attraverso il nodo locale per raggiungere un volume su

un nodo remoto. In questi casi, è possibile spostare un volume nel nodo locale o creare una LIF sul nodo remoto in cui è possibile connettere il traffico proveniente dagli host che accedono a tale volume.

Fasi

1. Nella pagina **Performance/Node Explorer** del nodo selezionato, dal grafico IOPS, selezionare **Total** dal menu a discesa.

   Viene visualizzato il grafico IOPS - Total.

2. Fare clic su **Zoom View** per visualizzare una versione più grande del grafico in una nuova scheda del browser.
3. Nella pagina **Performance/Node Explorer**, dal grafico IOPS, selezionare **Total (Local)** (totale (locale)*) dal menu a discesa.

   Viene visualizzato il grafico IOPS - Total (Local) (IOPS - totale (locale)).

4. Fare clic su **Zoom View** per visualizzare una versione più grande del grafico in una nuova scheda del browser.
5. Visualizzare entrambi i grafici uno accanto all'altro e identificare le aree in cui i valori IOPS sembrano essere molto diversi.
6. Spostare il cursore su queste aree per confrontare gli IOPS locali e totali per un determinato punto nel tempo.

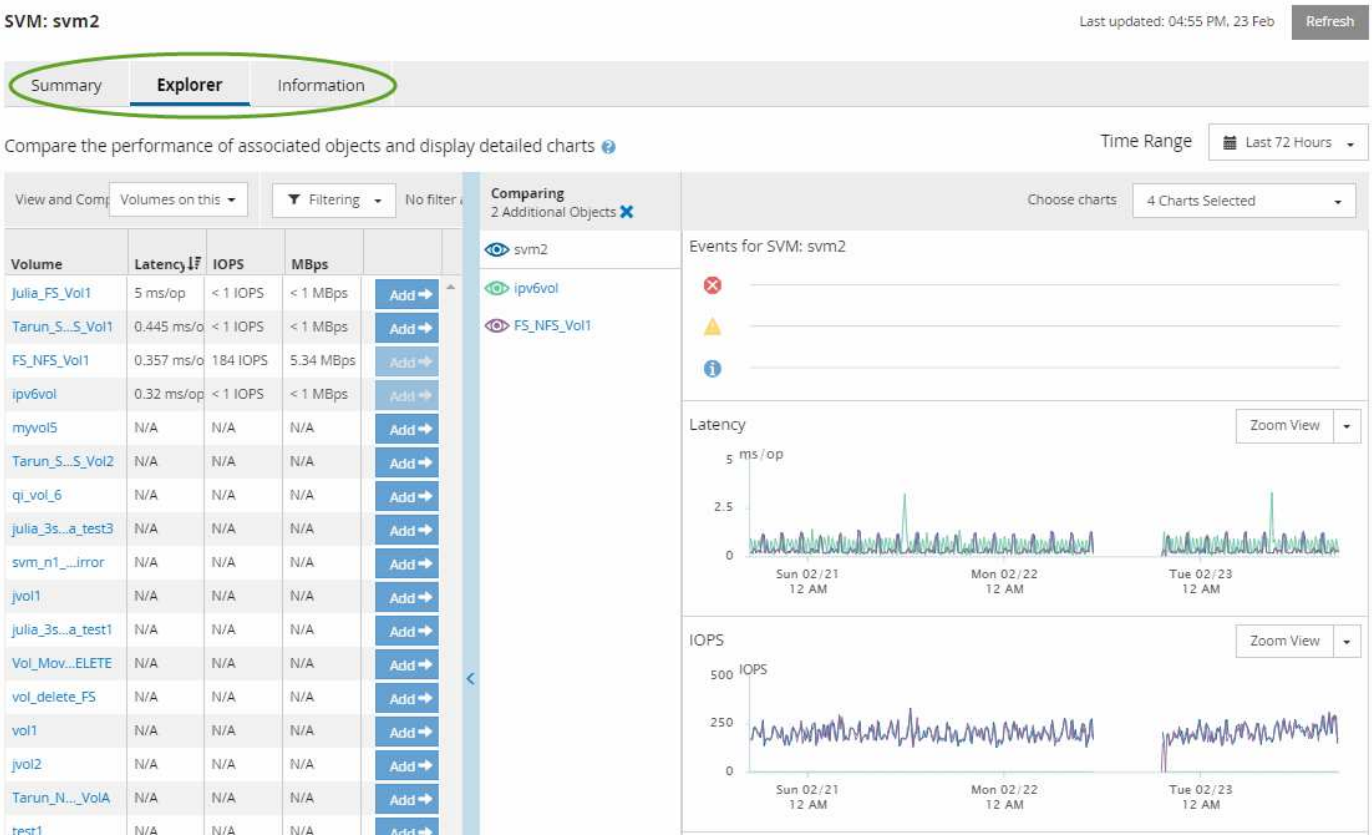
Componenti delle pagine di destinazione degli oggetti

Le pagine di destinazione degli oggetti forniscono dettagli su tutti gli eventi critici, di avviso e informativi. Forniscono una vista dettagliata delle performance di tutti gli oggetti del cluster, consentendo di selezionare e confrontare singoli oggetti in diversi periodi di tempo.

Le pagine di destinazione degli oggetti consentono di esaminare le prestazioni complessive di tutti gli oggetti e di confrontare i dati delle performance degli oggetti in un formato affiancato. Ciò è vantaggioso per la valutazione delle performance e per la risoluzione dei problemi relativi agli eventi.

> I dati visualizzati nei pannelli di riepilogo dei contatori e nei grafici dei contatori si basano su un intervallo di campionamento di cinque minuti. I dati visualizzati nella griglia di inventario degli oggetti sul lato sinistro della pagina si basano su un intervallo di campionamento di un'ora.

L'immagine seguente mostra un esempio di pagina di destinazione degli oggetti che visualizza le informazioni di Esplora risorse:



A seconda dell'oggetto di storage visualizzato, la pagina di destinazione degli oggetti può avere le seguenti schede che forniscono i dati relativi alle prestazioni dell'oggetto:

- Riepilogo

  Visualizza tre o quattro diagrammi dei contatori contenenti gli eventi e le prestazioni per oggetto per il periodo di 72 ore precedente, inclusa una linea di trend che mostra i valori alti e bassi durante il periodo.

- Esplora risorse

  Visualizza una griglia di oggetti di storage correlati all'oggetto corrente, che consente di confrontare i valori delle performance dell'oggetto corrente con quelli degli oggetti correlati. Questa scheda include fino a undici diagrammi di contatore e un selettore di intervalli di tempo, che consentono di eseguire una vasta gamma di confronti.

- Informazioni

  Visualizza i valori per gli attributi di configurazione non relativi alle performance dell'oggetto storage, tra cui la versione installata del software ONTAP, il nome del partner ha e il numero di porte e LIF.

- Migliori prestazioni

  Per i cluster: Visualizza gli oggetti storage con le performance più elevate o più basse, in base al contatore delle performance selezionato.

- Pianificazione del failover

  Per i nodi: Visualizza la stima dell'impatto delle performance su un nodo se il partner ha del nodo si guasta.

- Dettagli

Per i volumi: Visualizza statistiche dettagliate sulle performance per tutte le attività e le operazioni di i/o per il carico di lavoro del volume selezionato. Questa scheda è disponibile per FlexVol Volumes, FlexGroup Volumes e i componenti di FlexGroup.

Pagina di riepilogo

La pagina Summary (Riepilogo) visualizza i diagrammi dei contatori che contengono dettagli sugli eventi e sulle performance per oggetto per il periodo di 72 ore precedente. Questi dati non vengono aggiornati automaticamente, ma sono aggiornati al momento dell'ultimo caricamento della pagina. I grafici nella pagina di riepilogo rispondono alla domanda *devo approfondire?*

Grafici e statistiche dei contatori

I grafici riepilogativi forniscono una panoramica rapida e di alto livello per le ultime 72 ore e consentono di identificare i possibili problemi che richiedono ulteriori indagini.

Le statistiche del contatore delle pagine di riepilogo vengono visualizzate in grafici.

È possibile posizionare il cursore sulla linea di trend in un grafico per visualizzare i valori del contatore per un determinato punto temporale. I grafici riepilogativi visualizzano anche il numero totale di eventi critici e di avviso attivi per il periodo di 72 ore precedente per i seguenti contatori:

- **Latenza**

  Tempo medio di risposta per tutte le richieste i/o, espresso in millisecondi per operazione.

  Visualizzato per tutti i tipi di oggetto.

- **IOPS**

  Velocità operativa media; espressa in operazioni di input/output al secondo.

  Visualizzato per tutti i tipi di oggetto.

- **MB/s**

  Throughput medio, espresso in megabyte al secondo.

  Visualizzato per tutti i tipi di oggetto.

- **Capacità di performance utilizzata**

  Percentuale di capacità di performance consumata da un nodo o aggregato.

  Visualizzato solo per nodi e aggregati.

- **Utilizzo**

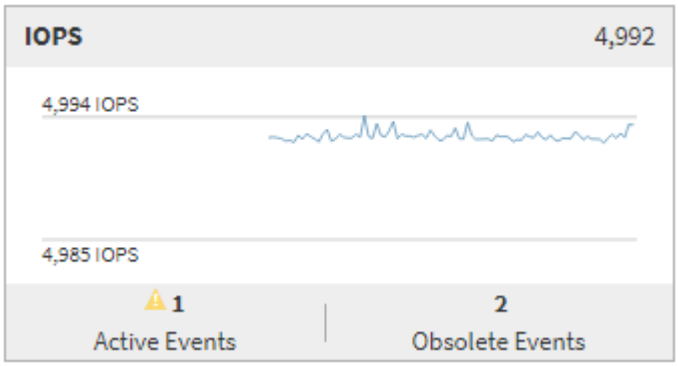
  Percentuale di utilizzo degli oggetti per nodi e aggregati o utilizzo della larghezza di banda per le porte.

  Visualizzato solo per nodi, aggregati e porte.

Posizionando il cursore sul numero di eventi attivi, vengono visualizzati il tipo e il numero di eventi. Gli eventi

critici sono visualizzati in rosso (🟥) e gli eventi di avviso sono visualizzati in giallo (🟨).

Il numero in alto a destra del grafico nella barra grigia è il valore medio delle ultime 72 ore. I numeri visualizzati nella parte inferiore e superiore del grafico a linee di trend sono i valori minimi e massimi per le ultime 72 ore. La barra grigia sotto il grafico contiene il numero di eventi attivi (nuovi e riconosciuti) e obsoleti degli ultimi 72 ore.



- **Grafico del contatore di latenza**

  Il grafico del contatore di latenza fornisce una panoramica di alto livello della latenza dell'oggetto per il periodo di 72 ore precedente. La latenza si riferisce al tempo di risposta medio per tutte le richieste di i/o, espresso in millisecondi per operazione, tempo di servizio, tempo di attesa o entrambi sperimentati da un pacchetto di dati o da un blocco nel componente di storage del cluster in esame.

  Top (valore contatore): il numero nell'intestazione visualizza la media per il periodo di 72 ore precedente.

  Middle (grafico delle performance): il numero nella parte inferiore del grafico mostra la latenza più bassa, mentre il numero nella parte superiore del grafico mostra la latenza più elevata per il periodo precedente di 72 ore. Posizionare il cursore sulla linea di trend del grafico per visualizzare il valore di latenza per un tempo specifico.

  Bottom (eventi): quando si passa il mouse, la finestra a comparsa visualizza i dettagli degli eventi. Fare clic sul collegamento **Eventi attivi** sotto il grafico per accedere alla pagina inventario eventi e visualizzare i dettagli completi dell'evento.

- **Grafico del contatore IOPS**

  Il grafico del contatore IOPS fornisce una panoramica di alto livello dello stato degli IOPS degli oggetti per il periodo di 72 ore precedente. IOPS indica la velocità del sistema di storage in numero di operazioni di input/output al secondo.

  Top (valore contatore): il numero nell'intestazione visualizza la media per il periodo di 72 ore precedente.

  Middle (grafico delle prestazioni): il numero nella parte inferiore del grafico mostra gli IOPS più bassi, mentre il numero nella parte superiore del grafico mostra gli IOPS più elevati per il periodo di 72 ore precedente. Posizionare il cursore sulla linea di trend del grafico per visualizzare il valore IOPS per un tempo specifico.

  Bottom (eventi): quando si passa il mouse, la finestra a comparsa visualizza i dettagli degli eventi. Fare clic sul collegamento **Eventi attivi** sotto il grafico per accedere alla pagina inventario eventi e visualizzare i dettagli completi dell'evento.

- **Grafico del contatore MB/s**

Il grafico del contatore MB/s visualizza le prestazioni dell'oggetto in MB/s e indica la quantità di dati trasferiti da e verso l'oggetto in megabyte al secondo. Il grafico del contatore MB/s fornisce una panoramica di alto livello dello stato dei MB/s dell'oggetto per il periodo di 72 ore precedente.

Top (valore contatore): il numero nell'intestazione visualizza il numero medio di MB/s per il periodo di 72 ore precedente.

Middle (grafico delle prestazioni): il valore nella parte inferiore del grafico mostra il numero più basso di MB/s, mentre il valore nella parte superiore del grafico mostra il numero più alto di MB/s per il periodo di 72 ore precedente. Posizionare il cursore sulla linea di trend del grafico per visualizzare il valore in MB/s per un tempo specifico.

Bottom (eventi): quando si passa il mouse, la finestra a comparsa visualizza i dettagli degli eventi. Fare clic sul collegamento **Eventi attivi** sotto il grafico per accedere alla pagina inventario eventi e visualizzare i dettagli completi dell'evento.

- **Grafico contatore capacità di performance utilizzata**

  Il grafico contatore capacità di performance utilizzata visualizza la percentuale di capacità di performance consumata dall'oggetto.

  Top (valore del contatore): il numero nell'intestazione visualizza la capacità media utilizzata per le performance del periodo precedente di 72 ore.

  Middle (grafico delle performance): il valore nella parte inferiore del grafico mostra la percentuale di capacità delle performance più bassa utilizzata, mentre il valore nella parte superiore del grafico mostra la percentuale di capacità delle performance più elevata utilizzata per il periodo di 72 ore precedente. Posizionare il cursore sulla linea di trend del grafico per visualizzare il valore della capacità di performance utilizzata per un tempo specifico.

  Bottom (eventi): quando si passa il mouse, la finestra a comparsa visualizza i dettagli degli eventi. Fare clic sul collegamento **Eventi attivi** sotto il grafico per accedere alla pagina inventario eventi e visualizzare i dettagli completi dell'evento.

- **Grafico contatore di utilizzo**

  Il grafico del contatore di utilizzo visualizza la percentuale di utilizzo degli oggetti. Il grafico del contatore di utilizzo fornisce una panoramica di alto livello della percentuale di utilizzo dell'oggetto o della larghezza di banda per il periodo di 72 ore precedente.

  Top (valore contatore): il numero nell'intestazione visualizza la percentuale di utilizzo media per il periodo di 72 ore precedente.

  Middle (grafico delle performance): il valore nella parte inferiore del grafico mostra la percentuale di utilizzo più bassa e il valore nella parte superiore del grafico mostra la percentuale di utilizzo più alta per il periodo di 72 ore precedente. Posizionare il cursore sulla linea di trend del grafico per visualizzare il valore di utilizzo per un tempo specifico.

  Bottom (eventi): quando si passa il mouse, la finestra a comparsa visualizza i dettagli degli eventi. Fare clic sul collegamento **Eventi attivi** sotto il grafico per accedere alla pagina inventario eventi e visualizzare i dettagli completi dell'evento.

Eventi

La tabella della cronologia degli eventi, se applicabile, elenca gli eventi più recenti che si sono verificati in

quell'oggetto. Facendo clic sul nome dell'evento, i dettagli dell'evento vengono visualizzati nella pagina Dettagli evento.

Componenti della pagina Performance Explorer

La pagina Performance Explorer (Esplora prestazioni) consente di confrontare le prestazioni di oggetti simili in un cluster, ad esempio tutti i volumi in un cluster. Ciò è vantaggioso quando si troubleshooting degli eventi relativi alle performance e si ottimizza la performance degli oggetti. È inoltre possibile confrontare gli oggetti con l'oggetto root, che rappresenta la base rispetto alla quale vengono effettuati altri confronti tra gli oggetti.

È possibile fare clic sul pulsante **passa alla visualizzazione salute** per visualizzare la pagina dei dettagli sullo stato di salute dell'oggetto. In alcuni casi, è possibile ottenere importanti informazioni sulle impostazioni di configurazione dello storage per questo oggetto che potrebbero essere utili per la risoluzione di un problema.

La pagina Performance Explorer (Esplora prestazioni) visualizza un elenco di oggetti cluster e dei relativi dati sulle prestazioni. In questa pagina vengono visualizzati tutti gli oggetti cluster dello stesso tipo (ad esempio, i volumi e le relative statistiche sulle prestazioni specifiche dell'oggetto) in formato tabulare. Questa vista offre una panoramica efficiente delle performance degli oggetti del cluster.

Se "N/A" viene visualizzato in una cella della tabella, significa che un valore per quel contatore non è disponibile perché al momento non c'è alcun i/o su quell'oggetto.

La pagina Performance Explorer contiene i seguenti componenti:

- **Intervallo di tempo**

  Consente di selezionare un intervallo di tempo per i dati dell'oggetto.

  È possibile scegliere un intervallo predefinito o specificare un intervallo di tempo personalizzato.

- **Visualizza e confronta**

  Consente di selezionare il tipo di oggetto correlato da visualizzare nella griglia.

  Le opzioni disponibili dipendono dal tipo di oggetto root e dai dati disponibili. Fare clic sull'elenco a discesa Visualizza e confronta per selezionare un tipo di oggetto. Il tipo di oggetto selezionato viene visualizzato nell'elenco.

- **Filtraggio**

  Consente di ridurre la quantità di dati ricevuti in base alle preferenze.

  È possibile creare filtri applicabili ai dati dell'oggetto, ad esempio IOPS superiori a 4. È possibile aggiungere fino a quattro filtri simultanei.

- **Confronto**

  Visualizza un elenco degli oggetti selezionati per il confronto con l'oggetto root.

  I dati degli oggetti nel pannello di confronto vengono visualizzati nei Counter Chart.

- **Visualizza statistiche in**

Per volumi e LUN, consente di selezionare se visualizzare le statistiche dopo ogni ciclo di raccolta (impostazione predefinita: 5 minuti) o se visualizzare le statistiche come media oraria. Questa funzionalità consente di visualizzare il grafico della latenza a supporto del programma "Performance Guarantee" di NetApp.

- **Counter Chart**

  Visualizza i dati grafici per ciascuna categoria di prestazioni dell'oggetto.

  In genere, per impostazione predefinita vengono visualizzati solo tre o quattro grafici. Il componente Scegli grafici consente di visualizzare grafici aggiuntivi o di nascondere grafici specifici. Puoi anche scegliere di mostrare o nascondere la cronologia degli eventi.

- **Cronologia eventi**

  Visualizza gli eventi relativi alle performance e allo stato di salute che si verificano nella sequenza temporale selezionata nel componente intervallo di tempo.

Gestione delle performance utilizzando le informazioni del gruppo di policy QoS

Unified Manager consente di visualizzare i gruppi di policy di qualità del servizio (QoS) disponibili su tutti i cluster monitorati. Le policy possono essere state definite utilizzando il software ONTAP (Gestore di sistema o l'interfaccia utente di ONTAP) o le policy del livello di servizio per le performance di Unified Manager. Unified Manager visualizza anche i volumi e le LUN a cui è stato assegnato un gruppo di criteri QoS.

Per ulteriori informazioni sulla regolazione delle impostazioni QoS, vedere "Panoramica sulla gestione delle performance"

In che modo la QoS dello storage può controllare il throughput dei carichi di lavoro

È possibile creare un gruppo di criteri QoS (Quality of Service) per controllare il limite di i/o al secondo (IOPS) o throughput (MB/s) per i carichi di lavoro in esso contenuti. Se i carichi di lavoro si trovano in un gruppo di policy senza limiti impostati, ad esempio il gruppo di policy predefinito, o se il limite impostato non soddisfa le esigenze, è possibile aumentare il limite o spostare i carichi di lavoro in un gruppo di policy nuovo o esistente con il limite desiderato.

I gruppi di policy QoS "tradizionale" possono essere assegnati a singoli carichi di lavoro, ad esempio un singolo volume o LUN. In questo caso, il carico di lavoro può utilizzare il limite di throughput completo. I gruppi di policy di QoS possono anche essere assegnati a più carichi di lavoro, nel qual caso il limite di throughput è "sharred" tra i carichi di lavoro. Ad esempio, un limite di QoS di 9,000 IOPS assegnati a tre carichi di lavoro limiterebbe gli IOPS combinati a superare 9,000 IOPS.

I gruppi di policy QoS "Adaptive" possono essere assegnati anche a singoli carichi di lavoro o a più carichi di lavoro. Tuttavia, anche se assegnato a più carichi di lavoro, ogni carico di lavoro ottiene il limite massimo di throughput invece di condividere il valore di throughput con altri carichi di lavoro. Inoltre, le policy QoS adattive regolano automaticamente l'impostazione del throughput in base alle dimensioni del volume, per ogni carico di lavoro, mantenendo così il rapporto tra IOPS e terabyte al variare delle dimensioni del volume. Ad esempio, se il picco è impostato su 5,000 IOPS/TB in una policy QoS adattiva, un volume da 10 TB avrà un throughput

massimo di 50,000 IOPS. Se il volume viene ridimensionato successivamente a 20 TB, la QoS adattiva regola il massimo a 100,000 IOPS.

A partire da ONTAP 9.5, è possibile includere le dimensioni del blocco quando si definisce un criterio QoS adattivo. In questo modo, la policy viene convertita da una soglia IOPS/TB a una soglia MB/s per i casi in cui i carichi di lavoro utilizzano blocchi di dimensioni molto grandi e, in ultima analisi, utilizzano una grande percentuale di throughput.

Per le policy QoS di gruppo condiviso, quando gli IOPS o i MB/s di tutti i workload di un gruppo di policy superano il limite impostato, il gruppo di policy limita i workload per limitare la loro attività, riducendo così le performance di tutti i workload del gruppo di policy. Se un evento di performance dinamica viene generato dalla limitazione del gruppo di criteri, la descrizione dell'evento visualizza il nome del gruppo di criteri interessato.

Nella vista Performance: All Volumes (prestazioni: Tutti i volumi), è possibile ordinare i volumi interessati in base a IOPS e MB/s per vedere quali carichi di lavoro hanno il massimo utilizzo che potrebbe aver contribuito all'evento. Nella pagina Performance/Volumes Explorer (Esplora prestazioni/volumi), è possibile selezionare altri volumi o LUN sul volume per confrontare l'utilizzo del throughput IOPS o Mbps del carico di lavoro interessato.

Assegnando i carichi di lavoro che stanno utilizzando in eccesso le risorse del nodo a un'impostazione di gruppo di policy più restrittiva, il gruppo di policy limita i carichi di lavoro per limitare la loro attività, riducendo così l'utilizzo delle risorse su quel nodo. Tuttavia, se si desidera che il carico di lavoro sia in grado di utilizzare più risorse del nodo, è possibile aumentare il valore del gruppo di criteri.

È possibile utilizzare Gestione di sistema, i comandi ONTAP o i livelli di servizio delle prestazioni di Unified Manager per gestire i gruppi di criteri, incluse le seguenti attività:

- Creazione di un gruppo di criteri
- Aggiunta o rimozione di workload in un gruppo di policy
- Spostamento di un workload tra gruppi di policy
- Modifica del limite di throughput di un gruppo di criteri
- Spostamento di un workload in un aggregato e/o nodo diverso

Visualizzazione di tutti i gruppi di policy QoS disponibili su tutti i cluster

È possibile visualizzare un elenco di tutti i gruppi di criteri QoS disponibili nei cluster monitorati da Unified Manager. Ciò include le policy QoS tradizionali, le policy QoS adattive e le policy QoS gestite dalle policy del livello di servizio delle performance di Unified Manager.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **QoS Policy Groups**.

   Per impostazione predefinita, viene visualizzata la vista Performance: Traditional QoS Policy Groups (prestazioni: Gruppi policy QoS tradizionali)

2. Visualizzare le impostazioni di configurazione dettagliate per ciascun gruppo di policy QoS tradizionale disponibile.
3. Fare clic sul pulsante Espandi ( ) Accanto al nome del gruppo di criteri QoS per visualizzare ulteriori dettagli sul gruppo di criteri.
4. Nel menu View (Visualizza), selezionare una delle opzioni aggiuntive per visualizzare tutti i gruppi di criteri

QoS adattivi o tutti i gruppi di criteri QoS creati utilizzando i livelli di servizio delle prestazioni di Unified Manager.

Visualizzazione di volumi o LUN che si trovano nello stesso gruppo di criteri QoS

È possibile visualizzare un elenco dei volumi e delle LUN assegnati allo stesso gruppo di criteri QoS.

Nel caso di gruppi di policy QoS tradizionali che sono “scontrassegnati” tra più volumi, ciò può essere utile per verificare se alcuni volumi stanno utilizzando in eccesso il throughput definito per il gruppo di policy. Può anche aiutare a decidere se aggiungere altri volumi al gruppo di criteri senza influire negativamente sugli altri volumi.

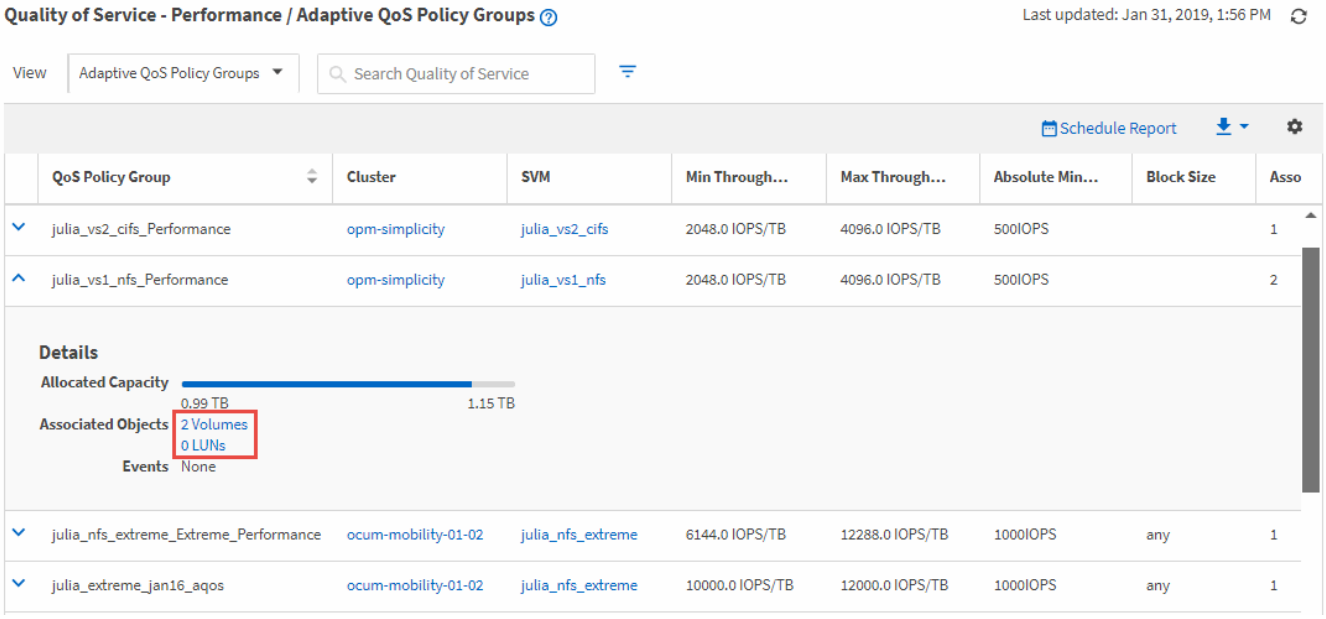
Nel caso di policy QoS adattive e policy dei livelli di servizio delle performance di Unified Manager, Questa operazione può essere utile per visualizzare tutti i volumi o le LUN che utilizzano un gruppo di criteri in modo da visualizzare gli oggetti interessati se si modificano le impostazioni di configurazione per il criterio QoS.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **QoS Policy Groups**.

   Per impostazione predefinita, viene visualizzata la vista Performance: Traditional QoS Policy Groups (prestazioni: Gruppi policy QoS tradizionali)

2. Se sei interessato al gruppo di policy tradizionale, consulta questa pagina. In caso contrario, selezionare una delle opzioni di visualizzazione aggiuntive per visualizzare tutti i gruppi di criteri QoS adattivi o tutti i gruppi di criteri QoS creati dai livelli di servizio delle prestazioni di Unified Manager.
3. Nella policy QoS desiderata, fare clic sul pulsante Espandi ( ) Accanto al nome del gruppo di criteri QoS per visualizzare ulteriori
   dettagli.



4. Fare clic sul collegamento Volumes (volumi) o LUNs (LUN) per visualizzare gli oggetti che utilizzano questo criterio QoS.

   Viene visualizzata la pagina Performance Inventory (inventario delle performance) per i volumi o le LUN con l’elenco ordinato degli oggetti che utilizzano la policy QoS.

Visualizzazione delle impostazioni del gruppo di criteri QoS applicate a volumi o LUN specifici

È possibile visualizzare i gruppi di criteri QoS applicati ai volumi e alle LUN e collegarsi alla vista Performance/QoS Policy Groups per visualizzare le impostazioni di configurazione dettagliate per ciascun criterio QoS.

Di seguito sono riportati i passaggi per visualizzare il criterio QoS applicato a un volume. I passaggi per visualizzare queste informazioni per un LUN sono simili.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.

   Per impostazione predefinita, viene visualizzata la vista Health: All Volumes (Salute: Tutti i volumi).

2. Nel menu View (Visualizza), selezionare **Performance: Volumes in QoS Policy Group** (prestazioni: Volumi nel gruppo di criteri QoS).
3. Individuare il volume che si desidera rivedere e scorrere verso destra fino a visualizzare la colonna **QoS Policy Group**.
4. Fare clic sul nome del gruppo di criteri QoS.

   La pagina qualità del servizio corrispondente viene visualizzata a seconda che si tratti di una policy QoS tradizionale, di una policy QoS adattiva o di una policy QoS creata utilizzando i livelli di servizio delle performance di Unified Manager.

5. Visualizzare le impostazioni di configurazione dettagliate per il gruppo di criteri QoS.
6. Fare clic sul pulsante Espandi ( ) Accanto al nome del gruppo di criteri QoS per visualizzare ulteriori dettagli sul gruppo di criteri.

Visualizzazione dei grafici delle performance per confrontare volumi o LUN che si trovano nello stesso gruppo di criteri QoS

È possibile visualizzare i volumi e le LUN che si trovano negli stessi gruppi di policy QoS e confrontare le performance su un singolo grafico IOPS, MB/s o IOPS/TB per identificare eventuali problemi.

Di seguito sono riportati i passaggi per confrontare le prestazioni dei volumi nello stesso gruppo di criteri QoS. I passaggi per visualizzare queste informazioni per un LUN sono simili.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.

   Per impostazione predefinita, viene visualizzata la vista Health: All Volumes (Salute: Tutti i volumi).

2. Nel menu View (Visualizza), selezionare **Performance: Volumes in QoS Policy Group** (prestazioni: Volumi nel gruppo di criteri QoS).
3. Fare clic sul nome del volume che si desidera rivedere.

   Viene visualizzata la pagina Performance Explorer (Esplora prestazioni) per il volume.

4. Nel menu View and compare (Visualizza e confronta), selezionare **Volumes in same QoS Policy Group**

(volumi nello stesso gruppo di criteri QoS).

Gli altri volumi che condividono la stessa policy QoS sono elencati nella tabella seguente.

5. Fare clic sul pulsante **Add** (Aggiungi) per aggiungere i volumi ai grafici in modo da poter confrontare IOPS, MB/s, IOPS/TB e altri contatori delle prestazioni per tutti i volumi selezionati nei grafici.

   È possibile modificare l'intervallo di tempo per visualizzare le prestazioni su intervalli di tempo diversi da quelli predefiniti di 72 ore.

Come vengono visualizzati i diversi tipi di policy QoS nei grafici di throughput

È possibile visualizzare le impostazioni dei criteri di qualità del servizio (QoS) definite da ONTAP che sono state applicate a un volume o LUN nei grafici IOPS, IOPS/TB e MB/s di Performance Explorer e Workload Analysis. Le informazioni visualizzate nei grafici variano a seconda del tipo di policy QoS applicata al carico di lavoro.

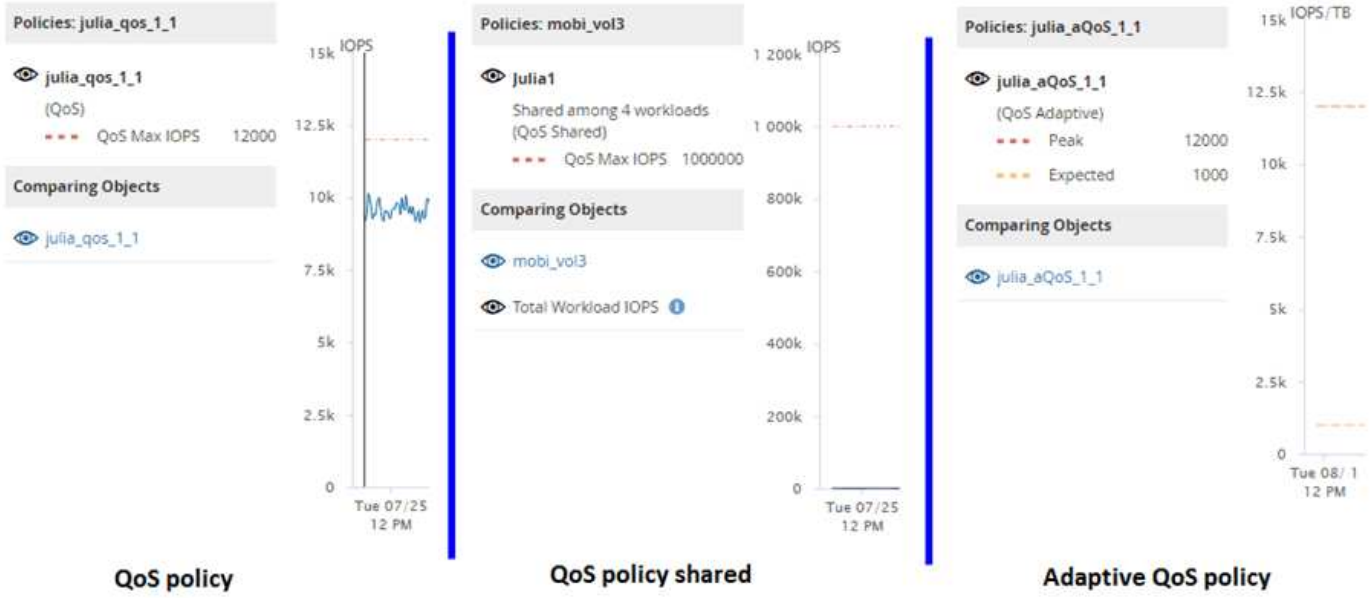
Un'impostazione di throughput massimo (o "peak") definisce il throughput massimo che il carico di lavoro può consumare, limitando così l'impatto sui carichi di lavoro concorrenti per le risorse di sistema. Un'impostazione di throughput minimo (o "previsto") definisce il throughput minimo che deve essere disponibile per il carico di lavoro in modo che un carico di lavoro critico soddisfi gli obiettivi di throughput minimi indipendentemente dalla domanda dei carichi di lavoro concorrenti.

Le policy QoS condivise e non condivise per IOPS e MB/s utilizzano i termini "minimum" e "maximum" per definire il piano e il soffitto. Le policy di QoS adattive per IOPS/TB, introdotte in ONTAP 9.3, utilizzano i termini "previsto" e "picco" per definire il pavimento e il soffitto.

Mentre ONTAP consente di creare questi due tipi di policy di qualità del servizio, a seconda di come vengono applicate ai carichi di lavoro, esistono tre modi in cui la policy di qualità del servizio verrà visualizzata nei grafici delle performance.

Tipo di policy	Funzionalità	Indicatore nell'interfaccia di Unified Manager
Policy condivisa QoS assegnata a un singolo carico di lavoro o policy non condivisa QoS assegnata a un singolo carico di lavoro o a più carichi di lavoro	Ogni carico di lavoro può utilizzare l'impostazione di throughput specificata	Visualizza "(QoS)"
Policy condivisa QoS assegnata a più carichi di lavoro	Tutti i carichi di lavoro condividono l'impostazione di throughput specificata	Visualizza "(QoS Shared)"
Policy QoS adattiva assegnata a un singolo workload o a più workload	Ogni carico di lavoro può utilizzare l'impostazione di throughput specificata	Visualizza "(QoS Adaptive)"

La figura seguente mostra un esempio di come le tre opzioni sono mostrate nei diagrammi dei contatori.



Quando una normale policy di QoS definita in IOPS viene visualizzata nel grafico IOPS/TB per un carico di lavoro, ONTAP converte il valore IOPS in un valore IOPS/TB e visualizza tale policy nel grafico IOPS/TB insieme al testo “QoS, defined in IOPS”.

Quando una policy QoS adattiva definita in IOPS/TB viene visualizzata nel grafico IOPS per un carico di lavoro, ONTAP converte il valore IOPS/TB in un valore IOPS e Unified Manager visualizza tale policy nel grafico IOPS insieme al testo “QoS adattiva - utilizzato, Definito in IOPS/TB” o “QoS Adaptive - Allocated, defined in IOPS/TB” a seconda di come è configurata l’impostazione di allocazione IOPS di picco. Quando l’impostazione di allocazione è impostata su “allocated-space”, gli IOPS di picco vengono calcolati in base alle dimensioni del volume. Quando l’impostazione di allocazione è impostata su “used-space”, gli IOPS di picco vengono calcolati in base alla quantità di dati memorizzati nel volume, tenendo conto dell’efficienza dello storage.

Il grafico IOPS/TB visualizza i dati sulle prestazioni solo quando la capacità logica utilizzata dal volume è maggiore o uguale a 128 GB. I gap vengono visualizzati nel grafico quando la capacità utilizzata scende al di sotto di 128 GB durante il periodo di tempo selezionato.

Visualizzazione delle impostazioni minime e massime QoS del carico di lavoro in Performance Explorer

È possibile visualizzare le impostazioni dei criteri della qualità del servizio (QoS) definita da ONTAP su un volume o LUN nei grafici di Performance Explorer. Un’impostazione del throughput massimo limita l’impatto dei carichi di lavoro concorrenti sulle risorse di sistema. Un’impostazione di throughput minimo garantisce che un carico di lavoro critico soddisfi gli obiettivi di throughput minimi indipendentemente dalla domanda dei carichi di lavoro concorrenti.

Le impostazioni di throughput QoS “minimum” e “maximum” IOPS e MB/s vengono visualizzate nei diagrammi dei contatori solo se sono state configurate in ONTAP. Le impostazioni minime di throughput sono disponibili solo sui sistemi che eseguono ONTAP 9.2 o software successivo, solo sui sistemi AFF e possono essere impostate solo per gli IOPS in questo momento.

Le policy QoS adattive sono disponibili a partire da ONTAP 9.3 e vengono espresse utilizzando IOPS/TB invece di IOPS. Questi criteri regolano automaticamente il valore del criterio QoS in base alle dimensioni del

volume, per ogni carico di lavoro, mantenendo così il rapporto tra IOPS e terabyte al variare delle dimensioni del volume. È possibile applicare un gruppo di criteri QoS adattivi solo ai volumi. La terminologia QoS "previsto" e "picco" vengono utilizzate per le policy QoS adattive invece che per quelle minime e massime.

Unified Manager genera eventi di avviso per le violazioni delle policy QoS quando il throughput del carico di lavoro ha superato l'impostazione della policy QoS massima definita durante ciascun periodo di raccolta delle performance per l'ora precedente. Il throughput del carico di lavoro può superare la soglia QoS solo per un breve periodo di tempo durante ciascun periodo di raccolta, ma Unified Manager visualizza il throughput "Average" durante il periodo di raccolta sul grafico. Per questo motivo, è possibile che vengano visualizzati eventi QoS mentre il throughput di un carico di lavoro potrebbe non aver superato la soglia di policy indicata nel grafico.

Fasi

1. Nella pagina **Performance Explorer** relativa al volume o al LUN selezionato, eseguire le seguenti operazioni per visualizzare le impostazioni relative al limite di QoS e al piano:

Se si desidera…	Eseguire questa operazione…
Visualizza il tetto IOPS (QoS max)	Nel grafico IOPS Total (totale IOPS) o Breakdown (dettaglio), fare clic su **Zoom View (Vista zoom)**.
Visualizzare il limite MB/s (QoS max)	Nel grafico MB/s Total (totale MB/s) o Breakdown (dettaglio), fare clic su **Zoom View (Vista zoom)**.
Visualizza il piano IOPS (QoS min)	Nel grafico IOPS Total (totale IOPS) o Breakdown (dettaglio), fare clic su **Zoom View (Vista zoom)**.
Visualizza il tetto di IOPS/TB (il picco di QoS)	Per i volumi, nel grafico IOPS/TB, fare clic su **Zoom View**.
Visualizza il piano IOPS/TB (QoS previsto)	Per i volumi, nel grafico IOPS/TB, fare clic su **Zoom View**.

   La linea orizzontale tratteggiata indica il valore massimo o minimo di throughput impostato in ONTAP. È inoltre possibile visualizzare quando sono state implementate le modifiche ai valori QoS.

2. Per visualizzare i valori IOPS e MB/s specifici rispetto all'impostazione QoS, spostare il cursore nell'area del grafico per visualizzare la finestra a comparsa.

Se si nota che alcuni volumi o LUN hanno IOPS o MB/s molto elevati e stanno insistendo sulle risorse di sistema, è possibile utilizzare Gestione di sistema o l'interfaccia utente di ONTAP per regolare le impostazioni di QoS in modo che questi carichi di lavoro non influiscano sulle prestazioni di altri carichi di lavoro.

Per ulteriori informazioni sulla regolazione delle impostazioni QoS, vedere "Panoramica sulla gestione delle performance"

Gestire le performance utilizzando la capacità delle performance e le informazioni IOPS disponibili

Performance Capacity indica la quantità di throughput che è possibile ottenere da una risorsa senza superare le utili performance di tale risorsa. Quando viene visualizzata

utilizzando i contatori delle performance esistenti, la capacità delle performance è il punto in cui si ottiene il massimo utilizzo da un nodo o aggregato prima che la latenza diventi un problema.

Unified Manager raccoglie le statistiche sulla capacità delle performance dai nodi e dagli aggregati di ciascun cluster. *Capacità di performance utilizzata* è la percentuale di capacità di performance attualmente utilizzata e *capacità di performance libera* è la percentuale di capacità di performance ancora disponibile.

Mentre la capacità delle performance libera fornisce una percentuale della risorsa ancora disponibile, *IOPS disponibili* indica il numero di IOPS che possono essere aggiunti alla risorsa prima di raggiungere la capacità di performance massima. Utilizzando questa metrica, puoi essere sicuro di poter aggiungere carichi di lavoro di un numero predeterminato di IOPS a una risorsa.

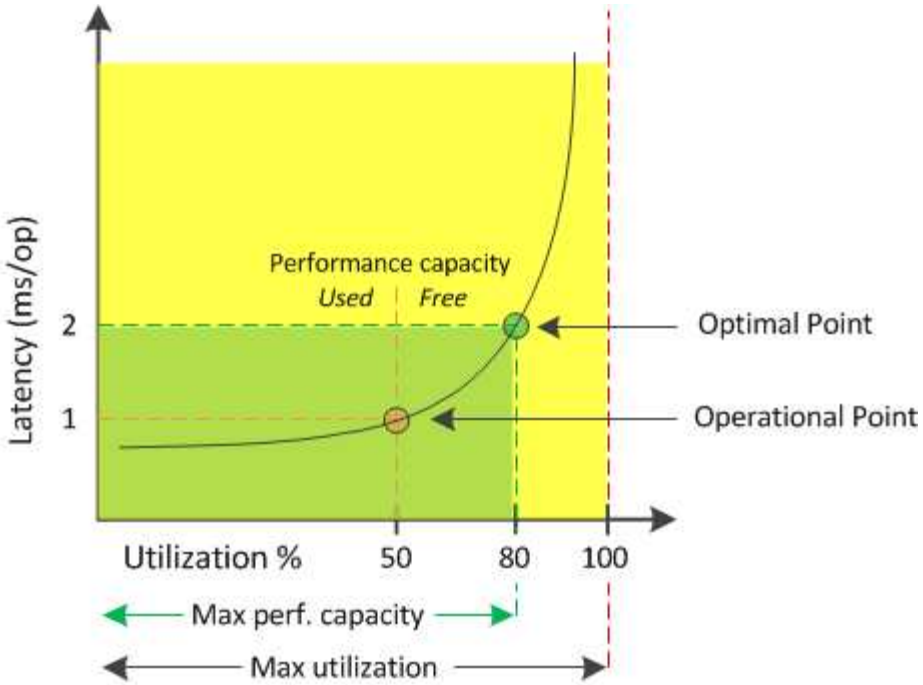
Il monitoraggio delle informazioni sulla capacità delle performance offre i seguenti vantaggi:

- Fornisce assistenza per il provisioning e il bilanciamento del workflow.
- Consente di evitare di sovraccaricare un nodo o di spingerne le risorse oltre il punto ottimale, riducendo così la necessità di eseguire il troubleshooting.
- Consente di determinare con maggiore precisione dove potrebbero essere necessarie apparecchiature di storage aggiuntive.

Qual è la capacità di performance utilizzata

Il contatore delle performance utilizzate consente di identificare se le performance di un nodo o di un aggregato stanno raggiungendo un punto in cui le performance potrebbero degradarsi se i carichi di lavoro aumentano. Può anche mostrare se un nodo o un aggregato è attualmente in uso in eccesso durante periodi di tempo specifici. La capacità di performance utilizzata è simile all'utilizzo, ma la prima fornisce maggiori informazioni sulle capacità di performance disponibili in una risorsa fisica per un carico di lavoro specifico.

La capacità di performance ottimale utilizzata è il punto in cui un nodo o un aggregato ha un utilizzo e una latenza ottimali (tempo di risposta) e viene utilizzato in modo efficiente. Nella figura seguente viene mostrata una curva di latenza rispetto all'utilizzo di esempio per un aggregato.



In questo esempio, il *punto operativo* indica che l'aggregato sta attualmente operando al 50% di utilizzo con una latenza di 1.0 ms/op. In base alle statistiche acquisite dall'aggregato, Unified Manager determina che è disponibile una capacità di performance aggiuntiva per questo aggregato. In questo esempio, il *punto ottimale* viene identificato come il punto in cui l'aggregato è al 80% di utilizzo con latenza di 2.0 ms/op. Pertanto, è possibile aggiungere più volumi e LUN a questo aggregato in modo che i sistemi vengano utilizzati in modo più efficiente.

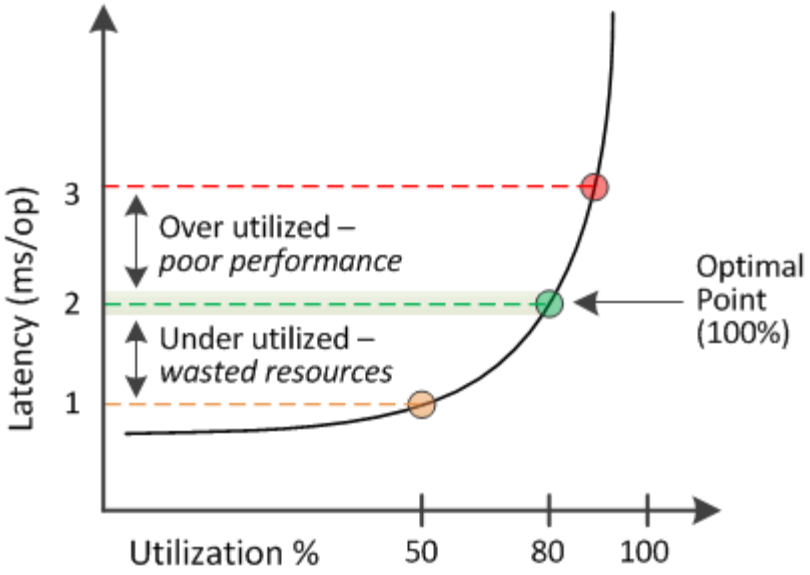
Si prevede che il contatore della capacità di performance utilizzata sia un numero maggiore del contatore "Utilization", in quanto la capacità di performance aumenta l'impatto sulla latenza. Ad esempio, se si utilizza un nodo o un aggregato al 70%, il valore della capacità delle performance può essere compreso tra il 80% e il 100%, a seconda del valore di latenza.

In alcuni casi, tuttavia, il contatore di utilizzo potrebbe essere più alto nella pagina Dashboard. Questo è normale perché il dashboard aggiorna i valori correnti del contatore in ogni periodo di raccolta; non visualizza le medie in un periodo di tempo come le altre pagine nell'interfaccia utente di Unified Manager. Il contatore della capacità di performance utilizzata viene utilizzato al meglio come indicatore delle performance medie in un periodo di tempo, mentre il contatore di utilizzo viene utilizzato al meglio per determinare l'utilizzo istantaneo di una risorsa.

Cosa significa il valore utilizzato dalla capacità delle performance

Il valore utilizzato per la capacità delle performance ti aiuta a identificare i nodi e gli aggregati che sono attualmente sovrautilizzati o sottoutilizzati. Ciò consente di ridistribuire i carichi di lavoro per rendere le risorse di storage più efficienti.

La figura seguente mostra la curva di latenza rispetto all'utilizzo di una risorsa e identifica, con punti colorati, tre aree in cui è possibile individuare il punto operativo corrente.



- Una percentuale di performance utilizzata pari a 100 è al punto ottimale.

  A questo punto, le risorse vengono utilizzate in modo efficiente.

- Una percentuale di performance utilizzata superiore a 100 indica che il nodo o l'aggregato è sovrautilizzato e che i carichi di lavoro ricevono performance non ottimali.

  Non aggiungere nuovi workload alla risorsa e potrebbe essere necessario ridistribuire i workload esistenti.

- Una percentuale di performance utilizzata inferiore a 100 indica che il nodo o l'aggregato è sottoutilizzato e che le risorse non vengono utilizzate in modo efficace.

  È possibile aggiungere più carichi di lavoro alla risorsa.

> A differenza dell'utilizzo, la percentuale di performance della capacità utilizzata può essere superiore al 100%. Non esiste una percentuale massima, ma le risorse in genere rientrano nell'intervallo compreso tra il 110% e il 140% quando vengono utilizzate in eccesso. Percentuali più elevate indicano una risorsa con problemi gravi.

Quali IOPS sono disponibili

Il contatore IOPS disponibile identifica il numero rimanente di IOPS che è possibile aggiungere a un nodo o a un aggregato prima che la risorsa raggiunga il limite.

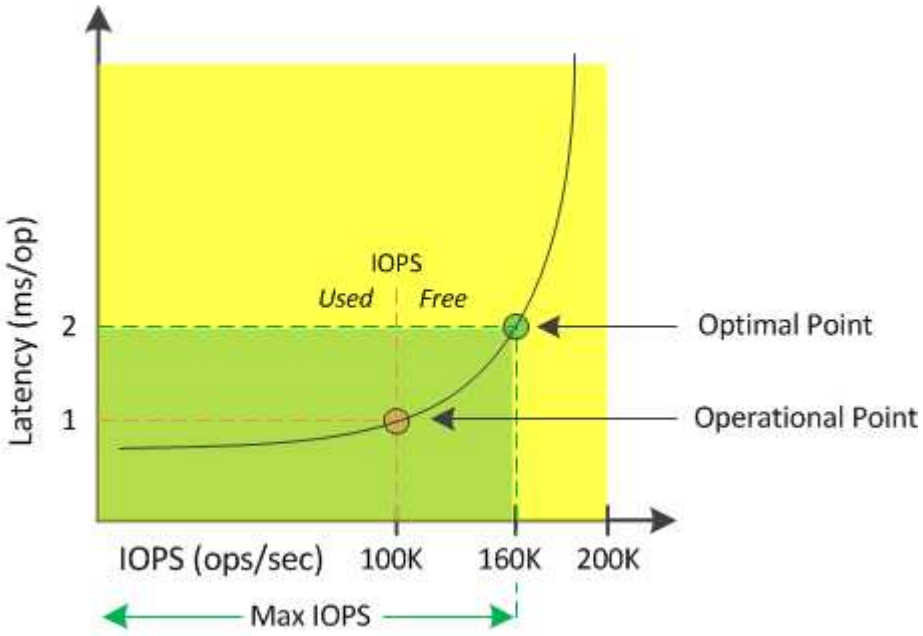
Gli IOPS totali che un nodo può fornire si basano sulle caratteristiche fisiche del nodo, ad esempio il numero di CPU, la velocità della CPU e la quantità di RAM. Gli IOPS totali che un aggregato può fornire si basano sulle proprietà fisiche dei dischi, ad esempio un disco SATA, SAS o SSD.

Gli IOPS totali di tutti i volumi in un aggregato potrebbero non corrispondere agli IOPS totali dell'aggregato. Questo argomento viene trattato nel seguente articolo della Knowledge base: KB "Perché la somma di tutti gli IOPS di un volume in un aggregato non corrisponde agli IOPS aggregati?"

Mentre il contatore di performance free fornisce la percentuale di una risorsa ancora disponibile, il contatore IOPS disponibile indica che è possibile aggiungere un numero esatto di IOPS (carichi di lavoro) a una risorsa prima di raggiungere la capacità di performance massima.

Ad esempio, se si utilizza una coppia di sistemi storage FAS2520 e FAS8060, un valore del 30% senza capacità di performance significa che si dispone di una certa capacità di performance libera. Tuttavia, questo valore non fornisce visibilità sul numero di workload che è possibile implementare in tali nodi. Il contatore IOPS disponibile potrebbe indicare che sono disponibili 500 IOPS su FAS8060, ma solo 100 IOPS su FAS2520.

Nella figura seguente viene mostrato un esempio di latenza rispetto alla curva IOPS per un nodo.



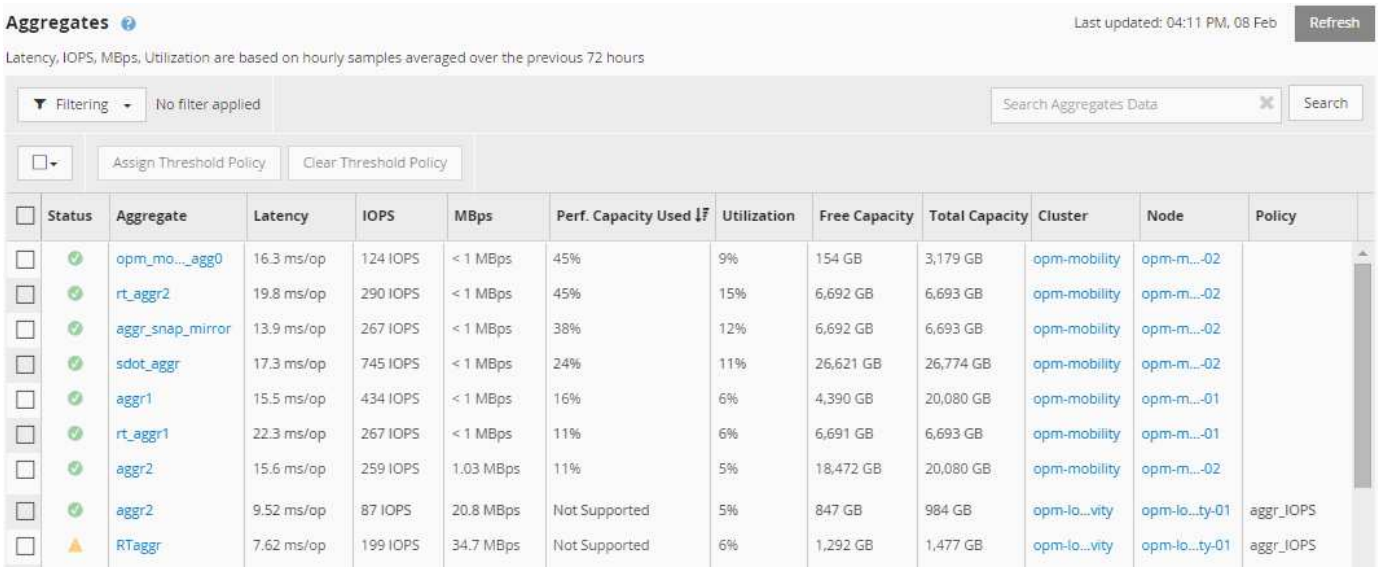
Il numero massimo di IOPS che una risorsa può fornire è il numero di IOPS quando il contatore della capacità di performance utilizzata è al 100% (il punto ottimale). Il punto operativo indica che il nodo sta attualmente operando a 100.000 IOPS con latenza di 1.0 ms/op. In base alle statistiche acquisite dal nodo, Unified Manager determina che il numero massimo di IOPS per il nodo è 160K, il che significa che ci sono 60K IOPS liberi o disponibili. Pertanto, è possibile aggiungere più carichi di lavoro a questo nodo in modo che i sistemi vengano utilizzati in modo più efficiente.

Quando l'attività dell'utente nella risorsa è minima, il valore IOPS disponibile viene calcolato ipotizzando un carico di lavoro generico basato su circa 4,500 IOPS per core della CPU. Ciò è dovuto al fatto che Unified Manager non dispone dei dati necessari per stimare con precisione le caratteristiche del carico di lavoro che viene servito.

Visualizzazione dei valori utilizzati per la capacità di nodo e le performance aggregate

È possibile monitorare i valori della capacità di performance utilizzata per tutti i nodi o per tutti gli aggregati di un cluster oppure visualizzare i dettagli di un singolo nodo o aggregato.

I valori utilizzati per la capacità delle performance vengono visualizzati nella dashboard, nelle pagine Performance Inventory, nella pagina Top Performer, nella pagina Create Threshold Policy, nelle pagine Performance Explorer e nei grafici dettagliati. Ad esempio, la pagina Performance: All aggregates (prestazioni: Tutti gli aggregati) fornisce una colonna Performance Capacity (capacità di performance) utilizzata per visualizzare il valore della capacità di performance utilizzata per tutti gli aggregati.



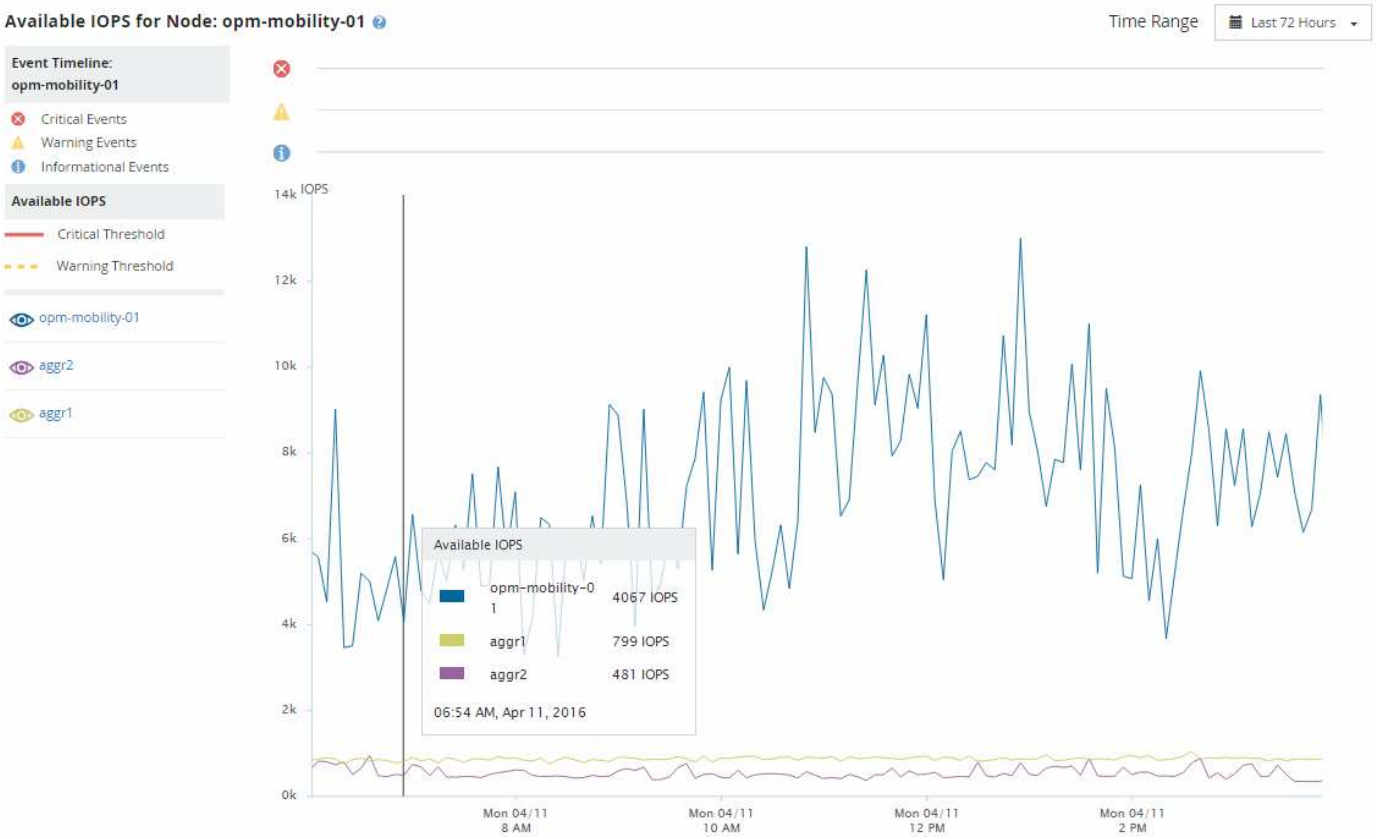
Il monitoraggio del contatore della capacità di performance utilizzata consente di identificare quanto segue:

- Sia che i nodi o gli aggregati di qualsiasi cluster abbiano un valore di utilizzo della capacità dalle performance elevate
- Sia che i nodi o gli aggregati di qualsiasi cluster abbiano eventi attivi di utilizzo della capacità delle performance
- I nodi e gli aggregati che hanno il valore più alto e più basso utilizzato per le performance in un cluster
- Valori dei contatori di latenza e utilizzo in combinazione con nodi o aggregati che hanno valori elevati di utilizzo della capacità delle performance
- In che modo la capacità di performance utilizzata per i nodi di una coppia ha sarà influenzata in caso di guasto di uno dei nodi
- I volumi e le LUN più impegnativi su un aggregato che ha un valore di utilizzo della capacità dalle performance elevate

Visualizzazione dei valori IOPS disponibili di nodo e aggregazione

È possibile monitorare i valori IOPS disponibili per tutti i nodi o per tutti gli aggregati di un cluster oppure visualizzare i dettagli di un singolo nodo o aggregato.

I valori IOPS disponibili vengono visualizzati nelle pagine Performance Inventory e nei grafici della pagina Performance Explorer per nodi e aggregati. Ad esempio, quando si visualizza un nodo nella pagina Node/Performance Explorer (Esplora nodi/prestazioni), è possibile selezionare il grafico del contatore “Available IOPS” (IOPS disponibili) dall’elenco in modo da poter confrontare i valori IOPS disponibili per il nodo e gli aggregati multipli su quel nodo.



Il monitoraggio del contatore IOPS disponibile consente di identificare:

- I nodi o gli aggregati che hanno i valori IOPS più elevati disponibili per determinare dove è possibile implementare i carichi di lavoro futuri.
- I nodi o gli aggregati che hanno i valori IOPS più piccoli disponibili per identificare le risorse da monitorare per potenziali problemi di performance futuri.
- I volumi e le LUN più impegnativi su un aggregato con un valore IOPS ridotto.

Visualizzazione dei grafici dei contatori di capacità delle performance per identificare i problemi

È possibile visualizzare i grafici relativi alla capacità di performance utilizzata per nodi e aggregati nella pagina Performance Explorer (Esplora prestazioni). In questo modo è possibile visualizzare dati dettagliati sulla capacità delle performance per i nodi e gli aggregati selezionati per un periodo di tempo specifico.

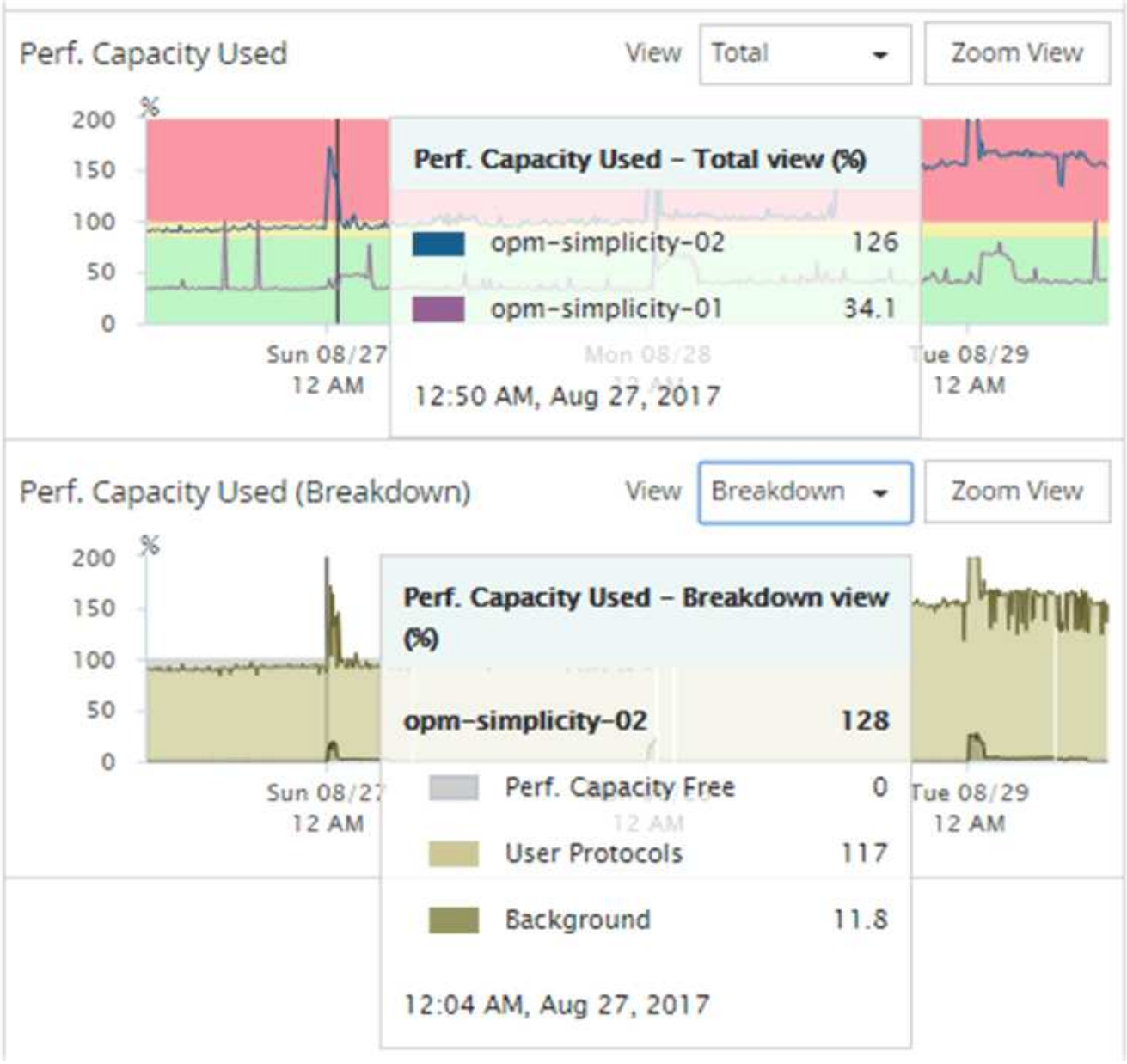
Il grafico standard del contatore visualizza i valori della capacità di performance utilizzata per i nodi o gli aggregati selezionati. Il grafico del contatore dei guasti visualizza i valori di capacità delle performance totali per l'oggetto root separati in base all'utilizzo in base ai protocolli utente rispetto ai processi di sistema in background. Inoltre, viene mostrata anche la quantità di capacità di performance libera.

Poiché alcune attività in background associate alla gestione del sistema e dei dati sono identificate come carichi di lavoro degli utenti e classificate come protocolli utente, la percentuale dei protocolli utente potrebbe apparire artificialmente elevata quando tali processi vengono eseguiti. In genere, questi processi vengono eseguiti intorno alla mezzanotte quando l'utilizzo del cluster è basso. Se si rileva un picco nell'attività del protocollo utente intorno alla mezzanotte, verificare se i processi di backup del cluster o altre attività in background sono configurati per l'esecuzione in quel momento.

Fasi

1. Selezionare la scheda **Explorer** da un nodo o da una pagina **Landing** aggregata.
2. Nel riquadro **Counter Chart**, fare clic su **Choose Chart**, quindi selezionare **Perf. Grafico della capacità utilizzata**.
3. Scorrere verso il basso fino a visualizzare la mappa.

   I colori del grafico standard mostrano quando l'oggetto si trova nell'intervallo ottimale (giallo), quando l'oggetto è sottoutilizzato (verde) e quando l'oggetto è sovrautilizzato (rosso). Il grafico dettagliato mostra i dettagli della capacità delle performance solo per l'oggetto root.



4. Se si desidera visualizzare uno dei grafici in un formato a dimensione intera, fare clic su **Zoom View** (Vista zoom).

   In questo modo è possibile aprire più diagrammi di contatore in una finestra separata per confrontare i valori di capacità delle performance utilizzati con i valori IOPS o Mbps nello stesso intervallo di tempo.

La capacità di performance ha utilizzato le condizioni di soglia delle performance

È possibile creare criteri di soglia delle performance definiti dall'utente in modo che gli eventi vengano attivati quando il valore della capacità di performance utilizzata per un nodo o aggregato supera l'impostazione di soglia definita per la capacità di performance utilizzata.

Inoltre, i nodi possono essere configurati con un criterio di soglia "Performance Capacity used Takeover". Questo criterio di soglia totalizza la capacità di performance utilizzata dalle statistiche per entrambi i nodi di una coppia ha per determinare se uno dei due nodi non dispone di capacità sufficiente in caso di guasto

dell'altro nodo. Poiché il carico di lavoro durante il failover è la combinazione dei carichi di lavoro dei due nodi partner`, la stessa capacità di performance utilizzata per la policy di takeover può essere applicata a entrambi i nodi.

> Questa equivalenza di capacità di performance utilizzata è generalmente vera tra i nodi. Tuttavia, se il traffico tra nodi è significativamente maggiore per uno dei nodi attraverso il partner di failover, la capacità di performance totale utilizzata per l'esecuzione di tutti i carichi di lavoro su un nodo partner rispetto all'altro nodo partner potrebbe essere leggermente diversa a seconda del nodo guasto.

Le condizioni di utilizzo della capacità di performance possono anche essere utilizzate come impostazioni di soglia delle performance secondarie per creare una policy di soglia combinata quando si definiscono le soglie per LUN e volumi. La condizione di capacità di performance utilizzata viene applicata all'aggregato o al nodo su cui risiede il volume o il LUN. Ad esempio, è possibile creare una combinazione di criteri di soglia utilizzando i seguenti criteri:

Oggetto di storage	Contatore delle performance	Soglia di avviso	Soglia critica	Durata
Volume	Latenza	15 ms/op	25 ms/op	20 minuti
Aggregato	Capacità di performance utilizzata	80%	95%	

I criteri di soglia combinati causano la generazione di un evento solo quando entrambe le condizioni vengono violate per l'intera durata.

Utilizzo della capacità di performance utilizzata per gestire le performance

In genere, le organizzazioni desiderano operare con una percentuale di capacità utilizzata per le performance inferiore a 100, in modo che le risorse vengano utilizzate in modo efficiente, riservando al tempo stesso una capacità di performance aggiuntiva per supportare le richieste di periodi di picco. È possibile utilizzare i criteri di soglia per personalizzare l'invio di avvisi per i valori di capacità utilizzata dalle performance elevate.

Puoi stabilire obiettivi specifici in base ai tuoi requisiti di performance. Ad esempio, le società di servizi finanziari potrebbero riservare una maggiore capacità di performance per garantire la tempestiva esecuzione delle negoziazioni. Queste aziende potrebbero voler impostare le soglie di utilizzo della capacità di performance nell'intervallo del 70-80%. Le aziende manifatturiere con margini inferiori potrebbero scegliere di riservare una capacità di performance inferiore se sono disposte a rischiare le performance per gestire meglio i costi IT. Queste aziende potrebbero impostare le soglie di utilizzo della capacità di performance nell'intervallo del 85-95%.

Quando il valore della capacità di performance utilizzata supera la percentuale impostata in un criterio di soglia definito dall'utente, Unified Manager invia un'email di avviso e aggiunge l'evento alla pagina Event Inventory. Ciò consente di gestire i potenziali problemi prima che influiscano sulle performance. Questi eventi possono anche essere utilizzati come indicatori necessari per spostare i carichi di lavoro e apportare modifiche all'interno dei nodi e degli aggregati.

Informazioni e utilizzo della pagina Node failover Planning (Pianificazione del failover del nodo)

La pagina Performance/Node failover Planning (Pianificazione delle performance/failover dei nodi) stima l'impatto delle performance su un nodo in caso di guasto del nodo partner ad alta disponibilità (ha) del nodo. Unified Manager basa le stime sulle performance storiche dei nodi nella coppia ha.

La stima dell'impatto delle performance di un failover consente di pianificare i seguenti scenari:

- Se un failover riduce costantemente le performance stimate del nodo di Takeover a un livello inaccettabile, è possibile prendere in considerazione azioni correttive per ridurre l'impatto delle performance dovuto a un failover.
- Prima di avviare un failover manuale per eseguire attività di manutenzione dell'hardware, è possibile stimare il modo in cui il failover influisce sulle prestazioni del nodo di Takeover per determinare il momento migliore per eseguire l'attività.

Utilizzo della pagina Node failover Planning (Pianificazione del failover del nodo) per determinare le azioni correttive

In base alle informazioni visualizzate nella pagina Performance/Node failover Planning (Pianificazione delle performance/failover dei nodi), è possibile intraprendere azioni per garantire che un failover non causi un calo delle performance di una coppia ha al di sotto di un livello accettabile.

Ad esempio, per ridurre l'impatto stimato sulle performance di un failover, è possibile spostare alcuni volumi o LUN da un nodo della coppia ha ad altri nodi del cluster. In questo modo si garantisce che il nodo primario possa continuare a offrire performance accettabili dopo un failover.

Componenti della pagina Node failover Planning (Pianificazione del failover del nodo)

I componenti della pagina Performance/Node failover Planning (Pianificazione del failover delle prestazioni/nodo) vengono visualizzati in una griglia e nel riquadro di confronto. Queste sezioni consentono di valutare l'impatto del failover di un nodo sulle prestazioni del nodo di Takeover.

Griglia delle statistiche delle performance

La pagina Performance/Node failover Planning (Pianificazione del failover delle performance/nodi) visualizza una griglia contenente le statistiche relative a latenza, IOPS, utilizzo e capacità delle performance utilizzate.

> I valori di latenza e IOPS visualizzati in questa pagina e nella pagina Esplora performance/Node Performance potrebbero non corrispondere perché vengono utilizzati contatori di performance diversi per calcolare i valori per prevedere il failover del nodo.

Nella griglia, a ciascun nodo viene assegnato uno dei seguenti ruoli:

- Primario

Nodo che assume il controllo del partner ha in caso di guasto del partner. L'oggetto root è sempre il nodo Primary.

- Partner

  Il nodo che si guasta nello scenario di failover.

- Takeover stimato

  Uguale al nodo primario. Le statistiche delle performance visualizzate per questo nodo mostrano le performance del nodo Takeover dopo che ha preso il controllo del partner guasto.

> Sebbene il carico di lavoro del nodo di Takeover sia equivalente ai carichi di lavoro combinati di entrambi i nodi dopo un failover, le statistiche per il nodo di Takeover stimato non sono la somma delle statistiche del nodo primario e del nodo Partner. Ad esempio, se la latenza del nodo primario è di 2 ms/op e la latenza del nodo Partner è di 3 ms/op, il nodo Takeover stimato potrebbe avere una latenza di 4 ms/op. Questo valore è un calcolo eseguito da Unified Manager.

È possibile fare clic sul nome del nodo Partner se si desidera che diventi l'oggetto root. Una volta visualizzata la pagina Explorer performance/Node Performance, fare clic sulla scheda **failover Planning** (Pianificazione failover) per vedere come cambiano le performance in questo scenario di guasto del nodo. Ad esempio, se Node1 è il nodo primario e Node2 è il nodo Partner, è possibile fare clic su Node2 per renderlo il nodo primario. In questo modo, è possibile vedere come cambiano le performance stimate in base al nodo che si guasta.

Pannello di confronto

Il seguente elenco descrive i componenti visualizzati nel riquadro di confronto per impostazione predefinita:

- **Grafici degli eventi**

  Vengono visualizzati nello stesso formato della pagina Esplora prestazioni/prestazioni nodo. Riguardano solo il nodo primario.

- **Counter chart**

  Vengono visualizzate le statistiche cronologiche del contatore delle performance mostrato nella griglia. In ciascun grafico, il grafico del nodo Estimated Takeover mostra le performance stimate se si è verificato un failover in un dato momento.

  Si supponga, ad esempio, che il grafico di utilizzo indichi il 73% per il nodo Estimated Takeover alle ore 11 L'8 febbraio. Se in quel momento si fosse verificato un failover, l'utilizzo del nodo di Takeover sarebbe stato del 73%.

  Le statistiche cronologiche consentono di individuare il tempo ottimale per l'avvio di un failover, riducendo al minimo la possibilità di sovraccaricare il nodo di Takeover. È possibile pianificare un failover solo quando le prestazioni previste del nodo di Takeover sono accettabili.

Per impostazione predefinita, le statistiche dell'oggetto root e del nodo partner vengono visualizzate nel riquadro di confronto. A differenza della pagina Explorer performance/Node Performance, in questa pagina non viene visualizzato il pulsante **Add** per aggiungere oggetti per il confronto delle statistiche.

È possibile personalizzare il pannello di confronto nello stesso modo in cui si utilizza la pagina Esplora

prestazioni/prestazioni nodo. L'elenco seguente mostra alcuni esempi di personalizzazione dei grafici:

- Fare clic sul nome di un nodo per visualizzare o nascondere le statistiche del nodo nei grafici contatore.
- Fare clic su **Zoom View** (Visualizza zoom) per visualizzare un grafico dettagliato di un determinato contatore in una nuova finestra.

Utilizzo di un criterio di soglia con la pagina Node failover Planning (Pianificazione del failover del nodo)

È possibile creare un criterio di soglia del nodo in modo da ricevere una notifica nella pagina Performance/Node failover Planning (Pianificazione delle performance/failover del nodo) quando un potenziale failover degraderebbe le prestazioni del nodo di Takeover a un livello inaccettabile.

La policy di soglia delle performance definita dal sistema, denominata "Node ha Pair over-utilizzed", genera un evento di avviso se la soglia viene violata per sei periodi di raccolta consecutivi (30 minuti). La soglia viene considerata violata se la capacità di performance combinata utilizzata dai nodi in una coppia ha supera il 200%.

L'evento del criterio di soglia definito dal sistema avvisa l'utente del fatto che un failover causa un aumento della latenza del nodo di Takeover a un livello inaccettabile. Quando viene visualizzato un evento generato da questo criterio per un nodo specifico, è possibile accedere alla pagina Performance/Node failover Planning per quel nodo per visualizzare il valore di latenza previsto dovuto a un failover.

Oltre a utilizzare questo criterio di soglia definito dal sistema, è possibile creare criteri di soglia utilizzando il contatore "Performance Capacity Used - Takeover", quindi applicare il criterio ai nodi selezionati. La specifica di una soglia inferiore al 200% consente di ricevere un evento prima che venga violata la soglia per la policy definita dal sistema. È inoltre possibile specificare il periodo di tempo minimo per il quale la soglia viene superata, inferiore a 30 minuti, se si desidera ricevere una notifica prima che venga generato l'evento di policy definito dal sistema.

Ad esempio, è possibile definire un criterio di soglia per generare un evento di avviso se la capacità di performance combinata utilizzata dai nodi in una coppia ha supera il 175% per più di 10 minuti. È possibile applicare questo criterio a Node1 e Node2, che formano una coppia ha. Dopo aver ricevuto una notifica di evento di avviso per Node1 o Node2, è possibile visualizzare la pagina Performance/Node failover Planning per quel nodo per valutare l'impatto stimato delle performance sul nodo di Takeover. È possibile intraprendere azioni correttive per evitare di sovraccaricare il nodo di Takeover in caso di failover. Se si interviene quando la capacità di performance combinata utilizzata dai nodi è inferiore al 200%, la latenza del nodo di Takeover non raggiunge un livello inaccettabile anche se si verifica un failover durante questo periodo di tempo.

Utilizzo del grafico di dettaglio Performance Capacity Used per la pianificazione del failover

Il grafico dettagliato della capacità di performance utilizzata - ripartizione mostra la capacità di performance utilizzata per il nodo primario e il nodo partner. Mostra inoltre la quantità di capacità di performance libera sul nodo Estimated Takeover. Queste informazioni consentono di determinare se si potrebbero verificare problemi di performance in caso di guasto del nodo partner.

Oltre a mostrare la capacità di performance totale utilizzata per i nodi, il grafico di ripartizione suddivide i valori per ciascun nodo in protocolli utente e processi in background.

- I protocolli utente sono le operazioni di i/o dalle applicazioni utente al e dal cluster.
- I processi in background sono i processi interni del sistema coinvolti nell'efficienza dello storage, nella replica dei dati e nello stato di salute del sistema.

Questo livello di dettaglio aggiuntivo consente di determinare se un problema di performance è causato dall'attività dell'applicazione dell'utente o dai processi di sistema in background, come deduplica, ricostruzione RAID, scrubbing del disco e copie SnapMirror.

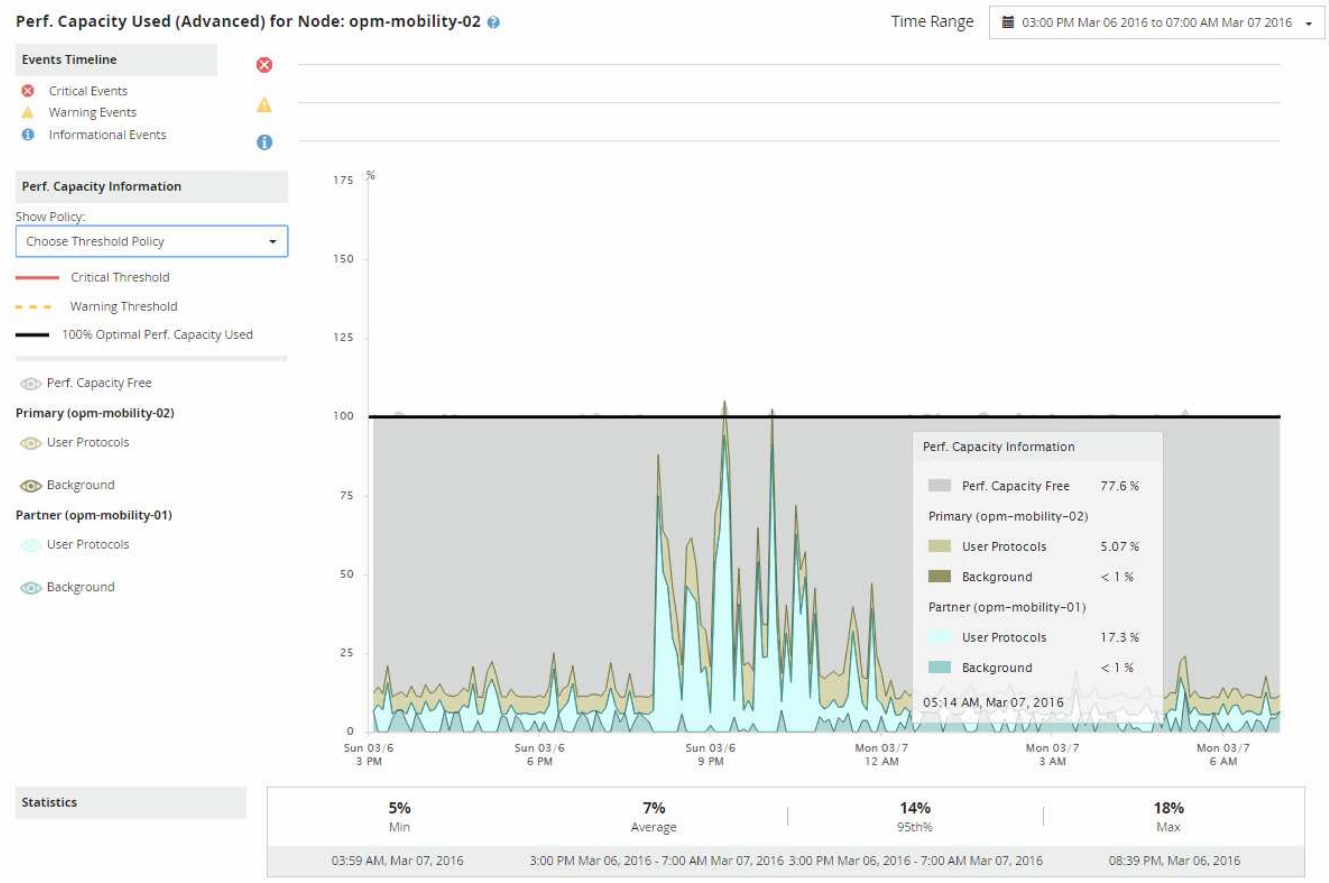
Fasi

1. Accedere alla pagina **Performance/Node failover Planning** del nodo che fungerà da nodo Estimated Takeover.
2. Dal selettore **intervallo di tempo**, scegliere il periodo di tempo per il quale le statistiche storiche vengono visualizzate nella griglia del contatore e nei grafici dei contatori.

   Vengono visualizzati i grafici dei contatori con le statistiche per il nodo primario, il nodo partner e il nodo Takeover stimato.

3. Dall'elenco **Scegli grafici**, selezionare **Perf. Capacità utilizzata**.
4. Nel campo **Perf. Grafico capacità utilizzata**, selezionare **dettaglio** e fare clic su **Vista zoom**.

   Il grafico dettagliato per Perf. Viene visualizzato Capacity used (capacità utilizzata).



5. Spostare il cursore sul grafico dettagliato per visualizzare le informazioni sulla capacità di performance utilizzata nella finestra a comparsa.

   Il Perf. La percentuale di Capacity Free è la capacità di performance disponibile sul nodo Estimated Takeover. Indica la capacità di performance rimasta nel nodo di Takeover dopo un failover. Se è pari a 0%,

un failover causerà un aumento della latenza a un livello inaccettabile sul nodo di Takeover.

6. Prendere in considerazione azioni correttive per evitare una percentuale di capacità senza capacità a basse performance.

   Se si prevede di avviare un failover per la manutenzione del nodo, scegliere un periodo di tempo in cui il nodo partner non riesce quando la percentuale di capacità libera dalle performance non è pari a 0.

Raccolta di dati e monitoraggio delle performance dei carichi di lavoro

Unified Manager raccoglie e analizza l'attività dei carichi di lavoro ogni 5 minuti per identificare gli eventi relativi alle performance e rileva le modifiche alla configurazione ogni 15 minuti. Conserva un massimo di 30 giorni di dati storici relativi alle performance e agli eventi di 5 minuti e utilizza questi dati per prevedere l'intervallo di latenza previsto per tutti i carichi di lavoro monitorati.

Unified Manager deve raccogliere un minimo di 3 giorni di attività del carico di lavoro prima che possa iniziare l'analisi e prima che la previsione di latenza per il tempo di risposta i/o possa essere visualizzata nella pagina workload Analysis e nella pagina Event Details. Durante la raccolta di questa attività, la previsione della latenza non visualizza tutte le modifiche che si verificano dall'attività del carico di lavoro. Dopo aver raccolto 3 giorni di attività, Unified Manager regola la previsione di latenza ogni 24 ore alle 12:00, per riflettere le modifiche dell'attività del carico di lavoro e stabilire una soglia di performance dinamica più precisa.

Durante i primi 4 giorni in cui Unified Manager sta monitorando un carico di lavoro, se sono trascorse più di 24 ore dall'ultima raccolta di dati, i grafici di latenza non visualizzano la previsione di latenza per quel carico di lavoro. Gli eventi rilevati prima dell'ultima raccolta sono ancora disponibili.

> L'ora legale (DST) modifica l'ora del sistema, che modifica la previsione di latenza delle statistiche delle performance per i carichi di lavoro monitorati. Unified Manager inizia immediatamente a correggere la previsione di latenza, che richiede circa 15 giorni per essere completata. Durante questo periodo di tempo è possibile continuare a utilizzare Unified Manager, ma poiché Unified Manager utilizza la previsione della latenza per rilevare eventi dinamici, alcuni eventi potrebbero non essere precisi. Gli eventi rilevati prima del cambiamento di orario non vengono influenzati.

Tipi di workload monitorati da Unified Manager

È possibile utilizzare Unified Manager per monitorare le performance di due tipi di carichi di lavoro: Definiti dall'utente e definiti dal sistema.

- ***workload definiti dall'utente***

  Il throughput di i/o dalle applicazioni al cluster. Si tratta di processi coinvolti nelle richieste di lettura e scrittura. Un volume, LUN, condivisione NFS, condivisione SMB/CIFS e un carico di lavoro è un carico di lavoro definito dall'utente.

  > Unified Manager monitora solo l'attività del carico di lavoro sul cluster. Non esegue il monitoraggio delle applicazioni, dei client o dei percorsi tra le applicazioni e il cluster.

Se una o più delle seguenti affermazioni relative a un carico di lavoro sono vere, non possono essere monitorate da Unified Manager:

  - Si tratta di una copia di protezione dei dati (DP) in modalità di sola lettura. (I volumi DP vengono monitorati per il traffico generato dall'utente).
  - Si tratta di un clone dei dati offline.
  - Si tratta di un volume mirrorato in una configurazione MetroCluster.

- ***workload definiti dal sistema***

  I processi interni legati all'efficienza dello storage, alla replica dei dati e allo stato del sistema, tra cui:

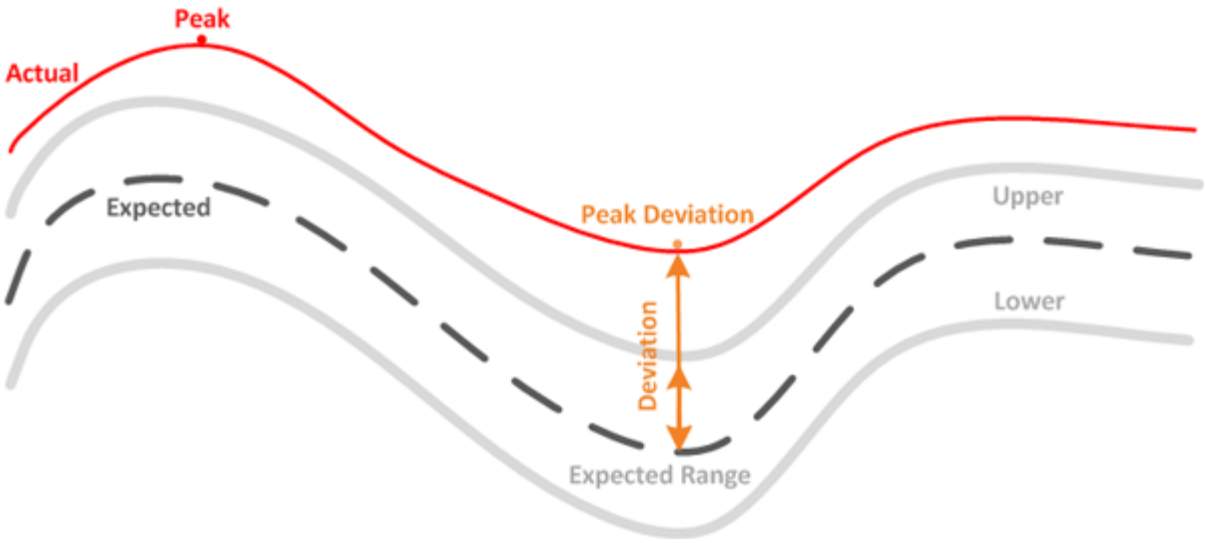
  - Efficienza dello storage, come la deduplica
  - Integrità del disco, che include la ricostruzione RAID, lo scrubbing del disco e così via
  - Replica dei dati, ad esempio le copie SnapMirror
  - Attività di gestione
  - Integrità del file system, che include varie attività di WAFL
  - Scanner del file system, come ad esempio la scansione WAFL
  - Offload delle copie, ad esempio operazioni di efficienza dello storage offload da host VMware
  - Stato del sistema, ad esempio spostamenti di volumi, compressione dei dati e così via
  - Volumi non monitorati

I dati sulle performance per i carichi di lavoro definiti dal sistema vengono visualizzati nella GUI solo quando il componente del cluster utilizzato da questi carichi di lavoro è in conflitto. Ad esempio, non è possibile cercare il nome di un carico di lavoro definito dal sistema per visualizzarne i dati sulle prestazioni nella GUI.

Valori di misurazione delle performance del carico di lavoro

Unified Manager misura le performance dei carichi di lavoro su un cluster in base a valori statistici storici e previsti, che formano la previsione di latenza dei valori per i carichi di lavoro. Confronta i valori statistici effettivi del carico di lavoro con la previsione di latenza per determinare quando le performance del carico di lavoro sono troppo alte o troppo basse. Un carico di lavoro che non funziona come previsto attiva un evento di performance dinamica per la notifica.

Nella seguente illustrazione, il valore effettivo, in rosso, rappresenta le statistiche effettive delle performance nel periodo di tempo. Il valore effettivo ha superato la soglia di performance, che è il limite superiore della previsione di latenza. Il picco è il valore effettivo più alto nell'intervallo di tempo. La deviazione misura la variazione tra i valori previsti (la previsione) e i valori effettivi, mentre la deviazione di picco indica la variazione maggiore tra i valori attesi e quelli effettivi.



La seguente tabella elenca i valori di misurazione delle performance del carico di lavoro.

Misurazione	Descrizione
Attività	La percentuale del limite di QoS utilizzato dai carichi di lavoro nel gruppo di criteri. Se Unified Manager rileva una modifica a un gruppo di criteri, ad esempio l'aggiunta o la rimozione di un volume o la modifica del limite di QoS, i valori effettivi e previsti potrebbero superare il 100% del limite impostato. Se un valore supera il 100% del limite impostato, viene visualizzato come >100%. Se un valore è inferiore all'1% del limite impostato, viene visualizzato come <1%.
Effettivo	Il valore misurato delle performance in un momento specifico per un determinato carico di lavoro.
Deviazione	Il cambiamento tra i valori previsti e quelli effettivi. Si tratta del rapporto tra il valore effettivo meno il valore previsto e il valore superiore dell'intervallo previsto meno il valore previsto. Un valore di deviazione negativo indica che le performance del carico di lavoro sono inferiori al previsto, mentre un valore di deviazione positivo indica che le performance del carico di lavoro sono superiori al previsto.

Misurazione	Descrizione
Previsto	I valori previsti si basano sull'analisi dei dati storici delle performance per un determinato carico di lavoro. Unified Manager analizza questi valori statistici per determinare l'intervallo previsto (previsione di latenza) dei valori.
Previsione di latenza (intervallo previsto)	La previsione di latenza è una previsione dei valori di performance superiori e inferiori previsti in un momento specifico. Per la latenza del carico di lavoro, i valori superiori costituiscono la soglia di performance. Quando il valore effettivo supera la soglia di performance, Unified Manager attiva un evento di performance dinamico.
Picco	Il valore massimo misurato in un periodo di tempo.
Deviazione di picco	Il valore di deviazione massimo misurato in un periodo di tempo.
Profondità della coda	Il numero di richieste i/o in sospeso che sono in attesa sul componente di interconnessione.
Utilizzo	Per l'elaborazione di rete, l'elaborazione dei dati e i componenti aggregati, la percentuale di tempo occupato per completare le operazioni dei carichi di lavoro in un determinato periodo di tempo. Ad esempio, la percentuale di tempo in cui i componenti di elaborazione dati o di elaborazione di rete elaborano una richiesta di i/o o un aggregato deve soddisfare una richiesta di lettura o scrittura.
Throughput in scrittura	La quantità di throughput in scrittura, espressa in megabyte al secondo (MB/s), dai carichi di lavoro su un cluster locale al cluster partner in una configurazione MetroCluster.

Qual è la gamma di performance prevista

La previsione di latenza è una previsione dei valori di performance superiori e inferiori previsti in un momento specifico. Per la latenza del carico di lavoro, i valori superiori costituiscono la soglia di performance. Quando il valore effettivo supera la soglia di performance, Unified Manager attiva un evento di performance dinamico.

Ad esempio, durante le normali ore di lavoro tra le 9:00 e alle 17:00, la maggior parte dei dipendenti potrebbe controllare la posta elettronica tra le 9:00 e alle 10:30 L'aumento della domanda sui server di posta elettronica comporta un aumento dell'attività dei carichi di lavoro sullo storage back-end durante questo periodo. I dipendenti potrebbero notare tempi di risposta lenti dai propri client di posta elettronica.

Durante l'ora di pranzo tra le 12:00 e alle 13:00 e alla fine della giornata lavorativa dopo le 17:00, la maggior parte dei dipendenti è probabilmente lontana dai computer. La domanda sui server di posta elettronica in genere diminuisce, diminuendo anche la domanda sullo storage back-end. In alternativa, potrebbero essere pianificate operazioni di carico di lavoro, come backup dello storage o scansione virus, che iniziano dopo le 17:00 e aumentare l'attività sullo storage back-end.

Nel corso di diversi giorni, l'aumento e la diminuzione dell'attività del carico di lavoro determina l'intervallo previsto (previsione di latenza) dell'attività, con limiti superiori e inferiori per un carico di lavoro. Quando l'attività effettiva del carico di lavoro di un oggetto si trova al di fuori dei limiti superiori o inferiori e rimane al di fuori dei limiti per un certo periodo di tempo, ciò potrebbe indicare che l'oggetto è stato utilizzato in eccesso o sottoutilizzato.

Come si forma la previsione di latenza

Unified Manager deve raccogliere un minimo di 3 giorni di attività del carico di lavoro prima che possa iniziare l'analisi e prima che la previsione di latenza per il tempo di risposta i/o possa essere visualizzata nella GUI. La raccolta dati minima richiesta non tiene conto di tutte le modifiche che si verificano dall'attività del carico di lavoro. Dopo aver raccolto i primi 3 giorni di attività, Unified Manager regola la previsione di latenza ogni 24 ore alle 12:00 riflettere le modifiche dell'attività del carico di lavoro e stabilire una soglia di performance dinamica più precisa.

L'ora legale (DST) modifica l'ora del sistema, che modifica la previsione di latenza delle statistiche delle performance per i carichi di lavoro monitorati. Unified Manager inizia immediatamente a correggere la previsione di latenza, che richiede circa 15 giorni per essere completata. Durante questo periodo di tempo è possibile continuare a utilizzare Unified Manager, ma poiché Unified Manager utilizza la previsione della latenza per rilevare eventi dinamici, alcuni eventi potrebbero non essere precisi. Gli eventi rilevati prima del cambiamento di orario non vengono influenzati.

Come viene utilizzata la previsione di latenza nell'analisi delle performance

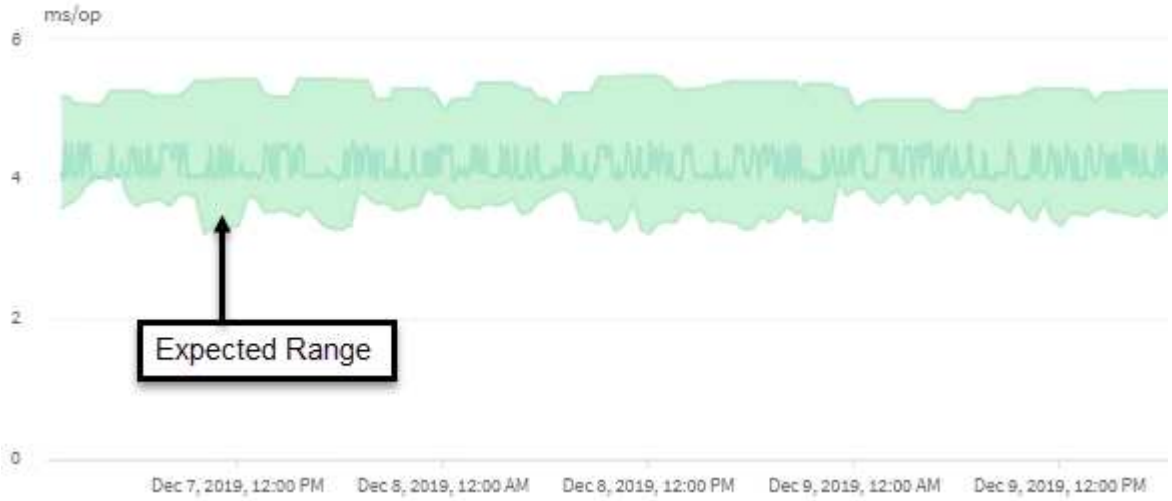
Unified Manager utilizza la previsione della latenza per rappresentare la tipica attività di latenza i/o (tempo di risposta) per i carichi di lavoro monitorati. Ti avvisa quando la latenza effettiva per un carico di lavoro supera i limiti superiori della previsione di latenza, che attiva un evento di performance dinamica, in modo da poter analizzare il problema delle performance e intraprendere azioni correttive per risolverlo.

La previsione della latenza definisce la linea di base delle performance per il carico di lavoro. Nel corso del tempo, Unified Manager apprende dalle precedenti misurazioni delle performance per prevedere i livelli di performance e attività previsti per il carico di lavoro. Il limite superiore dell'intervallo previsto stabilisce la soglia di performance dinamica. Unified Manager utilizza la linea di base per determinare quando la latenza effettiva è superiore o inferiore a una soglia o al di fuori dei limiti previsti. Il confronto tra i valori effettivi e quelli previsti crea un profilo di performance per il carico di lavoro.

Quando la latenza effettiva per un carico di lavoro supera la soglia di performance dinamica, a causa di un conflitto su un componente del cluster, la latenza è elevata e il carico di lavoro funziona più lentamente del previsto. Anche le performance di altri carichi di lavoro che condividono gli stessi componenti del cluster potrebbero essere più lente del previsto.

Unified Manager analizza l'evento di superamento della soglia e determina se l'attività è un evento di performance. Se l'elevata attività del carico di lavoro rimane costante per un lungo periodo di tempo, ad esempio diverse ore, Unified Manager considera l'attività normale e regola dinamicamente la previsione di latenza per formare la nuova soglia di performance dinamica.

Alcuni carichi di lavoro potrebbero avere un'attività costantemente bassa, dove la previsione di latenza per la latenza non ha un elevato tasso di cambiamento nel tempo. Per ridurre al minimo il numero di eventi durante l'analisi degli eventi delle performance, Unified Manager attiva un evento solo per volumi a bassa attività le cui operazioni e latenze sono molto più elevate del previsto.



In questo esempio, la latenza per un volume ha una previsione di latenza, in grigio, di 3.5 millisecondi per operazione (ms/op) al minimo e di 5.5 ms/op al massimo. Se la latenza effettiva, in blu, aumenta improvvisamente a 10 ms/op, a causa di un picco intermittente nel traffico di rete o di un conflitto su un componente del cluster, supera la previsione di latenza e supera la soglia di performance dinamica.

Quando il traffico di rete è diminuito o il componente del cluster non è più in conflitto, la latenza ritorna entro la previsione di latenza. Se la latenza rimane pari o superiore a 10 ms/op per un lungo periodo di tempo, potrebbe essere necessario intraprendere un'azione correttiva per risolvere l'evento.

Come Unified Manager utilizza la latenza dei workload per identificare i problemi di performance

La latenza del carico di lavoro (tempo di risposta) è il tempo necessario a un volume di un cluster per rispondere alle richieste di i/o provenienti dalle applicazioni client. Unified Manager utilizza la latenza per rilevare e avvisare gli utenti in caso di eventi relativi alle performance.

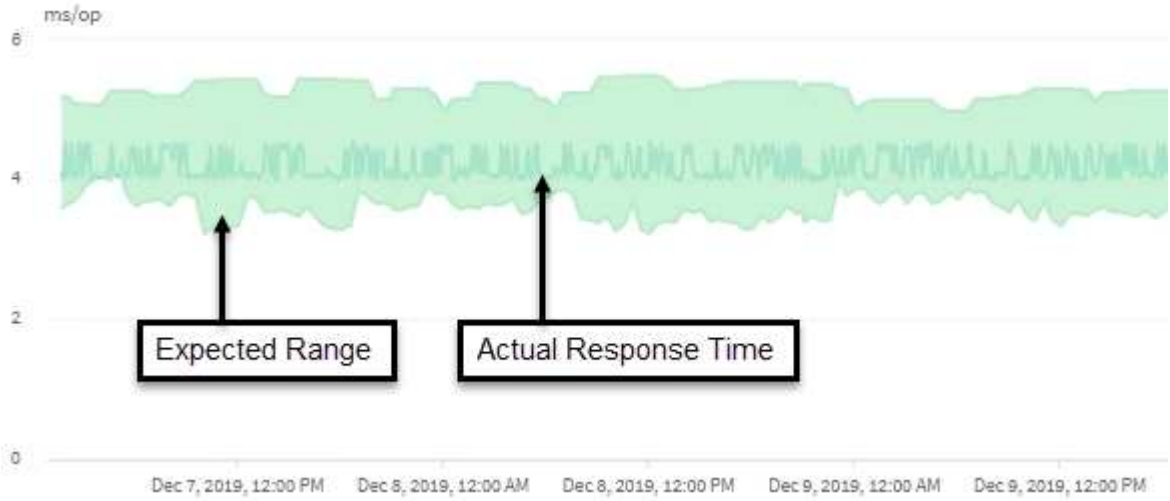
Un'elevata latenza significa che le richieste dalle applicazioni a un volume su un cluster richiedono più tempo del solito. La causa dell'elevata latenza potrebbe essere il cluster stesso, a causa di conflitti su uno o più componenti del cluster. L'elevata latenza potrebbe essere causata anche da problemi esterni al cluster, come colli di bottiglia della rete, problemi con il client che ospita le applicazioni o problemi con le applicazioni stesse.

Unified Manager monitora solo l'attività del carico di lavoro sul cluster. Non esegue il monitoraggio delle applicazioni, dei client o dei percorsi tra le applicazioni e il cluster.

Anche le operazioni sul cluster, come la creazione di backup o l'esecuzione della deduplica, che aumentano la domanda di componenti del cluster condivisi da altri carichi di lavoro possono contribuire a un'elevata latenza. Se la latenza effettiva supera la soglia di performance dinamica dell'intervallo previsto (previsione di latenza), Unified Manager analizza l'evento per determinare se si tratta di un evento di performance che potrebbe essere necessario risolvere. La latenza viene misurata in millisecondi per operazione (ms/op).

Nel grafico latenza totale della pagina analisi del carico di lavoro, è possibile visualizzare un'analisi delle

statistiche di latenza per vedere come l'attività dei singoli processi, come le richieste di lettura e scrittura, si confronta con le statistiche di latenza complessive. Il confronto consente di determinare quali operazioni hanno l'attività più elevata o se operazioni specifiche hanno attività anomale che influiscono sulla latenza di un volume. Quando si analizzano gli eventi delle performance, è possibile utilizzare le statistiche di latenza per determinare se un evento è stato causato da un problema nel cluster. È inoltre possibile identificare le attività specifiche del carico di lavoro o i componenti del cluster coinvolti nell'evento.



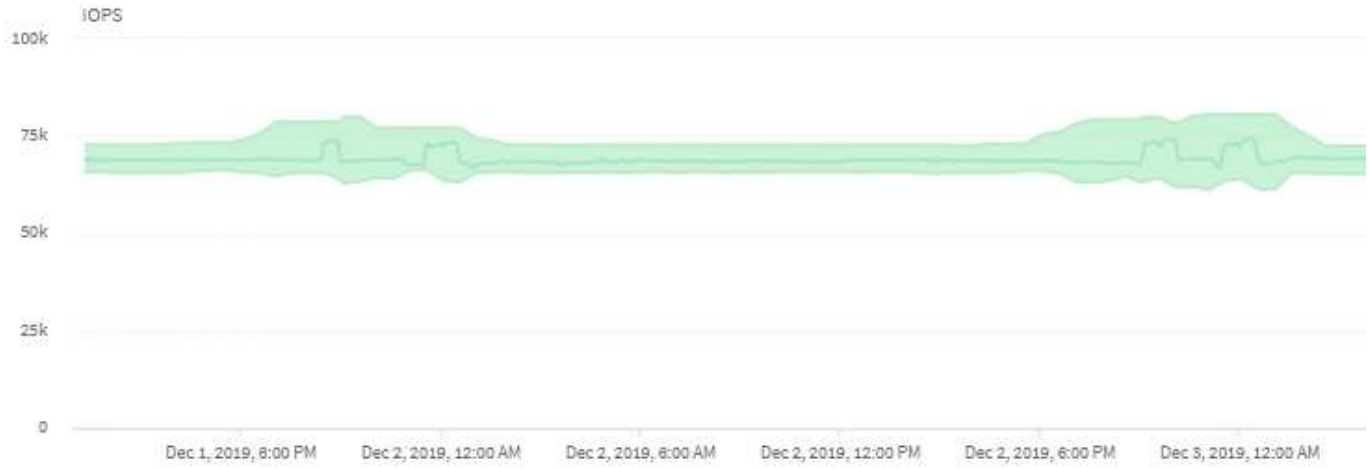
Questo esempio mostra il grafico della latenza . L'attività del tempo di risposta effettivo (latenza) è una linea blu e la previsione di latenza (intervallo previsto) è verde.

Se Unified Manager non è in grado di raccogliere i dati, la linea blu può presentare delle lacune. Ciò può verificarsi perché il cluster o il volume non era raggiungibile, Unified Manager è stato disattivato durante tale periodo o la raccolta richiede più tempo del periodo di raccolta di 5 minuti.

In che modo le operazioni del cluster possono influire sulla latenza del carico di lavoro

Le operazioni (IOPS) rappresentano l'attività di tutti i carichi di lavoro definiti dall'utente e dal sistema su un cluster. Le statistiche IOPS consentono di determinare se i processi del cluster, come l'esecuzione di backup o la deduplica, influiscono sulla latenza del carico di lavoro (tempo di risposta) o potrebbero aver causato o contribuito a un evento di performance.

Quando si analizzano gli eventi relativi alle performance, è possibile utilizzare le statistiche IOPS per determinare se un evento relativo alle performance è stato causato da un problema nel cluster. È possibile identificare le attività specifiche dei carichi di lavoro che potrebbero aver contribuito in maniera determinante all'evento delle performance. Gli IOPS vengono misurati in operazioni al secondo (Ops/sec).



Questo esempio mostra il grafico IOPS. Le statistiche effettive delle operazioni sono una linea blu e le previsioni IOPS delle statistiche delle operazioni sono verdi.

In alcuni casi in cui un cluster è sovraccarico, Unified Manager potrebbe visualizzare il messaggio `Data collection is taking too long on Cluster cluster_name`. Ciò significa che non sono state raccolte statistiche sufficienti per l'analisi di Unified Manager. È necessario ridurre le risorse utilizzate dal cluster in modo da poter raccogliere le statistiche.

Monitoraggio delle performance delle configurazioni MetroCluster

Unified Manager consente di monitorare il throughput di scrittura tra i cluster in una configurazione MetroCluster per identificare i carichi di lavoro con un'elevata quantità di throughput in scrittura.

Se questi carichi di lavoro dalle performance elevate causano elevati tempi di risposta i/o per altri volumi nel cluster locale, Unified Manager attiva gli eventi relativi alle performance per ricevere una notifica.

Unified Manager tratta i cluster in una configurazione MetroCluster come singoli cluster. Non distingue i cluster che sono partner o correlano il throughput di scrittura da ciascun cluster.

Quando un cluster locale in una configurazione MetroCluster esegue il mirroring dei dati nel cluster partner, i dati vengono scritti nella NVRAM e quindi trasferiti attraverso i collegamenti interswitch (ISL) agli aggregati remoti. Unified Manager analizza la NVRAM per identificare i carichi di lavoro il cui throughput di scrittura elevato sta utilizzando la NVRAM in eccesso, mettendo la NVRAM in conflitto.

I carichi di lavoro la cui deviazione nel tempo di risposta ha superato la soglia di performance sono denominati *vittime* e i carichi di lavoro la cui deviazione nel throughput di scrittura nella NVRAM è superiore al solito, causando il conflitto, sono denominati *bullies*. Poiché solo le richieste di scrittura vengono mirrorate al cluster partner, Unified Manager non analizza il throughput in lettura.

È possibile visualizzare il throughput di qualsiasi cluster in una configurazione MetroCluster analizzando i carichi di lavoro dei LUN e dei volumi corrispondenti dalle seguenti schermate. È possibile filtrare i risultati in base al cluster. Dal riquadro di navigazione di sinistra:

- Vista **Storage > Clusters > Performance: Tutti i Clusters**. Vedere
- Vista **Storage > Volumes > Performance: All Volumes**.

- **Storage > LUN > Performance: Vista di tutte le LUN**.
- **Analisi del carico di lavoro > tutti i carichi di lavoro**

Informazioni correlate

"Analisi e notifica degli eventi relativi alle performance"

"Analisi degli eventi di performance per una configurazione MetroCluster"

"Ruoli dei carichi di lavoro coinvolti in un evento di performance"

"Identificazione dei carichi di lavoro delle vittime coinvolti in un evento di performance"

"Identificazione dei carichi di lavoro ingombranti coinvolti in un evento di performance"

"Identificazione dei carichi di lavoro di Shark coinvolti in un evento di performance"

Informazioni su eventi e avvisi relativi alle performance

Gli eventi relativi alle performance sono incidenti legati alle performance dei carichi di lavoro su un cluster. Ti aiutano a identificare i carichi di lavoro con tempi di risposta lenti. Insieme agli eventi di salute che si sono verificati contemporaneamente, è possibile determinare i problemi che potrebbero aver causato o contribuito a ridurre i tempi di risposta.

Quando Unified Manager rileva più occorrenze della stessa condizione di evento per lo stesso componente del cluster, considera tutte le ricorrenze come un singolo evento, non come eventi separati.

È possibile configurare gli avvisi in modo che inviino automaticamente una notifica via email quando si verificano eventi di performance di determinati tipi di severità.

Fonti di eventi relativi alle performance

Gli eventi relativi alle performance sono problemi legati alle performance dei carichi di lavoro su un cluster. Consentono di identificare gli oggetti storage con tempi di risposta lenti, noti anche come alta latenza. Insieme ad altri eventi di salute che si sono verificati contemporaneamente, è possibile determinare i problemi che potrebbero aver causato o contribuito a ridurre i tempi di risposta.

Unified Manager riceve gli eventi relativi alle performance dalle seguenti fonti:

- **Eventi del criterio di soglia delle performance definiti dall'utente**

  Problemi di performance basati su valori di soglia personalizzati impostati. È possibile configurare i criteri di soglia delle performance per gli oggetti storage, ad esempio aggregati e volumi, in modo che gli eventi vengano generati quando viene violato un valore di soglia per un contatore delle performance.

  Per ricevere questi eventi, è necessario definire un criterio di soglia delle performance e assegnarlo a un oggetto di storage.

- **Eventi dei criteri di soglia delle performance definiti dal sistema**

Problemi di performance basati su valori di soglia definiti dal sistema. Questi criteri di soglia sono inclusi nell'installazione di Unified Manager per coprire i problemi comuni di performance.

Questi criteri di soglia sono attivati per impostazione predefinita e potrebbero essere visualizzati eventi poco dopo l'aggiunta di un cluster.

- **Dynamic performance threshold events**

  Problemi di performance dovuti a guasti o errori in un'infrastruttura IT o a carichi di lavoro che utilizzano in modo eccessivo le risorse del cluster. La causa di questi eventi potrebbe essere un semplice problema che si corregge per un certo periodo di tempo o che può essere risolto con una riparazione o una modifica della configurazione. Un evento di soglia dinamico indica che i carichi di lavoro su un sistema ONTAP sono lenti a causa di altri carichi di lavoro con un elevato utilizzo di componenti del cluster condivisi.

  Queste soglie sono attivate per impostazione predefinita e potrebbero verificarsi eventi dopo tre giorni di raccolta dei dati da un nuovo cluster.

Tipi di severità degli eventi relativi alle performance

Ogni evento di performance è associato a un tipo di severità per aiutarti a definire la priorità degli eventi che richiedono un'azione correttiva immediata.

- **Critico**

  Si è verificato un evento di performance che potrebbe portare a un'interruzione del servizio se non viene intrapresa immediatamente un'azione correttiva.

  Gli eventi critici vengono inviati solo dalle soglie definite dall'utente.

- **Attenzione**

  Un contatore delle performance per un oggetto cluster non rientra nell'intervallo normale e deve essere monitorato per assicurarsi che non raggiunga la severità critica. Gli eventi di questo livello di gravità non causano interruzioni del servizio e potrebbero non essere necessarie azioni correttive immediate.

  Gli eventi di avviso vengono inviati da soglie definite dall'utente, definite dal sistema o dinamiche.

- **Informazioni**

  L'evento si verifica quando viene rilevato un nuovo oggetto o quando viene eseguita un'azione dell'utente. Ad esempio, quando un oggetto di storage viene cancellato o quando vengono apportate modifiche alla configurazione, viene generato l'evento con tipo di severità informazioni.

  Gli eventi informativi vengono inviati direttamente da ONTAP quando rileva una modifica della configurazione.

Per ulteriori informazioni, consultare i seguenti collegamenti:

- "Cosa succede quando si riceve un evento"
- "Quali informazioni sono contenute in un messaggio di posta elettronica di avviso"
- "Aggiunta di avvisi"
- "Aggiunta di avvisi per eventi relativi alle performance"

Modifiche alla configurazione rilevate da Unified Manager

Unified Manager monitora i cluster per verificare la presenza di modifiche alla configurazione per determinare se una modifica potrebbe aver causato o contribuito a un evento di performance. Le pagine Performance Explorer (Esplora prestazioni) visualizzano un'icona di modifica dell'evento (●) per indicare la data e l'ora in cui è stata rilevata la modifica.

È possibile esaminare i grafici delle prestazioni nelle pagine Performance Explorer e nella pagina workload Analysis per verificare se l'evento di modifica ha influito sulle prestazioni dell'oggetto cluster selezionato. Se la modifica è stata rilevata in corrispondenza o intorno a un evento di performance, la modifica potrebbe aver contribuito al problema, causando l'attivazione dell'avviso di evento.

Unified Manager è in grado di rilevare i seguenti eventi di cambiamento, classificati come eventi informativi:

- Un volume si sposta tra gli aggregati.

  Unified Manager è in grado di rilevare quando lo spostamento è in corso, completato o non riuscito. Se Unified Manager è inattivo durante lo spostamento di un volume, durante il backup rileva lo spostamento del volume e visualizza un evento di modifica.

- Il limite di throughput (MB/s o IOPS) di un gruppo di policy QoS che contiene una o più modifiche dei carichi di lavoro monitorati.

  La modifica del limite di un gruppo di criteri può causare picchi intermittenti della latenza (tempo di risposta), che potrebbero anche attivare eventi per il gruppo di criteri. La latenza ritorna gradualmente alla normalità e gli eventi causati dai picchi diventano obsoleti.

- Un nodo in una coppia ha assume il controllo o restituisce lo storage del nodo partner.

  Unified Manager è in grado di rilevare quando l'operazione di Takeover, Takeover parziale o giveback è stata completata. Se il takeover è causato da un nodo in Panicked, Unified Manager non rileva l'evento.

- Un'operazione di aggiornamento o revert ONTAP è stata completata correttamente.

  Vengono visualizzate la versione precedente e la nuova.

Tipi di criteri di soglia delle performance definiti dal sistema

Unified Manager fornisce alcune policy di soglia standard che monitorano le performance del cluster e generano automaticamente gli eventi. Questi criteri sono attivati per impostazione predefinita e generano eventi di avviso o informazioni quando le soglie di performance monitorate vengono superate.

ⓘ I criteri di soglia delle performance definiti dal sistema non sono abilitati sui sistemi Cloud Volumes ONTAP, ONTAP Edge o ONTAP Select.

Se si ricevono eventi non necessari da qualsiasi criterio di soglia delle performance definito dal sistema, è possibile disattivare gli eventi per i singoli criteri dalla pagina Configurazione eventi.

Policy di soglia del cluster

I criteri di soglia delle performance del cluster definiti dal sistema vengono assegnati, per impostazione predefinita, a ogni cluster monitorato da Unified Manager:

- **Squilibrio del carico del cluster**

  Identifica le situazioni in cui un nodo opera con un carico molto più elevato rispetto agli altri nodi del cluster, con un potenziale impatto sulle latenze dei carichi di lavoro.

  A tale scopo, confronta il valore della capacità di performance utilizzata per tutti i nodi di un cluster per verificare se un nodo ha superato il valore di soglia del 30% per più di 24 ore. Si tratta di un evento di avviso.

- **Squilibrio della capacità del cluster**

  Identifica le situazioni in cui un aggregato ha una capacità utilizzata molto più elevata rispetto ad altri aggregati del cluster, e quindi potenzialmente influisce sullo spazio richiesto per le operazioni.

  A tale scopo, confronta il valore della capacità utilizzata per tutti gli aggregati del cluster per verificare se esiste una differenza del 70% tra gli aggregati. Si tratta di un evento di avviso.

Criteri di soglia dei nodi

I criteri di soglia delle performance dei nodi definiti dal sistema sono assegnati, per impostazione predefinita, a ogni nodo dei cluster monitorati da Unified Manager:

- **Soglia di utilizzo della capacità di performance violata**

  Identifica le situazioni in cui un singolo nodo opera al di sopra dei limiti della sua efficienza operativa e quindi potenzialmente influisce sulle latenze dei carichi di lavoro.

  Ciò avviene cercando nodi che utilizzano oltre il 100% della capacità delle performance per oltre 12 ore. Si tratta di un evento di avviso.

- **Coppia ha nodo sovra-utilizzata**

  Identifica le situazioni in cui i nodi di una coppia ha operano al di sopra dei limiti dell'efficienza operativa della coppia ha.

  Per farlo, è possibile esaminare il valore della capacità di performance utilizzata per i due nodi della coppia ha. Se la capacità delle performance combinate utilizzata dai due nodi supera il 200% per più di 12 ore, il failover del controller avrà un impatto sulle latenze dei carichi di lavoro. Si tratta di un evento informativo.

- **Frammentazione del disco del nodo**

  Identifica le situazioni in cui uno o più dischi di un aggregato sono frammentati, rallentando i servizi di sistema chiave e potenzialmente influenzando le latenze dei workload su un nodo.

  Questo è possibile esaminando alcuni rapporti operativi di lettura e scrittura in tutti gli aggregati di un nodo. Questo criterio potrebbe essere attivato anche durante la risincronizzazione di SyncMirror o quando vengono rilevati errori durante le operazioni di scrubbing del disco. Si tratta di un evento di avviso.

  > Il criterio "frammentazione del disco nodo" analizza gli aggregati solo HDD; gli aggregati di Flash Pool, SSD e FabricPool non vengono analizzati.

Policy di soglia aggregate

Il criterio di soglia delle performance aggregate definito dal sistema viene assegnato per impostazione predefinita a ogni aggregato dei cluster monitorati da Unified Manager:

- **Utilizzo eccessivo dei dischi aggregati**

  Identifica le situazioni in cui un aggregato opera al di sopra dei limiti della sua efficienza operativa, con un potenziale impatto sulle latenze dei carichi di lavoro. Identifica queste situazioni cercando aggregati in cui i dischi nell'aggregato vengono utilizzati per oltre il 95% per più di 30 minuti. Questo criterio di multi-condizione esegue quindi la seguente analisi per determinare la causa del problema:

  - Un disco nell'aggregato è attualmente sottoposto a attività di manutenzione in background?

    Alcune delle attività di manutenzione in background di un disco potrebbero essere la ricostruzione del disco, lo scrubbing del disco, la risincronizzazione SyncMirror e la retparità.

  - C'è un collo di bottiglia nelle comunicazioni nell'interconnessione Fibre Channel dello shelf di dischi?
  - Lo spazio libero nell'aggregato è insufficiente? Un evento di avviso viene emesso per questa policy solo se una (o più) delle tre policy subordinate viene considerata violata. Un evento di performance non viene attivato se vengono utilizzati solo i dischi nell'aggregato per più del 95%.

La policy "aggregate disks over-utilizzed" analizza gli aggregati solo HDD e gli aggregati di Flash Pool (ibridi); gli aggregati SSD e FabricPool non vengono analizzati.

Policy di soglia per la latenza del carico di lavoro

I criteri di soglia di latenza del carico di lavoro definiti dal sistema vengono assegnati a qualsiasi carico di lavoro con una policy del livello di servizio delle prestazioni configurata con un valore definito di "latenza prevista":

- **Soglia di latenza del volume di lavoro/LUN violata come definito dal livello di servizio delle performance**

  Identifica i volumi (condivisioni di file) e le LUN che hanno superato il limite di "latenza prevista" e che influiscono sulle prestazioni del carico di lavoro. Si tratta di un evento di avviso.

  Ciò avviene cercando workload che abbiano superato il valore di latenza previsto per il 30% del tempo nell'ora precedente.

Policy di soglia QoS

I criteri di soglia delle performance QoS definiti dal sistema vengono assegnati a qualsiasi carico di lavoro con una policy di throughput massimo QoS ONTAP configurata (IOPS, IOPS/TB o MB/s). Unified Manager attiva un evento quando il valore di throughput del carico di lavoro è inferiore del 15% rispetto al valore QoS configurato:

- **QoS soglia massima IOPS o MB/s**

  Identifica i volumi e le LUN che hanno superato il limite massimo di throughput di IOPS o MB/s di QoS e che influiscono sulla latenza del carico di lavoro. Si tratta di un evento di avviso.

  Quando un singolo carico di lavoro viene assegnato a un gruppo di policy, questo viene fatto cercando i carichi di lavoro che hanno superato la soglia massima di throughput definita nel gruppo di policy QoS

assegnato durante ciascun periodo di raccolta dell'ora precedente.

Quando più carichi di lavoro condividono una singola policy di QoS, questa operazione viene eseguita aggiungendo gli IOPS o i MB/s di tutti i carichi di lavoro della policy e controllando il totale rispetto alla soglia.

- **QoS Peak IOPS/TB o IOPS/TB con soglia di dimensione del blocco**

  Identifica i volumi che hanno superato il limite massimo di throughput di IOPS/TB di QoS adattiva (o IOPS/TB con il limite di dimensione del blocco) e che influiscono sulla latenza del carico di lavoro. Si tratta di un evento di avviso.

  A tale scopo, converte la soglia di picco IOPS/TB definita nella policy QoS adattiva in un valore IOPS massimo QoS in base alle dimensioni di ciascun volume, quindi cerca i volumi che hanno superato gli IOPS massimi QoS durante ciascun periodo di raccolta delle performance dell'ora precedente.

  Questo criterio viene applicato ai volumi solo quando il cluster viene installato con il software ONTAP 9.3 e versioni successive.

  Quando l'elemento "block size" è stato definito nel criterio QoS adattivo, la soglia viene convertita in un valore massimo di QoS in MB/s in base alle dimensioni di ciascun volume. Quindi, cerca i volumi che hanno superato il QoS max MB/s durante ciascun periodo di raccolta delle performance dell'ora precedente.

  Questo criterio viene applicato ai volumi solo quando il cluster viene installato con il software ONTAP 9.5 e versioni successive.

Analisi e notifica degli eventi relativi alle performance

Gli eventi relativi alle performance avvisano l'utente in merito a problemi di performance i/o su un carico di lavoro causati da conflitti su un componente del cluster. Unified Manager analizza l'evento per identificare tutti i carichi di lavoro coinvolti, il componente in conflitto e se l'evento è ancora un problema che potrebbe essere necessario risolvere.

Unified Manager monitora la latenza di i/o (tempo di risposta) e gli IOPS (operazioni) per i volumi su un cluster. Quando altri carichi di lavoro utilizzano in eccesso un componente del cluster, ad esempio, il componente è in conflitto e non può funzionare a un livello ottimale per soddisfare le esigenze dei carichi di lavoro. Le performance di altri carichi di lavoro che utilizzano lo stesso componente potrebbero risentirne, causando un aumento delle latenze. Se la latenza supera la soglia dinamica delle performance, Unified Manager attiva un evento di performance per avvisare l'utente.

Analisi degli eventi

Unified Manager esegue le seguenti analisi, utilizzando i 15 giorni precedenti di statistiche sulle performance, per identificare i carichi di lavoro delle vittime, i carichi di lavoro ingombranti e il componente del cluster coinvolto in un evento:

- Identifica i carichi di lavoro delle vittime la cui latenza ha superato la soglia di performance dinamica, che è il limite superiore della previsione di latenza:
  - Per i volumi su aggregati ibridi HDD o Flash Pool (Tier locale), gli eventi vengono attivati solo quando la latenza è superiore a 5 millisecondi (ms) e gli IOPS sono più di 10 operazioni al secondo (Ops/sec).

    - Per i volumi su aggregati all-SSD o aggregati FabricPool (cloud Tier), gli eventi vengono attivati solo quando la latenza è superiore a 1 ms e gli IOPS sono superiori a 100 Ops/sec.
- Identifica il componente del cluster in conflitto.

> Se la latenza dei carichi di lavoro delle vittime nell'interconnessione del cluster è superiore a 1 ms, Unified Manager considera questa condizione come significativa e attiva un evento per l'interconnessione del cluster.

- Identifica i carichi di lavoro ingombranti che stanno utilizzando in eccesso il componente del cluster e che lo causano in conflitto.
- Classifica i carichi di lavoro coinvolti, in base alla loro deviazione nell'utilizzo o nell'attività di un componente del cluster, per determinare quali bulli hanno il cambiamento più elevato nell'utilizzo del componente del cluster e quali sono le vittime più interessate.

Un evento potrebbe verificarsi solo per un breve momento e poi correggersi una volta che il componente che sta utilizzando non è più in conflitto. Un evento continuo si verifica nuovamente per lo stesso componente del cluster entro un intervallo di cinque minuti e rimane nello stato attivo. Per gli eventi continui, Unified Manager attiva un avviso dopo aver rilevato lo stesso evento durante due intervalli di analisi consecutivi.

Quando un evento viene risolto, rimane disponibile in Unified Manager come parte della registrazione dei problemi di performance passati per un volume. Ogni evento ha un ID univoco che identifica il tipo di evento e i volumi, il cluster e i componenti del cluster coinvolti.

> Un singolo volume può essere coinvolto in più eventi contemporaneamente.

Stato dell'evento

Gli eventi possono trovarsi in uno dei seguenti stati:

- **Attivo**

  Indica che l'evento di performance è attualmente attivo (nuovo o confermato). Il problema che causa l'evento non è stato risolto o non è stato risolto. Il contatore delle performance per l'oggetto storage rimane al di sopra della soglia di performance.

- **Obsoleto**

  Indica che l'evento non è più attivo. Il problema che ha causato l'evento è stato risolto o risolto. Il contatore delle performance per l'oggetto storage non è più al di sopra della soglia di performance.

Notifica degli eventi

Gli eventi vengono visualizzati nella pagina Dashboard e in molte altre pagine dell'interfaccia utente e gli avvisi relativi a tali eventi vengono inviati a indirizzi e-mail specifici. È possibile visualizzare informazioni di analisi dettagliate su un evento e ottenere suggerimenti per risolverlo nella pagina Dettagli evento e nella pagina analisi del carico di lavoro.

Interazione con gli eventi

Nella pagina Dettagli evento e nella pagina analisi del carico di lavoro, è possibile interagire con gli eventi nei seguenti modi:

- Spostando il mouse su un evento viene visualizzato un messaggio che mostra la data e l'ora in cui è stato rilevato l'evento.

  Se sono presenti più eventi per lo stesso periodo di tempo, il messaggio mostra il numero di eventi.

- Facendo clic su un singolo evento viene visualizzata una finestra di dialogo che mostra informazioni più dettagliate sull'evento, inclusi i componenti del cluster coinvolti.

  Il componente in conflitto viene cerchiato ed evidenziato in rosso. È possibile fare clic su **View full analysis** (Visualizza analisi completa) per visualizzare l'analisi completa nella pagina Event Details (Dettagli evento). Se sono presenti più eventi per lo stesso periodo di tempo, la finestra di dialogo mostra i dettagli relativi ai tre eventi più recenti. È possibile fare clic su un evento per visualizzarne l'analisi nella pagina Dettagli evento.

In che modo Unified Manager determina l'impatto delle performance di un evento

Unified Manager utilizza la deviazione nell'attività, nell'utilizzo, nel throughput di scrittura, nell'utilizzo dei componenti del cluster o nella latenza di i/o (tempo di risposta) per un carico di lavoro per determinare il livello di impatto sulle performance del carico di lavoro. Queste informazioni determinano il ruolo di ciascun carico di lavoro nell'evento e il modo in cui sono classificati nella pagina Dettagli evento.

Unified Manager confronta gli ultimi valori analizzati per un carico di lavoro con l'intervallo previsto (previsione di latenza) dei valori. La differenza tra gli ultimi valori analizzati e l'intervallo di valori previsto identifica i carichi di lavoro le cui performance sono state maggiormente influenzate dall'evento.

Ad esempio, supponiamo che un cluster contenga due carichi di lavoro: Workload A e workload B. La previsione di latenza per il carico di lavoro A è di 5-10 millisecondi per operazione (ms/op) e la latenza effettiva è di solito di circa 7 ms/op. La latenza prevista per il carico di lavoro B è di 10-20 ms/op e la latenza effettiva è di solito di circa 15 ms/op. Entrambi i carichi di lavoro rientrano nella loro previsione di latenza. A causa del conflitto sul cluster, la latenza di entrambi i carichi di lavoro aumenta fino a 40 ms/op, superando la soglia di performance dinamica, che è il limite superiore della previsione di latenza, e attivando gli eventi. La deviazione nella latenza, dai valori previsti ai valori superiori alla soglia di performance, per il carico di lavoro A è di circa 33 ms/op e la deviazione per il carico di lavoro B è di circa 25 ms/op. La latenza di entrambi i carichi di lavoro è aumentata fino a 40 ms/op, ma il carico di lavoro A ha avuto un impatto maggiore sulle performance perché aveva una maggiore deviazione della latenza a 33 ms/op.

Nella pagina Dettagli evento, nella sezione Diagnosi del sistema, è possibile ordinare i carichi di lavoro in base alla loro deviazione nell'attività, nell'utilizzo o nel throughput per un componente del cluster. Puoi anche ordinare i workload in base alla latenza. Quando si seleziona un'opzione di ordinamento, Unified Manager analizza la deviazione nell'attività, nell'utilizzo, nel throughput o nella latenza dal momento in cui l'evento è stato rilevato dai valori previsti per determinare l'ordinamento dei carichi di lavoro. Per la latenza, i punti rossi (🔴) indicano un superamento della soglia di performance da parte di un carico di lavoro della vittima e il conseguente impatto sulla latenza. Ogni punto rosso indica un livello più elevato di deviazione nella latenza, che consente di identificare i carichi di lavoro delle vittime la cui latenza è stata maggiormente influenzata da un evento.

Componenti del cluster e perché possono essere in conflitto

È possibile identificare i problemi di performance del cluster quando un componente del cluster entra in conflitto. Le performance dei carichi di lavoro che utilizzano il componente rallentano e il loro tempo di risposta (latenza) per le richieste dei client aumenta, il che

attiva un evento in Unified Manager.

Un componente in conflitto non può funzionare a un livello ottimale. Le sue performance sono diminuite e le performance di altri componenti e carichi di lavoro del cluster, denominati *vittime*, potrebbero avere una maggiore latenza. Per eliminare un componente dai conflitti, è necessario ridurre il carico di lavoro o aumentare la capacità di gestire più lavoro, in modo che le performance possano tornare ai livelli normali. Poiché Unified Manager raccoglie e analizza le performance dei carichi di lavoro in intervalli di cinque minuti, rileva solo quando un componente del cluster viene costantemente utilizzato in eccesso. I picchi transitori di utilizzo eccessivo che durano solo per una breve durata nell'intervallo di cinque minuti non vengono rilevati.

Ad esempio, un aggregato di storage potrebbe essere in conflitto perché uno o più carichi di lavoro su di esso sono in competizione per soddisfare le richieste di i/O. Altri carichi di lavoro sull'aggregato possono risentirne, causando una diminuzione delle performance. Per ridurre la quantità di attività sull'aggregato, è possibile eseguire diverse operazioni, ad esempio lo spostamento di uno o più carichi di lavoro in un aggregato o nodo meno occupato, per ridurre la domanda complessiva del carico di lavoro sull'aggregato corrente. Per un gruppo di policy QoS, è possibile regolare il limite di throughput o spostare i carichi di lavoro in un gruppo di policy diverso, in modo che i carichi di lavoro non vengano più rallentati.

Unified Manager monitora i seguenti componenti del cluster per avvisare l'utente quando si trovano in conflitto:

- **Rete**

  Rappresenta il tempo di attesa delle richieste di i/o da parte dei protocolli di rete esterni sul cluster. Il tempo di attesa è il tempo impiegato in attesa del completamento delle transazioni "transfer ready" prima che il cluster possa rispondere a una richiesta di i/O. Se il componente di rete è in conflitto, significa che il tempo di attesa elevato a livello di protocollo influisce sulla latenza di uno o più carichi di lavoro.

- **Elaborazione di rete**

  Rappresenta il componente software del cluster coinvolto nell'elaborazione i/o tra il livello di protocollo e il cluster. Il nodo che gestisce l'elaborazione di rete potrebbe essere cambiato da quando è stato rilevato l'evento. Se il componente di elaborazione di rete è in conflitto, significa che un utilizzo elevato nel nodo di elaborazione di rete influisce sulla latenza di uno o più carichi di lavoro.

  Quando si utilizza un cluster All SAN Array in una configurazione Active-Active, il valore di latenza di elaborazione della rete viene visualizzato per entrambi i nodi, in modo da poter verificare che i nodi condividano il carico in maniera uguale.

- **QoS Limit Max**

  Rappresenta l'impostazione di throughput massimo (picco) del gruppo di criteri QoS (Quality of Service) dello storage assegnato al carico di lavoro. Se il componente del gruppo di policy è in conflitto, significa che tutti i carichi di lavoro nel gruppo di policy vengono rallentati dal limite di throughput impostato, il che influisce sulla latenza di uno o più di tali carichi di lavoro.

- **Limite QoS min**

  Rappresenta la latenza per un carico di lavoro causata dall'impostazione QoS throughput Minimum (previsto) assegnata ad altri carichi di lavoro. Se il valore minimo di QoS impostato su alcuni carichi di lavoro utilizza la maggior parte della larghezza di banda per garantire il throughput promesso, altri carichi di lavoro verranno rallentati e otterranno una maggiore latenza.

- **Interconnessione cluster**

  Rappresenta i cavi e gli adattatori con cui i nodi in cluster sono fisicamente connessi. Se il componente di

interconnessione del cluster è in conflitto, significa che l'elevato tempo di attesa per le richieste di i/o dell'interconnessione del cluster influisce sulla latenza di uno o più carichi di lavoro.

- **Elaborazione dei dati**

  Rappresenta il componente software del cluster coinvolto nell'elaborazione i/o tra il cluster e l'aggregato di storage che contiene il carico di lavoro. Il nodo che gestisce l'elaborazione dei dati potrebbe essere cambiato da quando è stato rilevato l'evento. Se il componente di elaborazione dei dati è in conflitto, significa che un utilizzo elevato nel nodo di elaborazione dei dati influisce sulla latenza di uno o più carichi di lavoro.

- **Attivazione del volume**

  Rappresenta il processo che tiene traccia dell'utilizzo di tutti i volumi attivi. In ambienti di grandi dimensioni in cui sono attivi più di 1000 volumi, questo processo tiene traccia del numero di volumi critici necessari per accedere alle risorse attraverso il nodo allo stesso tempo. Quando il numero di volumi attivi simultanei supera la soglia massima consigliata, alcuni volumi non critici sperimenteranno la latenza come indicato qui.

- **Risorse MetroCluster**

  Rappresenta le risorse MetroCluster, tra cui NVRAM e ISL (Interswitch link), utilizzate per eseguire il mirroring dei dati tra cluster in una configurazione MetroCluster. Se il componente MetroCluster è in conflitto, significa che un elevato throughput di scrittura dai carichi di lavoro sul cluster locale o un problema di integrità del collegamento sta influenzando la latenza di uno o più carichi di lavoro sul cluster locale. Se il cluster non si trova in una configurazione MetroCluster, questa icona non viene visualizzata.

- **Operazioni aggregate o aggregate SSD**

  Rappresenta l'aggregato di storage su cui vengono eseguiti i carichi di lavoro. Se il componente aggregato è in conflitto, significa che un utilizzo elevato dell'aggregato influisce sulla latenza di uno o più carichi di lavoro. Un aggregato è costituito da tutti i dischi rigidi o da una combinazione di dischi rigidi e SSD (un aggregato di pool flash) o da una combinazione di dischi rigidi e un Tier cloud (un aggregato FabricPool). Un "Saggregato SD" è costituito da tutti gli SSD (un aggregato all-flash) o da una combinazione di SSD e un Tier cloud (un aggregato FabricPool).

- **Latenza cloud**

  Rappresenta il componente software del cluster coinvolto nell'elaborazione i/o tra il cluster e il livello cloud in cui vengono memorizzati i dati dell'utente. Se il componente di latenza del cloud è in conflitto, significa che una grande quantità di letture da volumi ospitati sul Tier cloud influisce sulla latenza di uno o più carichi di lavoro.

- **Sync SnapMirror**

  Rappresenta il componente software del cluster coinvolto nella replica dei dati utente dal volume primario al volume secondario in una relazione sincrona di SnapMirror. Se il componente Sync SnapMirror è in conflitto, significa che l'attività delle operazioni di SnapMirror Synchronous influisce sulla latenza di uno o più carichi di lavoro.

Ruoli dei carichi di lavoro coinvolti in un evento di performance

Unified Manager utilizza i ruoli per identificare il coinvolgimento di un workload in un evento di performance. I ruoli includono vittime, tori e squali. Un carico di lavoro definito

dall'utente può essere una vittima, un bullo e uno squalo allo stesso tempo.

Ruolo	Descrizione
Vittima	Un carico di lavoro definito dall'utente le cui performance sono diminuite a causa di altri carichi di lavoro, detti "bulli", che utilizzano in modo eccessivo un componente del cluster. Solo i workload definiti dall'utente sono identificati come vittime. Unified Manager identifica i carichi di lavoro delle vittime in base alla loro deviazione nella latenza, in cui la latenza effettiva, durante un evento, è notevolmente aumentata rispetto alle previsioni di latenza (intervallo previsto).
Bully	Un workload definito dall'utente o dal sistema il cui utilizzo eccessivo di un componente del cluster ha causato la diminuzione delle performance di altri workload, denominati vittime. Unified Manager identifica i carichi di lavoro ingombranti in base alla loro deviazione nell'utilizzo di un componente del cluster, in cui l'utilizzo effettivo, durante un evento, è notevolmente aumentato rispetto all'intervallo di utilizzo previsto.
Squalo	Un carico di lavoro definito dall'utente con il massimo utilizzo di un componente del cluster rispetto a tutti i carichi di lavoro coinvolti in un evento. Unified Manager identifica i carichi di lavoro di Shark in base all'utilizzo di un componente del cluster durante un evento.

I carichi di lavoro su un cluster possono condividere molti dei componenti del cluster, come gli aggregati e la CPU per l'elaborazione di rete e dati. Quando un carico di lavoro, ad esempio un volume, aumenta l'utilizzo di un componente del cluster al punto che il componente non riesce a soddisfare in modo efficiente le richieste di carico di lavoro, il componente è in conflitto. Il carico di lavoro che sta utilizzando in eccesso un componente del cluster è un'operazione molto importante. Gli altri carichi di lavoro che condividono tali componenti e le cui performance sono influenzate dal problema sono le vittime. Anche le attività dei carichi di lavoro definiti dal sistema, come la deduplica o le copie Snapshot, possono essere sottoposte a escalation in "bullismo".

Quando Unified Manager rileva un evento, identifica tutti i carichi di lavoro e i componenti del cluster coinvolti, inclusi i carichi di lavoro ingombranti che hanno causato l'evento, il componente del cluster in conflitto e i carichi di lavoro vittime le cui performance sono diminuite a causa dell'aumento dell'attività dei carichi di lavoro ingombranti.

Se Unified Manager non riesce a identificare i carichi di lavoro ingombrante, avvisa solo sui carichi di lavoro vittime e sul componente del cluster interessato.

Unified Manager è in grado di identificare i carichi di lavoro vittime di carichi di lavoro ingombranti e di identificare anche i casi in cui questi stessi carichi di lavoro diventano carichi di lavoro ingombranti. Un carico di lavoro può essere un'attività molto ingombrante per se stesso. Ad esempio, un carico di lavoro dalle performance elevate che viene rallentato da un limite di gruppo di policy causa la limitazione di tutti i workload

del gruppo di policy, anche se stesso. Un carico di lavoro ingombrante o vittima di un evento di performance in corso potrebbe cambiare il proprio ruolo o non essere più un partecipante all'evento.

Gestione delle soglie di performance

I criteri di soglia delle performance consentono di determinare il punto in cui Unified Manager genera un evento per informare gli amministratori di sistema su problemi che potrebbero influire sulle performance dei workload. Questi criteri di soglia sono noti come soglie di performance *definite dall'utente*.

Questa versione supporta soglie di performance dinamiche, definite dall'utente e definite dal sistema. Con soglie di performance dinamiche e definite dal sistema, Unified Manager analizza l'attività del carico di lavoro per determinare il valore di soglia appropriato. Con le soglie definite dall'utente, è possibile definire i limiti di performance superiori per molti contatori di performance e per molti oggetti di storage.

Le soglie di performance definite dal sistema e le soglie di performance dinamiche vengono impostate da Unified Manager e non sono configurabili. Se si ricevono eventi non necessari da qualsiasi criterio di soglia delle performance definito dal sistema, è possibile disattivare i singoli criteri dalla pagina di configurazione degli eventi.

Come funzionano le policy di soglia delle performance definite dall'utente

È possibile impostare criteri di soglia delle performance sugli oggetti storage (ad esempio, su aggregati e volumi) in modo che un evento possa essere inviato all'amministratore dello storage per informare l'amministratore che il cluster sta riscontrando un problema di performance.

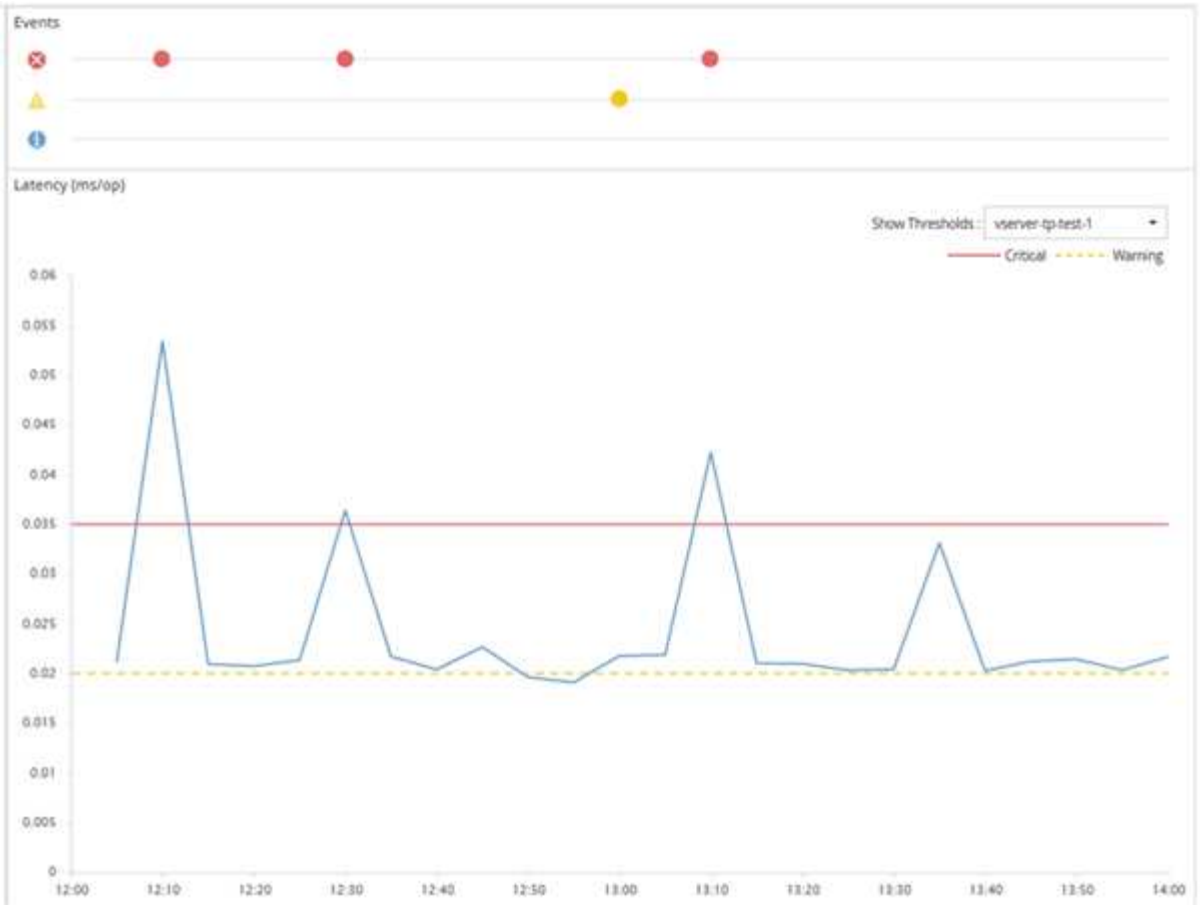
È possibile creare un criterio di soglia delle performance per un oggetto di storage:

- Selezione di un oggetto di storage
- Selezione di un contatore di performance associato a quell'oggetto
- Specificare i valori che definiscono i limiti superiori del contatore delle prestazioni considerati situazioni critiche e di avviso
- Specificare un periodo di tempo che definisce il tempo per il quale il contatore deve superare il limite massimo

Ad esempio, è possibile impostare un criterio di soglia delle performance su un volume in modo da ricevere una notifica di eventi critici ogni volta che gli IOPS per quel volume superano le 750 operazioni al secondo per 10 minuti consecutivi. Questo stesso criterio di soglia può anche specificare che un evento di avviso deve essere inviato quando IOPS supera 500 operazioni al secondo per 10 minuti.

La release corrente fornisce soglie che inviano eventi quando un valore del contatore supera l'impostazione della soglia. Non è possibile impostare soglie che inviino eventi quando un valore del contatore scende al di sotto di un'impostazione di soglia.

Viene visualizzato un esempio di tabella dei contatori, che indica che una soglia di avviso (icona gialla) è stata violata alle 1:00 e che una soglia critica (icona rossa) è stata violata alle 12:10, 12:30 e 1:10:



Una violazione di soglia deve verificarsi continuamente per la durata specificata. Se la soglia scende al di sotto dei valori limite per qualsiasi motivo, una successiva violazione viene considerata l'inizio di una nuova durata.

Alcuni oggetti cluster e contatori delle performance consentono di creare una policy di soglia combinata che richiede che due contatori delle performance superino i limiti massimi prima che venga generato un evento. Ad esempio, è possibile creare un criterio di soglia utilizzando i seguenti criteri:

Oggetto cluster	Contatore delle performance	Soglia di avviso	Soglia critica	Durata
Volume	Latenza	10 millisecondi	20 millisecondi	15 minuti
Aggregato	Utilizzo	65%	85%	

I criteri di soglia che utilizzano due oggetti cluster generano un evento solo quando entrambe le condizioni vengono violate. Ad esempio, utilizzando il criterio di soglia definito nella tabella:

Se la latenza del volume è in media…	E l'utilizzo dei dischi aggregati è…	Quindi…
15 millisecondi	50%	Nessun evento segnalato.
15 millisecondi	75%	Viene segnalato un evento di avviso.

Se la latenza del volume è in media…	E l'utilizzo dei dischi aggregati è…	Quindi…
25 millisecondi	75%	Viene segnalato un evento di avviso.
25 millisecondi	90%	Viene segnalato un evento critico.

Cosa accade quando una policy di soglia delle performance viene violata

Quando un valore del contatore supera il valore di soglia delle prestazioni definito per il periodo di tempo specificato nella durata, la soglia viene violata e viene segnalato un evento.

L'evento causa l'avvio delle seguenti azioni:

- L'evento viene visualizzato nella dashboard, nella pagina Riepilogo cluster di prestazioni, nella pagina Eventi e nella pagina inventario delle prestazioni specifico dell'oggetto.
- (Facoltativo) è possibile inviare un avviso e-mail relativo all'evento a uno o più destinatari e-mail e inviare una trap SNMP a un destinatario della trap.
- (Facoltativo) è possibile eseguire Uno script per modificare o aggiornare automaticamente gli oggetti di storage.

La prima azione viene sempre eseguita. È possibile configurare se le azioni opzionali vengono eseguite nella pagina Configurazione avvisi. È possibile definire azioni univoche in base alla violazione di un criterio di avviso o di soglia critica.

Dopo che si è verificata una violazione del criterio di soglia delle performance su un oggetto di storage, non vengono generati ulteriori eventi per tale criterio fino a quando il valore del contatore non scende al di sotto del valore di soglia, a questo punto la durata viene reimpostata per tale limite. Mentre la soglia continua a essere superata, l'ora di fine dell'evento viene aggiornata costantemente per riflettere che l'evento è in corso.

Un evento di soglia acquisisce o blocca le informazioni relative alla severità e alla definizione del criterio in modo che le informazioni di soglia univoche vengano visualizzate insieme all'evento, anche se il criterio di soglia viene modificato in futuro.

Quali contatori delle performance possono essere monitorati utilizzando le soglie

Alcuni contatori di performance comuni, come IOPS e MB/s, possono avere soglie impostate per tutti gli oggetti di storage. Esistono altri contatori che possono avere soglie impostate solo per determinati oggetti di storage.

Contatori delle performance disponibili

Oggetto di storage	Contatore delle performance	Descrizione
Cluster	IOPS	Numero medio di operazioni di input/output che il cluster elabora al secondo.

Oggetto di storage	Contatore delle performance	Descrizione
MB/s.	Numero medio di megabyte di dati trasferiti da e verso questo cluster al secondo.	Nodo
IOPS	Numero medio di operazioni di input/output che il nodo elabora al secondo.	MB/s.
Numero medio di megabyte di dati trasferiti da e verso questo nodo al secondo.	Latenza	Numero medio di millisecondi necessari al nodo per rispondere alle richieste dell'applicazione.
Utilizzo	Percentuale media di CPU e RAM del nodo utilizzata.	Capacità di performance utilizzata
Percentuale media di capacità di performance consumata dal nodo.	Capacità di performance utilizzata - Takeover	Percentuale media di capacità di performance consumata dal nodo, più la capacità di performance del nodo partner.
Aggregato	IOPS	Numero medio di operazioni di input/output che l'aggregato elabora al secondo.
MB/s.	Numero medio di megabyte di dati trasferiti da e verso questo aggregato al secondo.	Latenza
Numero medio di millisecondi necessari all'aggregato per rispondere alle richieste dell'applicazione.	Utilizzo	Percentuale media dei dischi dell'aggregato utilizzati.
Capacità di performance utilizzata	Percentuale media di capacità di performance consumata dall'aggregato.	VM di storage
IOPS	Numero medio di operazioni di input/output che SVM elabora al secondo.	MB/s.
Numero medio di megabyte di dati trasferiti da e verso questa SVM al secondo.	Latenza	Numero medio di millisecondi impiegato da SVM per rispondere alle richieste dell'applicazione.

Oggetto di storage	Contatore delle performance	Descrizione
Volume	IOPS	Numero medio di operazioni di input/output che il volume elabora al secondo.
MB/s.	Numero medio di megabyte di dati trasferiti da e verso questo volume al secondo.	Latenza
Numero medio di millisecondi necessari al volume per rispondere alle richieste dell'applicazione.	Rapporto di perdita della cache	Percentuale media di richieste di lettura provenienti dalle applicazioni client restituite dal volume invece di essere restituite dalla cache.
LUN	IOPS	Numero medio di operazioni di input/output che il LUN elabora al secondo.
MB/s.	Numero medio di megabyte di dati trasferiti da e verso questa LUN al secondo.	Latenza
Numero medio di millisecondi che il LUN impiega per rispondere alle richieste dell'applicazione.	Namespace	IOPS
Numero medio di operazioni di input/output che lo spazio dei nomi elabora al secondo.	MB/s.	Numero medio di megabyte di dati trasferiti da e verso questo namespace al secondo.
Latenza	Numero medio di millisecondi necessari allo spazio dei nomi per rispondere alle richieste dell'applicazione.	Porta
Utilizzo della larghezza di banda	Percentuale media della larghezza di banda disponibile della porta utilizzata.	MB/s.
Numero medio di megabyte di dati trasferiti da e verso questa porta al secondo.	Interfaccia di rete (LIF)	MB/s.

Quali oggetti e contatori possono essere utilizzati in policy di soglia combinate

Solo alcuni contatori delle performance possono essere utilizzati insieme in policy di combinazione. Quando si specificano i contatori delle prestazioni primari e secondari,

entrambi i contatori delle prestazioni devono superare i limiti massimi prima che venga generato un evento.

Oggetto e contatore dello storage primario	Contatore e oggetto storage secondario
Latenza del volume	IOPS del volume
Volume MB/s.	Utilizzo dell'aggregato
Capacità di performance aggregata utilizzata	Utilizzo del nodo
Capacità di performance del nodo utilizzata	Capacità di performance del nodo utilizzata - Takeover
Latenza del LUN	IOPS LUN
LUN MB/s	Utilizzo dell'aggregato
Capacità di performance aggregata utilizzata	Utilizzo del nodo
Capacità di performance del nodo utilizzata	Capacità di performance del nodo utilizzata - Takeover

Quando un criterio di combinazione di volumi viene applicato a un volume FlexGroup, anziché a un volume FlexVol, è possibile selezionare come contatore secondario solo gli attributi "IOPS volume" e "MB/s volume". Se il criterio di soglia contiene uno degli attributi di nodo o aggregato, il criterio non verrà applicato al volume FlexGroup e verrà visualizzato un messaggio di errore che descrive questo caso. Questo perché i volumi FlexGroup possono esistere su più di un nodo o aggregato.

Creazione di criteri di soglia delle performance definiti dall'utente

Vengono creati criteri di soglia delle performance per gli oggetti storage in modo che le notifiche vengano inviate quando un contatore delle performance supera un valore specifico. La notifica dell'evento indica che il cluster sta riscontrando un problema di performance.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

È possibile creare criteri di soglia delle prestazioni immettendo i valori di soglia nella pagina Crea criterio di soglia delle prestazioni. È possibile creare nuovi criteri definendo tutti i valori dei criteri in questa pagina oppure creare una copia di un criterio esistente e modificare i valori della copia (denominata *cloning*).

I valori di soglia validi sono compresi tra 0.001 e 10,000,000 per i numeri, 0.001-100 per le percentuali e 0.001-200 per le percentuali di utilizzo della capacità di performance.

La release corrente fornisce soglie che inviano eventi quando un valore del contatore supera l'impostazione della soglia. Non è possibile impostare soglie che inviino eventi quando un valore del contatore scende al di sotto di un'impostazione di soglia.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **soglie evento** > **prestazioni**.

   Viene visualizzata la pagina Performance Thresholds (soglie delle prestazioni).

2. Fare clic sul pulsante appropriato a seconda che si desideri creare un nuovo criterio o clonare un criterio simile e modificare la versione clonata.

Per…	Fare clic su…
Creare una nuova policy	**Crea**
Clonare un criterio esistente	Selezionare un criterio esistente e fare clic su **Clone**

   Viene visualizzata la pagina Create Performance Threshold Policy (Crea policy soglia prestazioni) o Clone Performance Threshold Policy (criterio soglia Clone performance)

3. Definire il criterio di soglia specificando i valori di soglia del contatore delle prestazioni che si desidera impostare per oggetti di storage specifici:

   a. Selezionare il tipo di oggetto di storage e specificare un nome e una descrizione per il criterio.
   b. Selezionare il contatore delle prestazioni da tenere traccia e specificare i valori limite che definiscono gli eventi di avviso e critici.

      È necessario definire almeno un avviso o un limite critico. Non è necessario definire entrambi i tipi di limiti.

   c. Selezionare un contatore secondario delle prestazioni, se necessario, e specificare i valori limite per gli eventi critici e di avviso.

      L'inclusione di un contatore secondario richiede che entrambi i contatori superino i valori limite prima che la soglia venga violata e venga segnalato un evento. È possibile configurare solo determinati oggetti e contatori utilizzando un criterio di combinazione.

   d. Selezionare il periodo di tempo per il quale i valori limite devono essere violati per l'invio di un evento.

   Durante la clonazione di un criterio esistente, è necessario immettere un nuovo nome per il criterio.

4. Fare clic su **Save** (Salva) per salvare il criterio.

   Viene visualizzata nuovamente la pagina soglie di performance. Un messaggio di successo nella parte superiore della pagina conferma che il criterio di soglia è stato creato e fornisce un collegamento alla pagina di inventario per quel tipo di oggetto, in modo da poter applicare immediatamente il nuovo criterio agli oggetti di storage.

Se si desidera applicare il nuovo criterio di soglia agli oggetti di storage in questo momento, fare clic sul collegamento **Vai a Object_TYPE** per accedere alla pagina inventario.

Assegnazione di criteri di soglia delle performance agli oggetti di storage

Si assegna un criterio di soglia delle performance definito dall'utente a un oggetto storage in modo che Unified Manager rifera un evento se il valore del contatore delle performance supera l'impostazione del criterio.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

I criteri di soglia delle prestazioni che si desidera applicare all'oggetto devono esistere.

È possibile applicare un solo criterio di performance alla volta a un oggetto o a un gruppo di oggetti.

È possibile assegnare un massimo di tre criteri di soglia a ciascun oggetto di storage. Quando si assegnano criteri a più oggetti, se uno qualsiasi degli oggetti ha già assegnato il numero massimo di criteri, Unified Manager esegue le seguenti azioni:

- Applica il criterio a tutti gli oggetti selezionati che non hanno raggiunto il massimo
- Ignora gli oggetti che hanno raggiunto il numero massimo di criteri
- Visualizza un messaggio che indica che il criterio non è stato assegnato a tutti gli oggetti

Fasi

1. Dalla pagina Performance Inventory di qualsiasi oggetto di storage, selezionare l'oggetto o gli oggetti a cui si desidera assegnare un criterio di soglia:

Per assegnare le soglie a…	Fare clic su…
Un singolo oggetto	La casella di controllo a sinistra dell'oggetto.
Oggetti multipli	La casella di controllo a sinistra di ciascun oggetto.
Tutti gli oggetti della pagina	Il ☐▾ E scegliere **Seleziona tutti gli oggetti in questa pagina**.
Tutti gli oggetti dello stesso tipo	Il ☐▾ E scegliere **Seleziona tutti gli oggetti**.

   È possibile utilizzare la funzionalità di ordinamento e filtraggio per perfezionare l'elenco di oggetti nella pagina di inventario per semplificare l'applicazione di criteri di soglia a molti oggetti.

2. Effettuare la selezione, quindi fare clic su **Assign Performance Threshold Policy**.

   Viene visualizzata la pagina Assign Performance Threshold Policy (Assegna criterio soglia prestazioni), che mostra un elenco di criteri di soglia esistenti per quel tipo specifico di oggetto di storage.

3. Fare clic su ciascun criterio per visualizzare i dettagli delle impostazioni delle soglie delle prestazioni e verificare di aver selezionato il criterio di soglia corretto.
4. Dopo aver selezionato il criterio di soglia appropriato, fare clic su **Assign Policy** (Assegna policy).

   Un messaggio di esito positivo visualizzato nella parte superiore della pagina conferma che il criterio di soglia è stato assegnato all'oggetto o agli oggetti e fornisce un collegamento alla pagina Avvisi in modo da

poter configurare le impostazioni degli avvisi per questo oggetto e criterio.

Se si desidera che gli avvisi vengano inviati tramite e-mail o come trap SNMP, per notificare che è stato generato un particolare evento di performance, è necessario configurare le impostazioni degli avvisi nella pagina Configurazione avvisi.

Visualizzazione dei criteri di soglia delle performance

È possibile visualizzare tutti i criteri di soglia delle performance attualmente definiti dalla pagina soglie delle performance.

L'elenco dei criteri di soglia è ordinato in ordine alfabetico in base al nome del criterio e include i criteri per tutti i tipi di oggetti di storage. È possibile fare clic sull'intestazione di una colonna per ordinare i criteri in base a tale colonna. Se stai cercando una policy specifica, utilizza il filtro e i meccanismi di ricerca per perfezionare l'elenco delle policy di soglia che appaiono nell'elenco di inventario.

Per visualizzare i dettagli di configurazione del criterio, spostare il cursore del mouse sul nome del criterio e sul nome della condizione. Inoltre, è possibile utilizzare i pulsanti forniti per creare, clonare, modificare ed eliminare i criteri di soglia definiti dall'utente.

Fase

1. Nel riquadro di navigazione a sinistra, selezionare **soglie evento** > **prestazioni**.

   Viene visualizzata la pagina Performance Thresholds (soglie delle prestazioni).

Modifica dei criteri di soglia delle performance definiti dall'utente

È possibile modificare le impostazioni di soglia per i criteri di soglia delle performance esistenti. Questo può essere utile se si ricevono troppi o pochi avvisi per determinate condizioni di soglia.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Non è possibile modificare il nome del criterio o il tipo di oggetto di storage monitorato per i criteri di soglia esistenti.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **soglie evento** > **prestazioni**.

   Viene visualizzata la pagina soglie di performance.

2. Selezionare il criterio di soglia che si desidera modificare e fare clic su **Edit** (Modifica).

   Viene visualizzata la pagina Edit Performance Threshold Policy (Modifica policy soglia prestazioni).

3. Apportare le modifiche al criterio di soglia e fare clic su **Save** (Salva).

   Viene visualizzata nuovamente la pagina soglie di performance.

Una volta salvate, le modifiche vengono aggiornate immediatamente su tutti gli oggetti di storage che

utilizzano il criterio.

A seconda del tipo di modifiche apportate al criterio, è possibile rivedere le impostazioni degli avvisi configurate per gli oggetti che utilizzano il criterio nella pagina Configurazione avvisi.

Rimozione dei criteri di soglia delle performance dagli oggetti storage

È possibile rimuovere un criterio di soglia delle performance definito dall'utente da un oggetto storage quando non si desidera più che Unified Manager monitori il valore del contatore delle performance.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

È possibile rimuovere un solo criterio alla volta da un oggetto selezionato.

È possibile rimuovere un criterio di soglia da più oggetti di storage selezionando più di un oggetto nell'elenco.

Fasi

1. Dalla pagina **inventario** di qualsiasi oggetto di storage, selezionare uno o più oggetti per i quali è stata applicata almeno una policy di soglia delle performance.

Per cancellare le soglie da…	Eseguire questa operazione…
Un singolo oggetto	Selezionare la casella di controllo a sinistra dell'oggetto.
Oggetti multipli	Selezionare la casella di controllo a sinistra di ciascun oggetto.
Tutti gli oggetti della pagina	Fare clic su nell'intestazione della colonna.

2. Fare clic su **Cancella policy soglia performance**.

   Viene visualizzata la pagina Clear Threshold Policy (Elimina policy di soglia), che mostra un elenco di criteri di soglia attualmente assegnati agli oggetti di storage.

3. Selezionare il criterio di soglia che si desidera rimuovere dagli oggetti e fare clic su **Clear Policy**.

   Quando si seleziona un criterio di soglia, vengono visualizzati i dettagli del criterio in modo da poter confermare di aver selezionato il criterio appropriato.

Cosa accade quando viene modificata una policy di soglia delle performance

Se si regola il valore del contatore o la durata di un criterio di soglia delle prestazioni esistente, la modifica del criterio viene applicata a tutti gli oggetti di storage che utilizzano il criterio. La nuova impostazione viene eseguita immediatamente e Unified Manager inizia a confrontare i valori dei contatori delle performance con le nuove impostazioni di soglia per tutti i dati delle performance appena raccolti.

Se esistono eventi attivi per oggetti che utilizzano il criterio di soglia modificato, gli eventi vengono contrassegnati come obsoleti e il criterio di soglia inizia a monitorare il contatore come criterio di soglia appena definito.

Quando si visualizza il contatore su cui è stata applicata la soglia nella visualizzazione dettagliata dei grafici dei contatori, le righe di soglia critiche e di avviso riflettono le impostazioni di soglia correnti. Le impostazioni di soglia originali non vengono visualizzate in questa pagina anche se si visualizzano i dati storici quando era attiva la vecchia impostazione di soglia.

Poiché le impostazioni di soglia precedenti non vengono visualizzate nella visualizzazione dettagliata dei grafici dei contatori, è possibile che vengano visualizzati eventi storici al di sotto delle righe di soglia correnti.

Cosa accade ai criteri di soglia delle performance quando un oggetto viene spostato

Poiché i criteri di soglia delle performance vengono assegnati agli oggetti di storage, se si sposta un oggetto, tutti i criteri di soglia assegnati rimangono associati all'oggetto dopo il completamento dello spostamento. Ad esempio, se si sposta un volume o un LUN in un aggregato diverso, i criteri di soglia rimangono attivi per il volume o il LUN sul nuovo aggregato.

Se esiste una condizione di contatore secondaria per il criterio di soglia (un criterio di combinazione), ad esempio se viene assegnata una condizione aggiuntiva a un aggregato o a un nodo, la condizione di contatore secondario viene applicata al nuovo aggregato o nodo a cui il volume o il LUN è stato spostato.

Se esistono nuovi eventi attivi per gli oggetti che utilizzano il criterio di soglia modificato, gli eventi vengono contrassegnati come obsoleti e il criterio di soglia inizia a monitorare il contatore come criterio di soglia appena definito.

Un'operazione di spostamento del volume fa in modo che ONTAP invii un evento di modifica informativo. Un'icona di modifica degli eventi viene visualizzata nella timeline Eventi nella pagina Performance Explorer e nella pagina workload Analysis per indicare l'ora in cui l'operazione di spostamento è stata completata.

Se si sposta un oggetto in un cluster diverso, il criterio di soglia definito dall'utente viene rimosso dall'oggetto. Se necessario, è necessario assegnare un criterio di soglia all'oggetto al termine dell'operazione di spostamento. Tuttavia, i criteri di soglia dinamici e definiti dal sistema vengono applicati automaticamente a un oggetto dopo che è stato spostato in un nuovo cluster.

Funzionalità dei criteri di soglia durante il takeover e il giveback di ha

Quando si verifica un'operazione di Takeover o giveback in una configurazione ad alta disponibilità (ha), gli oggetti spostati da un nodo all'altro mantengono le proprie policy di soglia nello stesso modo delle operazioni di spostamento manuale. Poiché Unified Manager verifica le modifiche alla configurazione del cluster ogni 15 minuti, l'impatto del passaggio al nuovo nodo non viene identificato fino al successivo polling della configurazione del cluster.

Se si verificano operazioni di Takeover e giveback entro un periodo di raccolta di modifiche alla configurazione di 15 minuti, le statistiche sulle performance potrebbero non spostarsi da un nodo all'altro.

Funzionalità dei criteri di soglia durante il trasferimento dell'aggregato

Se si sposta un aggregato da un nodo a un altro utilizzando `aggregate relocation start` comando, i criteri di soglia sia singoli che combinati vengono mantenuti su tutti gli oggetti e la parte di nodo del criterio di soglia viene applicata al nuovo nodo.

Funzionalità dei criteri di soglia durante lo switchover MetroCluster

Gli oggetti che si spostano da un cluster a un altro in una configurazione MetroCluster non mantengono le impostazioni dei criteri di soglia definiti dall'utente. Se necessario, è possibile applicare criteri di soglia ai volumi e alle LUN che sono stati spostati nel cluster del partner. Dopo che un oggetto è stato spostato di nuovo nel cluster originale, il criterio di soglia definito dall'utente viene riapplicato automaticamente.

Per ulteriori informazioni, vedere "Comportamento del volume durante lo switchover e lo switchback".

Analisi degli eventi relativi alle performance

È possibile analizzare gli eventi relativi alle performance per identificare quando sono stati rilevati, se sono attivi (nuovi o riconosciuti) o obsoleti, i carichi di lavoro e i componenti del cluster coinvolti e le opzioni per la risoluzione degli eventi autonomamente.

Visualizzazione di informazioni sugli eventi relativi alle performance

È possibile utilizzare la pagina inventario gestione eventi per visualizzare un elenco di tutti gli eventi relativi alle performance dei cluster monitorati da Unified Manager. La visualizzazione di queste informazioni consente di determinare gli eventi più critici e di eseguire il drill-down delle informazioni dettagliate per determinare la causa dell'evento.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

L'elenco degli eventi viene ordinato in base all'ora rilevata, con gli eventi più recenti elencati per primi. È possibile fare clic sull'intestazione di una colonna per ordinare gli eventi in base a tale colonna. Ad esempio, è possibile ordinare gli eventi in base alla colonna Stato per visualizzarli in base alla gravità. Se si sta cercando un evento specifico o un tipo specifico di evento, è possibile utilizzare i meccanismi di filtro e ricerca per perfezionare l'elenco degli eventi visualizzati nell'elenco.

Gli eventi di tutte le origini vengono visualizzati in questa pagina:

- Policy di soglia delle performance definite dall'utente
- Policy di soglia delle performance definite dal sistema
- Soglia dinamica delle performance

La colonna tipo di evento elenca l'origine dell'evento. È possibile selezionare un evento per visualizzarne i dettagli nella pagina Dettagli evento.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**.

2. Dal menu View (Visualizza), selezionare **Active performance events** (Eventi performance attivi).

   La pagina visualizza tutti gli eventi New e Acknowledged Performance generati negli ultimi 7 giorni.

3. Individuare un evento che si desidera analizzare e fare clic sul nome dell'evento.

   Viene visualizzata la pagina dei dettagli dell'evento.

> È inoltre possibile visualizzare la pagina dei dettagli di un evento facendo clic sul collegamento relativo al nome dell'evento dalla pagina Performance Explorer e da un'email di avviso.

Analisi degli eventi dalle soglie di performance definite dall'utente

Gli eventi generati dalle soglie definite dall'utente indicano che un contatore delle prestazioni per un determinato oggetto di storage, ad esempio un aggregato o un volume, ha superato la soglia definita nel criterio. Questo indica che l'oggetto cluster sta riscontrando un problema di performance.

La pagina Dettagli evento consente di analizzare l'evento relativo alle performance e, se necessario, di intraprendere azioni correttive per riportare le performance alla normalità.

Risposta agli eventi di soglia delle performance definiti dall'utente

È possibile utilizzare Unified Manager per analizzare gli eventi relativi alle performance causati da un contatore delle performance che supera un avviso definito dall'utente o una soglia critica. È inoltre possibile utilizzare Unified Manager per controllare lo stato del componente del cluster per verificare se gli eventi di integrità recenti rilevati sul componente hanno contribuito all'evento delle performance.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Devono essere presenti eventi di performance nuovi o obsoleti.

Fasi

1. Visualizzare la pagina **Dettagli evento** per visualizzare le informazioni relative all'evento.
2. Esaminare la **Descrizione**, che descrive la violazione di soglia che ha causato l'evento.

   Ad esempio, il messaggio "Latency value of 456 ms/op has triggered a WARNING event based on threshold setting of 400 ms/op" indica che si è verificato un evento di avviso di latenza per l'oggetto.

3. Posizionare il cursore sul nome del criterio per visualizzare i dettagli relativi al criterio di soglia che ha attivato l'evento.

   Sono inclusi il nome della policy, il contatore delle performance da valutare, il valore del contatore che deve essere violato per essere considerato un evento critico o di avviso e la durata entro cui il contatore deve superare il valore.

4. Prendere nota del **tempo di attivazione dell'evento** in modo da poter verificare se altri eventi potrebbero aver avuto luogo contemporaneamente e che potrebbero aver contribuito a questo evento.
5. Seguire una delle opzioni riportate di seguito per esaminare ulteriormente l'evento e determinare se è necessario eseguire azioni per risolvere il problema di performance:

Opzione	Possibili azioni di indagine
Fare clic sul nome dell'oggetto di origine per visualizzare la pagina Explorer relativa all'oggetto.	Questa pagina consente di visualizzare i dettagli dell'oggetto e di confrontarlo con altri oggetti di storage simili per verificare se altri oggetti di storage presentano problemi di performance contemporaneamente. Ad esempio, per verificare se anche altri volumi sullo stesso aggregato presentano un problema di performance.
Fare clic sul nome del cluster per visualizzare la pagina Cluster Summary (Riepilogo cluster).	Questa pagina consente di visualizzare i dettagli del cluster in cui risiede questo oggetto per verificare se si sono verificati altri problemi di performance contemporaneamente.

Analisi degli eventi dalle soglie di performance definite dal sistema

Gli eventi generati dalle soglie delle performance definite dal sistema indicano che un contatore delle performance, o un insieme di contatori delle performance, per un determinato oggetto di storage ha superato la soglia di un criterio definito dal sistema. Ciò indica che l'oggetto storage, ad esempio un aggregato o un nodo, sta riscontrando un problema di performance.

La pagina Dettagli evento consente di analizzare l'evento relativo alle performance e, se necessario, di intraprendere azioni correttive per riportare le performance alla normalità.

I criteri di soglia definiti dal sistema non sono abilitati sui sistemi Cloud Volumes ONTAP, ONTAP Edge o ONTAP Select.

Risposta agli eventi di soglia delle performance definiti dal sistema

È possibile utilizzare Unified Manager per analizzare gli eventi relativi alle performance causati da un contatore delle performance che supera una soglia di avviso definita dal sistema. È inoltre possibile utilizzare Unified Manager per controllare lo stato del componente del cluster e verificare se gli eventi recenti rilevati sul componente hanno contribuito all'evento delle performance.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Devono essere presenti eventi di performance nuovi o obsoleti.

Fasi

1. Visualizzare la pagina **Dettagli evento** per visualizzare le informazioni relative all'evento.
2. Esaminare la **Descrizione**, che descrive la violazione di soglia che ha causato l'evento.

   Ad esempio, il messaggio "Node Utilization value of 90 % has triggered a WARNING event based on threshold setting of 85 %" indica che si è verificato un evento di avviso di utilizzo del nodo per l'oggetto cluster.

3. Prendere nota del **tempo di attivazione dell'evento** in modo da poter verificare se altri eventi potrebbero aver avuto luogo contemporaneamente e che potrebbero aver contribuito a questo evento.
4. In **System Diagnosis** (Diagnosi del sistema), esaminare la breve descrizione del tipo di analisi che la policy definita dal sistema sta eseguendo sull'oggetto cluster.

   Per alcuni eventi viene visualizzata un'icona verde o rossa accanto alla diagnosi per indicare se è stato rilevato un problema in quella particolare diagnosi. Per altri tipi di eventi definiti dal sistema, i grafici dei contatori visualizzano le prestazioni dell'oggetto.

5. Nella sezione **azioni consigliate**, fare clic sul collegamento **Aiutami a eseguire questa operazione** per visualizzare le azioni consigliate che è possibile eseguire per provare a risolvere l'evento di performance autonomamente.

Risposta agli eventi di performance del gruppo di policy QoS

Unified Manager genera eventi di avviso relativi ai criteri QoS quando il throughput del carico di lavoro (IOPS, IOPS/TB o Mbps) supera l'impostazione del criterio QoS ONTAP definito e la latenza del carico di lavoro ne risulta compromessa. Questi eventi definiti dal sistema offrono l'opportunità di correggere potenziali problemi di performance prima che molti carichi di lavoro siano influenzati dalla latenza.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Devono esserci eventi di performance nuovi, riconosciuti o obsoleti.

Unified Manager genera eventi di avviso per le violazioni delle policy QoS quando il throughput del carico di lavoro ha superato l'impostazione delle policy QoS definite durante ciascun periodo di raccolta delle performance dell'ora precedente. Il throughput del carico di lavoro può superare la soglia QoS solo per un breve periodo di tempo durante ciascun periodo di raccolta, ma Unified Manager visualizza solo il throughput "Average" durante il periodo di raccolta sul grafico. Per questo motivo, è possibile che si ricevano eventi QoS mentre il throughput di un carico di lavoro potrebbe non aver superato la soglia di policy indicata nel grafico.

È possibile utilizzare Gestione sistema o i comandi ONTAP per gestire i gruppi di criteri, incluse le seguenti attività:

- Creazione di un nuovo gruppo di policy per il carico di lavoro
- Aggiunta o rimozione di workload in un gruppo di policy
- Spostamento di un workload tra gruppi di policy
- Modifica del limite di throughput di un gruppo di criteri
- Spostamento di un workload in un aggregato o nodo diverso

Fasi

1. Visualizzare la pagina **Dettagli evento** per visualizzare le informazioni relative all'evento.
2. Esaminare la **Descrizione**, che descrive la violazione di soglia che ha causato l'evento.

   Ad esempio, il messaggio "valore IOPS di 1,352 IOPS su vol1_NFS1 ha attivato un evento DI AVVISO per identificare potenziali problemi di performance per il carico di lavoro" indica che si è verificato un evento QoS Max IOPS sul volume vol1_NFS1.

3. Consultare la sezione **informazioni evento** per ulteriori informazioni su quando si è verificato l'evento e per quanto tempo l'evento è stato attivo.

   Inoltre, per i volumi o le LUN che condividono il throughput di una policy di QoS, è possibile visualizzare i nomi dei tre principali carichi di lavoro che consumano il maggior numero di IOPS o Mbps.

4. Nella sezione **System Diagnosis** (Diagnosi del sistema), esaminare i due grafici: Uno per la media totale di IOPS o Mbps (a seconda dell'evento) e uno per la latenza. Una volta sistemati in questo modo, è possibile vedere quali componenti del cluster influiscono maggiormente sulla latenza quando il carico di lavoro ha raggiunto il limite massimo di QoS.

   Per un evento di policy QoS condivisa, i tre carichi di lavoro principali sono mostrati nel grafico del throughput. Se più di tre carichi di lavoro condividono la policy QoS, i carichi di lavoro aggiuntivi vengono aggiunti insieme in una categoria "altri carichi di lavoro". Inoltre, il grafico della latenza mostra la latenza media su tutti i carichi di lavoro che fanno parte della policy QoS.

   Si noti che per gli eventi del criterio QoS adattiva, i grafici IOPS e Mbps mostrano i valori IOPS o Mbps che ONTAP ha convertito dal criterio di soglia IOPS/TB assegnato in base alle dimensioni del volume.

5. Nella sezione **azioni consigliate**, esaminare i suggerimenti e determinare le azioni da eseguire per evitare un aumento della latenza per il carico di lavoro.

   Se necessario, fare clic sul pulsante **Help** (Guida) per visualizzare ulteriori dettagli sulle azioni consigliate che è possibile eseguire per tentare di risolvere l'evento relativo alle performance.

Comprendere gli eventi delle policy QoS adattive con una dimensione del blocco definita

I gruppi di policy QoS adattivi scalano automaticamente un limite di throughput o un piano in base alle dimensioni del volume, mantenendo il rapporto tra IOPS e TB al variare delle dimensioni del volume. A partire da ONTAP 9.5, è possibile specificare la dimensione del blocco nel criterio QoS per applicare efficacemente una soglia MB/s contemporaneamente.

L'assegnazione di una soglia IOPS in una policy QoS adattiva pone un limite solo al numero di operazioni che si verificano in ogni workload. A seconda della dimensione del blocco impostata sul client che genera i carichi di lavoro, alcuni IOPS includono molto più dati e quindi pongono un carico molto maggiore sui nodi che elaborano le operazioni.

Il valore in MB/s per un carico di lavoro viene generato utilizzando la seguente formula:

```
MB/s = (IOPS * Block Size) / 1000
```

Se un carico di lavoro ha una media di 3,000 IOPS e la dimensione del blocco sul client è impostata su 32 KB, i MB/s effettivi per questo carico di lavoro sono 96. Se lo stesso carico di lavoro ha una media di 3,000 IOPS e

la dimensione del blocco sul client è impostata su 48 KB, il MB/s effettivo per questo carico di lavoro è 144. È possibile notare che il nodo sta elaborando il 50% di dati in più quando la dimensione del blocco è maggiore.

Esaminiamo la seguente policy QoS adattiva che ha una dimensione del blocco definita e il modo in cui gli eventi vengono attivati in base alla dimensione del blocco impostata sul client.

Creare una policy e impostare il throughput di picco su 2,500 IOPS/TB con una dimensione del blocco di 32 KB. In questo modo si imposta la soglia MB/s a 80 MB/s ((2500 IOPS * 32 KB) / 1000) per un volume con 1 TB di capacità utilizzata. Si noti che Unified Manager genera un evento Warning quando il valore di throughput è inferiore del 10% rispetto alla soglia definita. Gli eventi vengono generati nelle seguenti situazioni:

Capacità utilizzata	**L'evento viene generato quando il throughput supera questo numero di …**	
	IOPS	MB/s.
1 TB	2,250 IOPS	72 MB/s.
2 TB	4,500 IOPS	144 MB/s.
5 TB	11,250 IOPS	360 MB/s.

Se il volume utilizza 2 TB di spazio disponibile e IOPS è 4,000 e la dimensione del blocco QoS è impostata su 32 KB sul client, il throughput in MB/ps è 128 MB/s ((4,000 IOPS * 32 KB) / 1000). In questo scenario non viene generato alcun evento, in quanto 4,000 IOPS e 128 MB/s sono al di sotto della soglia per un volume che utilizza 2 TB di spazio.

Se il volume utilizza 2 TB di spazio disponibile e IOPS è 4,000 e la dimensione del blocco QoS è impostata su 64 KB sul client, il throughput in MB/s è 256 MB/s ((4,000 IOPS * 64 KB) / 1000). In questo caso, 4,000 IOPS non genera un evento, ma il valore MB/s di 256 MB/s è superiore alla soglia di 144 MB/s e viene generato un evento.

Per questo motivo, quando un evento viene attivato in base a una violazione in MB/s per una policy QoS adattiva che include le dimensioni del blocco, viene visualizzato un grafico in MB/s nella sezione Diagnosi del sistema della pagina Dettagli evento. Se l'evento viene attivato in base a una violazione IOPS per la policy QoS adattiva, nella sezione Diagnosi del sistema viene visualizzato un grafico IOPS. Se si verifica una violazione per IOPS e MB/s, si riceveranno due eventi.

Per ulteriori informazioni sulla regolazione delle impostazioni QoS, vedere "Panoramica sulla gestione delle performance".

Rispondere agli eventi di performance sovrautilizzati dalle risorse dei nodi

Unified Manager genera eventi di avviso di risorse del nodo sovrautilizzate quando un singolo nodo opera al di sopra dei limiti della sua efficienza operativa e quindi potenzialmente influisce sulle latenze dei carichi di lavoro. Questi eventi definiti dal sistema offrono l'opportunità di correggere potenziali problemi di performance prima che molti carichi di lavoro siano influenzati dalla latenza.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

- Devono essere presenti eventi di performance nuovi o obsoleti.

Unified Manager genera eventi di avviso per le violazioni delle policy di risorse dei nodi in eccesso cercando nodi che utilizzano oltre il 100% della loro capacità di performance per più di 30 minuti.

È possibile utilizzare Gestione sistema o i comandi ONTAP per correggere questo tipo di problemi di prestazioni, incluse le seguenti attività:

- Creazione e applicazione di una policy QoS a volumi o LUN che utilizzano in eccesso le risorse di sistema
- Riduzione del limite massimo di throughput QoS di un gruppo di policy a cui sono stati applicati i carichi di lavoro
- Spostamento di un workload in un aggregato o nodo diverso
- Aumento della capacità aggiungendo dischi al nodo o eseguendo l'aggiornamento a un nodo con una CPU più veloce e una maggiore quantità di RAM

Fasi

1. Visualizzare la pagina **Dettagli evento** per visualizzare le informazioni relative all'evento.
2. Esaminare la **Descrizione**, che descrive la violazione di soglia che ha causato l'evento.

   Ad esempio, il messaggio "Perf. Valore di capacità utilizzata del 139% su Simplicity-02 ha attivato un EVENTO DI AVVISO per identificare potenziali problemi di performance nell'unità di elaborazione dati." indica che la capacità delle performance sul nodo simplicity-02 viene utilizzata in eccesso e influisce sulle performance del nodo.

3. Nella sezione **System Diagnosis**, esaminate i tre grafici: Uno per la capacità di performance utilizzata sul nodo, uno per gli IOPS di storage medi utilizzati dai carichi di lavoro principali e uno per la latenza sui carichi di lavoro principali. Una volta disposti in questo modo, è possibile vedere quali carichi di lavoro sono la causa della latenza sul nodo.

   È possibile visualizzare i carichi di lavoro per i quali sono applicate le policy di QoS, e quali no, spostando il cursore sul grafico IOPS.

4. Nella sezione **azioni consigliate**, esaminare i suggerimenti e determinare le azioni da eseguire per evitare un aumento della latenza per il carico di lavoro.

   Se necessario, fare clic sul pulsante **Help** (Guida) per visualizzare ulteriori dettagli sulle azioni consigliate che è possibile eseguire per tentare di risolvere l'evento relativo alle performance.

Risposta agli eventi di sbilanciamento delle performance del cluster

Unified Manager genera eventi di avviso di squilibrio del cluster quando un nodo di un cluster opera a un carico molto più elevato rispetto ad altri nodi, con un potenziale impatto sulle latenze dei workload. Questi eventi definiti dal sistema offrono l'opportunità di correggere potenziali problemi di performance prima che molti carichi di lavoro siano influenzati dalla latenza.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Unified Manager genera eventi di avviso per le violazioni delle policy di soglia dello squilibrio del cluster

confrontando il valore della capacità di performance utilizzata per tutti i nodi del cluster per verificare se esiste una differenza di carico del 30% tra i nodi.

Questi passaggi consentono di identificare le seguenti risorse in modo da poter spostare i carichi di lavoro dalle performance elevate in un nodo meno utilizzato:

- I nodi dello stesso cluster meno utilizzati
- Gli aggregati sul nuovo nodo che sono i meno utilizzati
- I volumi dalle performance più elevate sul nodo corrente

Fasi

1. Visualizzare la pagina dei dettagli **evento** per visualizzare le informazioni sull'evento.
2. Esaminare la **Descrizione**, che descrive la violazione di soglia che ha causato l'evento.

   Ad esempio, il messaggio "il contatore della capacità di performance utilizzata indica una differenza di carico del 62% tra i nodi sul cluster Dallas-1-8 e ha attivato un evento DI AVVISO basato sulla soglia di sistema del 30%" indica che la capacità di performance su uno dei nodi è in eccesso e influisce sulle performance del nodo.

3. Consultare il testo nella sezione **azioni consigliate** per spostare un volume dalle performance elevate dal nodo con il valore di capacità utilizzata dalle performance elevate a un nodo con il valore di capacità utilizzata dalle performance più basso.
4. Identificare i nodi con il valore più alto e più basso utilizzato per la capacità di performance:
   a. Nella sezione **informazioni evento**, fare clic sul nome del cluster di origine.
   b. Nella pagina **Cluster / Performance Summary**, fare clic su **Nodes** nell'area **Managed Objects**.
   c. Nella pagina di inventario **nodi**, ordinare i nodi in base alla colonna **capacità di performance utilizzata**.
   d. Identificare i nodi con il valore più alto e più basso utilizzato per la capacità di performance e annotare i nomi.
5. Identificare il volume utilizzando il maggior numero di IOPS sul nodo con il valore di capacità utilizzata dalle performance più elevato:
   a. Fare clic sul nodo con il valore più elevato utilizzato per la capacità delle performance.
   b. Nella pagina **Node / Performance Explorer**, selezionare **Aggregates on this Node** (aggregati su questo nodo) dal menu **View and compare** (Visualizza e confronta).
   c. Fare clic sull'aggregato con il valore più elevato utilizzato per la capacità delle performance.
   d. Nella pagina **aggregato / Performance Explorer**, selezionare **volumi su questo aggregato** dal menu **Visualizza e confronta**.
   e. Ordinare i volumi in base alla colonna **IOPS** e annotare il nome del volume utilizzando il maggior numero di IOPS e il nome dell'aggregato in cui si trova il volume.
6. Identificare l'aggregato con l'utilizzo più basso sul nodo con il valore più basso utilizzato per la capacità di performance:
   a. Fare clic su **Storage** > **aggregati** per visualizzare la pagina di inventario **aggregati**.
   b. Selezionare la vista **Performance: All aggregates** (prestazioni: Tutti gli aggregati).
   c. Fare clic sul pulsante **Filter** (filtro) e aggiungere un filtro in cui "Node" (nodo) sia uguale al nome del nodo con il valore minimo di performance Capacity used (capacità di performance utilizzata) annotato al punto 4.

d. Annotare il nome dell'aggregato che ha il valore di capacità di performance più basso utilizzato.

7. Spostare il volume dal nodo sovraccarico all'aggregato identificato come a basso utilizzo nel nuovo nodo.

   È possibile eseguire l'operazione di spostamento utilizzando Gestione sistema di ONTAP, OnCommand Workflow Automation, comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, verificare se si sta ricevendo lo stesso evento di sbilanciamento del cluster da questo cluster.

Analisi degli eventi dalle soglie di performance dinamiche

Gli eventi generati dalle soglie dinamiche indicano che il tempo di risposta effettivo (latenza) per un carico di lavoro è troppo alto o troppo basso rispetto all'intervallo di tempo di risposta previsto. La pagina Dettagli evento consente di analizzare l'evento relativo alle performance e, se necessario, di intraprendere azioni correttive per riportare le performance alla normalità.

Le soglie di performance dinamiche non sono attivate sui sistemi Cloud Volumes ONTAP, ONTAP Edge o ONTAP Select.

Identificazione dei carichi di lavoro delle vittime coinvolti in un evento di performance dinamico

In Unified Manager, è possibile identificare i carichi di lavoro dei volumi con la maggiore deviazione nel tempo di risposta (latenza) causata da un componente dello storage in conflitto. L'identificazione di questi carichi di lavoro consente di capire perché le applicazioni client che accedono a tali carichi di lavoro hanno registrato performance più lente del solito.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Devono essere presenti eventi di performance dinamiche nuovi, riconosciuti o obsoleti.

La pagina Dettagli evento visualizza un elenco dei carichi di lavoro definiti dall'utente e dal sistema, classificati in base alla deviazione più elevata nell'attività o nell'utilizzo del componente o più interessati dall'evento. I valori si basano sui picchi identificati da Unified Manager al momento del rilevamento e dell'ultima analisi dell'evento.

Fasi

1. Visualizzare la pagina **Dettagli evento** per visualizzare le informazioni relative all'evento.
2. Nei grafici Workload Latency (latenza del carico di lavoro) e Workload Activity (attività del carico di lavoro), selezionare **vittime workload**.
3. Posizionare il cursore sui grafici per visualizzare i principali carichi di lavoro definiti dall'utente che influiscono sul componente e il nome del carico di lavoro della vittima.

Identificazione dei carichi di lavoro ingombranti coinvolti in un evento di performance dinamica

In Unified Manager, è possibile identificare i carichi di lavoro con la maggiore deviazione

nell'utilizzo di un componente del cluster in conflitto. L'identificazione di questi carichi di lavoro consente di capire perché alcuni volumi del cluster hanno tempi di risposta lenti (latenza).

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Devono essere presenti eventi di performance dinamiche nuovi, riconosciuti o obsoleti.

Nella pagina Dettagli evento viene visualizzato un elenco dei carichi di lavoro definiti dall'utente e dal sistema, classificati in base all'utilizzo più elevato del componente o più interessati dall'evento. I valori si basano sui picchi identificati da Unified Manager al momento del rilevamento e dell'ultima analisi dell'evento.

Fasi

1. Visualizzare la pagina Dettagli evento per visualizzare le informazioni relative all'evento.
2. Nei grafici latenza del carico di lavoro e attività del carico di lavoro, selezionare **carichi di lavoro bully**.
3. Posizionare il cursore sui grafici per visualizzare i principali carichi di lavoro ingombranti definiti dall'utente che influiscono sul componente.

Identificazione dei carichi di lavoro di Shark coinvolti in un evento di performance dinamico

In Unified Manager, è possibile identificare i carichi di lavoro con la maggiore deviazione nell'utilizzo di un componente storage in conflitto. L'identificazione di questi workload consente di determinare se questi workload devono essere spostati in un cluster meno utilizzato.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Esistono eventi dinamici di performance nuovi, riconosciuti o obsoleti.

Nella pagina Dettagli evento viene visualizzato un elenco dei carichi di lavoro definiti dall'utente e dal sistema, classificati in base all'utilizzo più elevato del componente o più interessati dall'evento. I valori si basano sui picchi identificati da Unified Manager al momento del rilevamento e dell'ultima analisi dell'evento.

Fasi

1. Visualizzare la pagina **Dettagli evento** per visualizzare le informazioni relative all'evento.
2. Nei grafici Workload Latency (latenza del carico di lavoro) e Workload Activity (attività del carico di lavoro), selezionare **Shark workload**.
3. Posizionare il cursore sui grafici per visualizzare i principali carichi di lavoro definiti dall'utente che influiscono sul componente e il nome del carico di lavoro di Shark.

Analisi degli eventi di performance per una configurazione MetroCluster

È possibile utilizzare Unified Manager per analizzare un evento di performance per una configurazione MetroCluster. È possibile identificare i carichi di lavoro coinvolti nell'evento e rivedere le azioni suggerite per risolverlo.

Gli eventi relativi alle performance di MetroCluster potrebbero essere dovuti a carichi di lavoro *voluminosi* che utilizzano in eccesso i collegamenti interswitch (ISL) tra i cluster o a problemi di integrità del collegamento. Unified Manager monitora ciascun cluster in una configurazione MetroCluster in modo indipendente, senza considerare gli eventi relativi alle performance su un cluster di partner.

Gli eventi relativi alle performance di entrambi i cluster nella configurazione di MetroCluster vengono visualizzati anche nella pagina della dashboard di Unified Manager. È inoltre possibile visualizzare le pagine Health di Unified Manager per controllare lo stato di salute di ciascun cluster e visualizzarne le relazioni.

Analisi di un evento di performance dinamica su un cluster in una configurazione MetroCluster

È possibile utilizzare Unified Manager per analizzare il cluster in una configurazione MetroCluster in cui è stato rilevato un evento di performance. È possibile identificare il nome del cluster, il tempo di rilevamento degli eventi e i carichi di lavoro *bully* e *vittima* coinvolti.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Per una configurazione MetroCluster devono essere presenti eventi di performance nuovi, riconosciuti o obsoleti.
- Entrambi i cluster nella configurazione di MetroCluster devono essere monitorati dalla stessa istanza di Unified Manager.

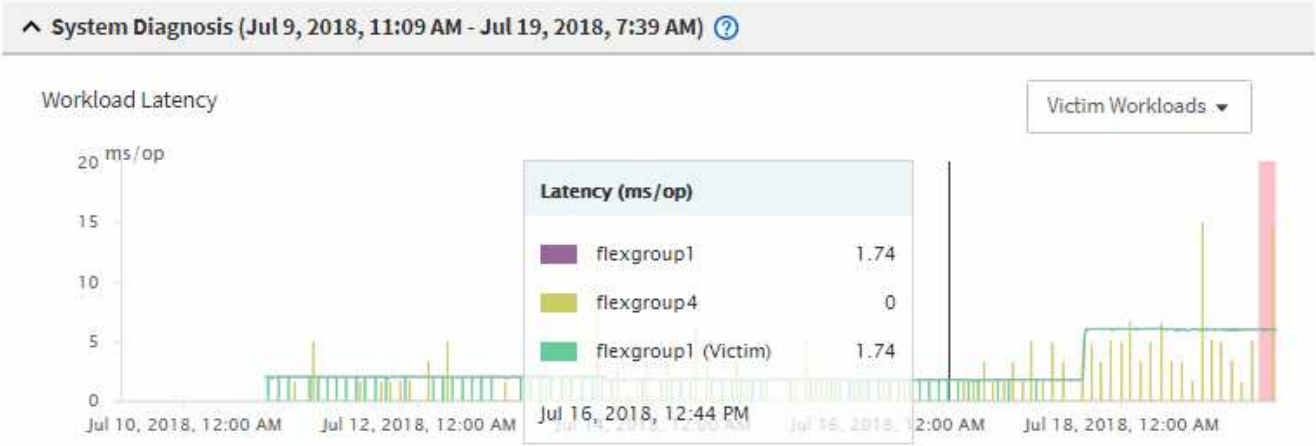
Fasi

1. Visualizzare la pagina **Dettagli evento** per visualizzare le informazioni relative all'evento.
2. Esaminare la descrizione dell'evento per visualizzare i nomi dei carichi di lavoro coinvolti e il numero di carichi di lavoro coinvolti.

   In questo esempio, l'icona risorse MetroCluster è rossa, a indicare che le risorse MetroCluster sono in conflitto. Posizionare il cursore sull'icona per visualizzare una descrizione dell'icona.

3. Prendere nota del nome del cluster e del tempo di rilevamento degli eventi, che è possibile utilizzare per analizzare gli eventi delle performance sul cluster del partner.
4. Nei grafici, esaminare i carichi di lavoro delle *vittime* per confermare che i tempi di risposta sono superiori alla soglia di performance.

   In questo esempio, il carico di lavoro della vittima viene visualizzato nel testo del passaggio del mouse. I grafici di latenza mostrano, ad alto livello, un modello di latenza coerente per i carichi di lavoro delle vittime coinvolti. Anche se la latenza anomala dei carichi di lavoro delle vittime ha attivato l'evento, un modello di latenza coerente potrebbe indicare che le prestazioni dei carichi di lavoro rientrano nell'intervallo previsto, ma che un picco di i/o ha aumentato la latenza e attivato l'evento.



Se di recente hai installato un'applicazione su un client che accede a questi workload di volume e tale applicazione invia loro una quantità elevata di i/o, potresti prevedere un aumento delle latenze. Se la latenza per i carichi di lavoro rientra nell'intervallo previsto, lo stato dell'evento diventa obsoleto e rimane in questo stato per più di 30 minuti, probabilmente è possibile ignorare l'evento. Se l'evento è in corso e rimane nel nuovo stato, è possibile esaminarlo ulteriormente per determinare se altri problemi hanno causato l'evento.

5. Nel grafico workload throughput, selezionare **Bully workload** per visualizzare i carichi di lavoro ingombrante.

   La presenza di carichi di lavoro ingombranti indica che l'evento potrebbe essere stato causato da uno o più carichi di lavoro nel cluster locale che utilizzano in maniera eccessiva le risorse MetroCluster. I carichi di lavoro ingombranti presentano un'elevata deviazione nel throughput di scrittura (MB/s).

   Questo grafico mostra, ad alto livello, lo schema di throughput in scrittura (MB/s) per i carichi di lavoro. È possibile rivedere il modello di scrittura MB/s per identificare un throughput anomalo, che potrebbe indicare che un carico di lavoro sta utilizzando in modo eccessivo le risorse MetroCluster.

   Se l'evento non coinvolge carichi di lavoro ingombranti, l'evento potrebbe essere stato causato da un problema di integrità del collegamento tra i cluster o da un problema di performance sul cluster partner. È possibile utilizzare Unified Manager per controllare lo stato di entrambi i cluster in una configurazione MetroCluster. È inoltre possibile utilizzare Unified Manager per controllare e analizzare gli eventi relativi alle performance nel cluster dei partner.

Analisi di un evento di performance dinamica per un cluster remoto su una configurazione MetroCluster

È possibile utilizzare Unified Manager per analizzare gli eventi di performance dinamiche su un cluster remoto in una configurazione MetroCluster. L'analisi consente di determinare se un evento nel cluster remoto ha causato un evento nel cluster del partner.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- È necessario aver analizzato un evento di performance su un cluster locale in una configurazione MetroCluster e aver ottenuto il tempo di rilevamento degli eventi.
- È necessario aver controllato lo stato del cluster locale e del cluster partner coinvolti nell'evento delle performance e aver ottenuto il nome del cluster partner.

Fasi

1. Accedere all'istanza di Unified Manager che sta monitorando il cluster partner.
2. Nel riquadro di spostamento di sinistra, fare clic su **Eventi** per visualizzare l'elenco degli eventi.
3. Dal selettore **intervallo di tempo**, selezionare **ultima ora**, quindi fare clic su **Applica intervallo**.
4. Nel selettore **Filtering**, selezionare **Cluster** dal menu a discesa a sinistra, digitare il nome del cluster partner nel campo di testo, quindi fare clic su **Apply Filter** (Applica filtro).

   Se non sono presenti eventi per il cluster selezionato nell'ultima ora, significa che il cluster non ha riscontrato problemi di performance durante il momento in cui l'evento è stato rilevato sul partner.

5. Se nel cluster selezionato sono stati rilevati eventi nell'ultima ora, confrontare l'ora di rilevamento degli eventi con l'ora di rilevamento dell'evento nel cluster locale.

   Se questi eventi coinvolgono carichi di lavoro ingombranti che causano conflitti sul componente di elaborazione dei dati, uno o più di questi problemi potrebbero aver causato l'evento nel cluster locale. È possibile fare clic sull'evento per analizzarlo ed esaminare le azioni suggerite per risolverlo nella pagina Dettagli evento.

   Se questi eventi non coinvolgono carichi di lavoro ingombranti, non hanno causato l'evento delle performance sul cluster locale.

Risposta a un evento di performance dinamico causato dalla limitazione del gruppo di policy QoS

È possibile utilizzare Unified Manager per analizzare un evento di performance causato da un gruppo di policy QoS (Quality of Service) che rallenta il throughput del carico di lavoro (MB/s). La limitazione ha aumentato i tempi di risposta (latenza) dei carichi di lavoro dei volumi nel gruppo di policy. È possibile utilizzare le informazioni sull'evento per determinare se sono necessari nuovi limiti per i gruppi di criteri per arrestare la limitazione.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Devono esserci eventi di performance nuovi, riconosciuti o obsoleti.

Fasi

1. Visualizzare la pagina **Dettagli evento** per visualizzare le informazioni relative all'evento.
2. Leggere la **Descrizione**, che mostra il nome dei carichi di lavoro interessati dalla limitazione.

   La descrizione può visualizzare lo stesso carico di lavoro per la vittima e per la vittima, perché la limitazione rende il carico di lavoro una vittima di se stesso.

3. Registrare il nome del volume utilizzando un'applicazione come un editor di testo.

   È possibile cercare il nome del volume per individuarlo in un secondo momento.

4. Nei grafici latenza del carico di lavoro e utilizzo del carico di lavoro, selezionare **carichi di lavoro bully**.
5. Passare il cursore del mouse sui grafici per visualizzare i principali carichi di lavoro definiti dall'utente che

influiscono sul gruppo di policy.

Il carico di lavoro nella parte superiore dell'elenco presenta la deviazione più elevata e ha causato la limitazione. L'attività è la percentuale del limite del gruppo di policy utilizzato da ciascun carico di lavoro.

6. Nell'area **azioni consigliate**, fare clic sul pulsante **Analyze workload** (analizza carico di lavoro) per il carico di lavoro principale.
7. Nella pagina workload Analysis, impostare il grafico di latenza per visualizzare tutti i componenti del cluster e il grafico di throughput per visualizzare la sezione.

   I diagrammi di dettaglio sono visualizzati sotto il grafico di latenza e il grafico IOPS.

8. Confronta i limiti di QoS nel grafico **latenza** per vedere quale quantità di rallentamento ha influito sulla latenza al momento dell'evento.

   Il gruppo di policy QoS ha un throughput massimo di 1,000 operazioni al secondo (op/sec), che i carichi di lavoro in esso contenuti non possono superare collettivamente. Al momento dell'evento, i carichi di lavoro nel gruppo di policy avevano un throughput combinato di oltre 1,200 op/sec, il che ha fatto sì che il gruppo di policy riducesse la propria attività a 1,000 op/sec.

9. Confrontare i valori di **latenza di lettura/scrittura** con i valori di **lettura/scrittura/altro**.

   Entrambi i grafici mostrano un elevato numero di richieste di lettura con latenza elevata, ma il numero di richieste e la quantità di latenza per le richieste di scrittura sono bassi. Questi valori consentono di determinare se la latenza è aumentata grazie a un elevato throughput o a un numero elevato di operazioni. È possibile utilizzare questi valori quando si decide di impostare un limite di gruppo di criteri sul throughput o sulle operazioni.

10. Utilizzare Gestione di sistema di ONTAP per aumentare il limite corrente del gruppo di criteri a 1,300 op/sec.
11. Dopo una giornata, tornare a Unified Manager e inserire il carico di lavoro registrato nella fase 3 della pagina **analisi del carico di lavoro**.
12. Selezionare il grafico di dettaglio del throughput.

    Viene visualizzato il grafico di lettura/scrittura/altro.

13. Nella parte superiore della pagina, puntare il cursore sull'icona di modifica dell'evento ( ) per la modifica del limite del gruppo di criteri.
14. Confrontare il grafico **Read/Scritture/other** con il grafico **latency**.

    Le richieste di lettura e scrittura sono le stesse, ma la limitazione si è interrotta e la latenza è diminuita.

Risposta a un evento di performance dinamico causato da un guasto al disco

È possibile utilizzare Unified Manager per analizzare un evento di performance causato da carichi di lavoro che utilizzano in modo eccessivo un aggregato. È inoltre possibile utilizzare Unified Manager per controllare lo stato dell'aggregato per verificare se gli eventi di salute recenti rilevati nell'aggregato hanno contribuito all'evento delle performance.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Devono esserci eventi di performance nuovi, riconosciuti o obsoleti.

Fasi

1. Visualizzare la pagina **Dettagli evento** per visualizzare le informazioni relative all'evento.
2. Leggi la **Descrizione**, che descrive i carichi di lavoro coinvolti nell'evento e il componente del cluster in conflitto.

   Esistono più volumi vittime la cui latenza è stata influenzata dal componente del cluster in conflitto. L'aggregato, che si trova nel mezzo di una ricostruzione RAID per sostituire il disco guasto con un disco spare, è il componente del cluster in conflitto. Sotto componente in conflitto, l'icona aggregata viene evidenziata in rosso e il nome dell'aggregato viene visualizzato tra parentesi.

3. Nella tabella relativa all'utilizzo del workload, selezionare **carichi di lavoro bully**.
4. Posizionare il cursore del mouse sul grafico per visualizzare i carichi di lavoro principali che influiscono sul componente.

   I carichi di lavoro più elevati con il massimo utilizzo dal momento in cui è stato rilevato l'evento vengono visualizzati nella parte superiore del grafico. Uno dei carichi di lavoro principali è lo stato dei dischi del carico di lavoro definito dal sistema, che indica una ricostruzione RAID. Una ricostruzione è il processo interno che comporta la ricostruzione dell'aggregato con il disco spare. Il carico di lavoro di integrità del disco, insieme ad altri carichi di lavoro sull'aggregato, probabilmente ha causato il conflitto sull'aggregato e sull'evento associato.

5. Dopo aver confermato che l'attività del carico di lavoro di integrità del disco ha causato l'evento, attendere circa 30 minuti per il completamento della ricostruzione e consentire a Unified Manager di analizzare l'evento e rilevare se l'aggregato è ancora in conflitto.
6. Aggiorna i **Dettagli evento**.

   Una volta completata la ricostruzione RAID, verificare che lo stato sia obsoleto, a indicare che l'evento è stato risolto.

7. Nel grafico sull'utilizzo del workload, selezionare **carichi di lavoro bully** per visualizzare i carichi di lavoro sull'aggregato in base all'utilizzo massimo.
8. Nell'area **azioni consigliate**, fare clic sul pulsante **Analyze workload** (analizza carico di lavoro) per il carico di lavoro principale.
9. Nella pagina **workload Analysis**, impostare l'intervallo di tempo per visualizzare le ultime 24 ore (1 giorno) di dati per il volume selezionato.

   Nella sequenza temporale degli eventi, un punto rosso (🛑) indica quando si è verificato un errore del disco.

10. Nel grafico di utilizzo del nodo e dell'aggregato, nascondere la riga per le statistiche del nodo in modo che rimanga solo la riga aggregata.
11. Confronta i dati di questo grafico con quelli al momento dell'evento nel grafico **latenza**.

    Al momento dell'evento, l'utilizzo dell'aggregato mostra un'elevata quantità di attività di lettura e scrittura, causata dai processi di ricostruzione RAID, che hanno aumentato la latenza del volume selezionato. Poche ore dopo il verificarsi dell'evento, sia le letture che le scritture e la latenza sono diminuite, confermando che l'aggregato non è più in conflitto.

Risposta a un evento di performance dinamico causato da ha Takeover

È possibile utilizzare Unified Manager per analizzare un evento di performance causato dall'elaborazione di dati elevati su un nodo del cluster che si trova in una coppia ad alta disponibilità (ha). È inoltre possibile utilizzare Unified Manager per controllare lo stato dei nodi e verificare se eventuali eventi di salute recenti rilevati sui nodi hanno contribuito all'evento delle performance.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Devono esserci eventi di performance nuovi, riconosciuti o obsoleti.

Fasi

1. Visualizzare la pagina **Dettagli evento** per visualizzare le informazioni relative all'evento.
2. Leggi la **Descrizione**, che descrive i carichi di lavoro coinvolti nell'evento e il componente del cluster in conflitto.

   Esiste un volume vittima la cui latenza è stata influenzata dal componente del cluster in conflitto. Il nodo di elaborazione dati, che ha preso il controllo di tutti i carichi di lavoro dal nodo partner, è la componente del cluster in conflitto. In Component in Contention (componente in conflitto), l'icona Data Processing (elaborazione dati) è evidenziata in rosso e il nome del nodo che stava gestendo l'elaborazione dei dati al momento dell'evento viene visualizzato tra parentesi.

3. In **Description**, fare clic sul nome del volume.

   Viene visualizzata la pagina Volume Performance Explorer (Esplora prestazioni volume). Nella parte superiore della pagina, nella barra degli orari degli eventi, viene visualizzata l'icona di modifica dell'evento () Indica l'ora in cui Unified Manager ha rilevato l'inizio del Takeover ha.

4. Puntare il cursore sull'icona dell'evento di modifica per l'acquisizione ha e i dettagli relativi all'acquisizione ha vengono visualizzati nel testo del passaggio del mouse.

   Nel grafico della latenza, un evento indica che il volume selezionato ha superato la soglia di performance a causa di un'elevata latenza circa nello stesso tempo del takeover ha.

5. Fare clic su **Zoom View** per visualizzare il grafico della latenza in una nuova pagina.
6. Nel menu View (Visualizza), selezionare **Cluster Components** (componenti cluster) per visualizzare la latenza totale per componente del cluster.
7. Puntare il cursore del mouse sull'icona di modifica dell'evento per l'inizio del takeover ha e confrontare la latenza per l'elaborazione dei dati con la latenza totale.

   All'epoca del takeover di ha, si è verificato un picco nell'elaborazione dei dati dovuto all'aumento della domanda di workload sul nodo di elaborazione dei dati. L'aumento dell'utilizzo della CPU ha aumentato la latenza e attivato l'evento.

8. Dopo aver corretto il nodo guasto, utilizzare Gestione sistema ONTAP per eseguire un giveback ha, che sposta i carichi di lavoro dal nodo partner al nodo fisso.
9. Una volta completato il giveback ha, dopo il successivo rilevamento della configurazione in Unified Manager (circa 15 minuti), individuare l'evento e il carico di lavoro che sono stati attivati dal takeover ha nella pagina di inventario **Event Management**.

L’evento attivato dal Takeover ha ora uno stato obsoleto, che indica che l’evento è stato risolto. La latenza nel componente di elaborazione dei dati è diminuita, il che ha ridotto la latenza totale. Il nodo utilizzato dal volume selezionato per l’elaborazione dei dati ha risolto l’evento.

Risoluzione degli eventi relativi alle performance

È possibile utilizzare le azioni suggerite per tentare di risolvere gli eventi relativi alle performance autonomamente. I primi tre suggerimenti vengono sempre visualizzati e le azioni sotto il quarto suggerimento sono specifiche per il tipo di evento visualizzato.

I collegamenti **Aiutami a eseguire questa operazione** forniscono informazioni aggiuntive per ciascuna azione suggerita, incluse le istruzioni per eseguire un’azione specifica. Alcune delle azioni possono comportare l’utilizzo di Unified Manager, Gestore di sistema di ONTAP, OnCommand Workflow Automation, comandi CLI di ONTAP o una combinazione di questi strumenti.

Conferma che la latenza rientra nell’intervallo previsto

Quando un componente del cluster è in conflitto, i carichi di lavoro dei volumi che lo utilizzano potrebbero aver ridotto il tempo di risposta (latenza). È possibile esaminare la latenza di ciascun carico di lavoro della vittima sul componente in conflitto per verificare che la latenza effettiva rientri nell’intervallo previsto. È inoltre possibile fare clic sul nome di un volume per visualizzare i dati storici del volume.

Se l’evento di performance si trova nello stato obsoleto, la latenza di ciascuna vittima coinvolta nell’evento potrebbe essere tornata entro l’intervallo previsto.

Esaminare l’impatto delle modifiche alla configurazione sulle performance del carico di lavoro

Le modifiche alla configurazione del cluster, come un disco guasto, il failover ha o un volume spostato, potrebbero avere un impatto negativo sulle performance del volume e causare una maggiore latenza.

In Unified Manager, è possibile esaminare la pagina analisi del carico di lavoro per vedere quando si è verificata una recente modifica della configurazione e confrontarla con le operazioni e la latenza (tempo di risposta) per verificare se si è verificata una modifica nell’attività per il carico di lavoro del volume selezionato.

Le pagine delle performance di Unified Manager sono in grado di rilevare solo un numero limitato di eventi di cambiamento. Le pagine di stato forniscono avvisi per altri eventi causati da modifiche della configurazione. È possibile cercare il volume in Unified Manager per visualizzare la cronologia degli eventi.

Opzioni per migliorare le performance dei carichi di lavoro dal lato client

È possibile controllare i carichi di lavoro dei client, ad esempio applicazioni o database, che inviano i/o ai volumi coinvolti in un evento di performance per determinare se una modifica lato client potrebbe correggere l’evento.

Quando i client connessi ai volumi su un cluster aumentano le richieste di i/o, il cluster deve lavorare di più per soddisfare la domanda. Se si conoscono i client con un elevato numero di richieste di i/o per un determinato

volume del cluster, è possibile migliorare le prestazioni del cluster regolando il numero di client che accedono al volume o diminuendo la quantità di i/o nel volume. È inoltre possibile applicare o aumentare un limite al gruppo di criteri QoS di cui il volume è membro.

È possibile analizzare i client e le relative applicazioni per determinare se i client stanno inviando più i/o del solito, il che potrebbe causare conflitti su un componente del cluster. Nella pagina Event Details (Dettagli evento), la sezione System Diagnosis (Diagnosi del sistema) visualizza i principali carichi di lavoro del volume che utilizzano il componente in conflitto. Se si conosce il client che sta accedendo a un determinato volume, è possibile accedere al client per determinare se l'hardware client o un'applicazione non funziona come previsto o sta svolgendo più lavoro del solito.

In una configurazione MetroCluster, le richieste di scrittura su un volume di un cluster locale vengono mirrorate su un volume del cluster remoto. Mantenendo il volume di origine sul cluster locale sincronizzato con il volume di destinazione sul cluster remoto, è anche possibile aumentare la domanda di entrambi i cluster nella configurazione MetroCluster. Riducendo le richieste di scrittura su questi volumi mirrorati, i cluster possono eseguire meno operazioni di sincronizzazione, riducendo così l'impatto delle performance su altri carichi di lavoro.

Verificare la presenza di problemi relativi al client o alla rete

Quando i client connessi ai volumi su un cluster aumentano le richieste di i/o, il cluster deve lavorare di più per soddisfare la domanda. L'aumento della domanda sul cluster può mettere in conflitto un componente, aumentare la latenza dei carichi di lavoro che lo utilizzano e attivare un evento in Unified Manager.

Nella pagina Event Details (Dettagli evento), la sezione System Diagnosis (Diagnosi del sistema) visualizza i principali carichi di lavoro del volume che utilizzano il componente in conflitto. Se si conosce il client che sta accedendo a un determinato volume, è possibile accedere al client per determinare se l'hardware client o un'applicazione non funziona come previsto o sta svolgendo più lavoro del solito. Potrebbe essere necessario contattare l'amministratore del client o il fornitore dell'applicazione per ricevere assistenza.

È possibile controllare l'infrastruttura di rete per determinare se sono presenti problemi hardware, colli di bottiglia o carichi di lavoro concorrenti che potrebbero aver causato un rallentamento delle prestazioni delle richieste di i/o tra il cluster e i client connessi. Potrebbe essere necessario contattare l'amministratore di rete per assistenza.

Verificare se altri volumi nel gruppo di policy QoS hanno un'attività insolitamente elevata

È possibile esaminare i carichi di lavoro nel gruppo di policy qualità del servizio (QoS) con la più alta variazione di attività per determinare se l'evento è stato causato da più di un carico di lavoro. Puoi anche vedere se altri carichi di lavoro superano ancora il limite di throughput impostato o se rientrano nell'intervallo di attività previsto.

Nella pagina Dettagli evento, nella sezione Diagnosi del sistema, è possibile ordinare i carichi di lavoro in base alla deviazione di picco nell'attività per visualizzare i carichi di lavoro con la variazione più alta nell'attività nella parte superiore della tabella. Questi carichi di lavoro potrebbero essere i "bulli" la cui attività ha superato il limite impostato e potrebbe aver causato l'evento.

È possibile accedere alla pagina workload Analysis (analisi del carico di lavoro) per ciascun workload di volume per esaminare la relativa attività IOPS. Se il carico di lavoro ha periodi di attività operative molto elevate, potrebbe aver contribuito all'evento. È possibile modificare le impostazioni del gruppo di criteri per il carico di lavoro o spostare il carico di lavoro in un altro gruppo di criteri.

È possibile utilizzare Gestione di sistema di ONTAP o i comandi dell'interfaccia utente di ONTAP per gestire i gruppi di criteri, come segue:

- Creare un gruppo di criteri.
- Aggiungere o rimuovere carichi di lavoro in un gruppo di policy.
- Spostare un carico di lavoro tra gruppi di policy.
- Modificare il limite di throughput di un gruppo di criteri.

Spostare le interfacce logiche (LIF)

Lo spostamento delle interfacce logiche (LIF) su una porta meno occupata può contribuire a migliorare il bilanciamento del carico, assistere nelle operazioni di manutenzione e di ottimizzazione delle performance e ridurre l'accesso indiretto.

L'accesso indiretto può ridurre l'efficienza del sistema. Si verifica quando un carico di lavoro di un volume utilizza nodi diversi per l'elaborazione di rete e dei dati. Per ridurre l'accesso indiretto, è possibile riorganizzare i LIF, che implica lo spostamento dei LIF per utilizzare lo stesso nodo per l'elaborazione della rete e dei dati. È possibile configurare il bilanciamento del carico in modo che ONTAP sposti automaticamente le LIF occupate su una porta diversa oppure è possibile spostare una LIF manualmente.

Benefici	Considerazioni
• Migliorare il bilanciamento del carico. • Ridurre l'accesso indiretto.	Quando si sposta una LIF connessa alle condivisioni CIFS, i client che accedono alle condivisioni CIFS vengono disconnessi. Qualsiasi richiesta di lettura o scrittura alle condivisioni CIFS viene interrotta.

I comandi ONTAP consentono di configurare il bilanciamento del carico. Per ulteriori informazioni, consultare la documentazione di rete di ONTAP.

Per spostare manualmente i file LIF, utilizzare Gestione di sistema di ONTAP e i comandi dell'interfaccia utente di ONTAP.

Eseguire operazioni di efficienza dello storage in tempi meno impegnati

È possibile modificare la policy o la pianificazione che gestisce le operazioni di efficienza dello storage da eseguire quando i carichi di lavoro dei volumi interessati sono meno occupati.

Le operazioni di efficienza dello storage possono utilizzare un'elevata quantità di risorse CPU del cluster e diventare un bullo dei volumi su cui vengono eseguite le operazioni. Se i volumi delle vittime hanno un'attività elevata contemporaneamente all'esecuzione delle operazioni di efficienza dello storage, la latenza può aumentare e attivare un evento.

Nella pagina Event Details (Dettagli evento), la sezione System Diagnosis (Diagnosi del sistema) visualizza i carichi di lavoro nel gruppo di policy QoS in base alla deviazione di picco nell'attività per identificare i carichi di lavoro ingombrati. Se nella parte superiore della tabella viene visualizzato "sTorage Efficiency" (efficienza del toraggio), queste operazioni sono in preda ai carichi di lavoro delle vittime. Modificando la policy di efficienza o

la pianificazione da eseguire quando questi carichi di lavoro sono meno occupati, è possibile evitare che le operazioni di efficienza dello storage causino conflitti su un cluster.

È possibile utilizzare Gestione di sistema di ONTAP per gestire le policy di efficienza. È possibile utilizzare i comandi ONTAP per gestire le policy e le pianificazioni di efficienza.

Qual è l'efficienza dello storage

L'efficienza dello storage consente di memorizzare la massima quantità di dati al costo più basso e di gestire una rapida crescita dei dati consumando meno spazio. La strategia di NetApp per l'efficienza dello storage si basa sulla base integrata della virtualizzazione dello storage e dello storage unificato fornita dal sistema operativo ONTAP e dal file system WAFL (Write Anywhere file Layout).

L'efficienza dello storage include l'utilizzo di tecnologie come thin provisioning, copia Snapshot, deduplica, compressione dei dati, FlexClone, Replica con risorse limitate con SnapVault e SnapMirror, RAID-DP, Flash cache, aggregato di Flash Pool e aggregati abilitati per FabricPool, che contribuiscono ad aumentare l'utilizzo dello storage e a ridurre i costi di storage.

L'architettura di storage unificata consente di consolidare in modo efficiente una SAN (Storage Area Network), NAS (Network-Attached Storage) e uno storage secondario su un'unica piattaforma.

Le unità disco ad alta densità, come le unità Serial Advanced Technology Attachment (SATA) configurate all'interno dell'aggregato Flash Pool o con Flash cache e tecnologia RAID-DP, aumentano l'efficienza senza compromettere le performance e la resilienza.

Un aggregato abilitato a FabricPool include un aggregato All SSD o HDD (a partire da ONTAP 9.8) come Tier di performance locale e un archivio di oggetti specificato come Tier cloud. La configurazione di FabricPool consente di gestire i dati del Tier storage (il Tier locale o il Tier cloud) da memorizzare in base all'accesso frequente ai dati.

Tecnologie come il thin provisioning, la copia Snapshot, la deduplica, la compressione dei dati, la replica con risorse limitate con SnapVault e il volume SnapMirror e FlexClone offrono risparmi migliori. È possibile utilizzare queste tecnologie singolarmente o insieme per ottenere la massima efficienza dello storage.

Aggiungere dischi e riallocare i dati

È possibile aggiungere dischi a un aggregato per aumentare la capacità di storage e le performance di tale aggregato. Dopo aver aggiunto i dischi, si otterrà un miglioramento delle prestazioni di lettura solo dopo aver riallocato i dati tra i dischi aggiunti.

È possibile utilizzare queste istruzioni quando Unified Manager ha ricevuto eventi aggregati attivati da soglie dinamiche o da soglie di performance definite dal sistema:

- Una volta ricevuto un evento di soglia dinamica, nella pagina Dettagli evento, l'icona del componente del cluster che rappresenta l'aggregato in conflitto viene evidenziata in rosso.

  Sotto l'icona, tra parentesi, si trova il nome dell'aggregato, che identifica l'aggregato a cui è possibile aggiungere dischi.

- Una volta ricevuto un evento di soglia definito dal sistema, nella pagina Dettagli evento, il testo della descrizione dell'evento elenca il nome dell'aggregato che ha il problema.

È possibile aggiungere dischi e riallocare i dati su questo aggregato.

I dischi aggiunti all'aggregato devono già esistere nel cluster. Se il cluster non dispone di dischi aggiuntivi, potrebbe essere necessario contattare l'amministratore o acquistare altri dischi. È possibile utilizzare Gestione di sistema di ONTAP o i comandi ONTAP per aggiungere dischi a un aggregato.

È necessario riallocare i dati solo quando si utilizzano aggregati HDD e Flash Pool. Non riallocare i dati su aggregati SSD o FabricPool.

In che modo l'attivazione di Flash cache su un nodo può migliorare le performance dei carichi di lavoro

È possibile migliorare le performance dei carichi di lavoro attivando il caching intelligente dei dati Flash cache™ su ciascun nodo del cluster.

Un modulo Flash cache, o modulo di memoria basato su PCIe Performance Acceleration Module, ottimizza le performance dei carichi di lavoro a lettura intensiva casuale, funzionando come una cache di lettura esterna intelligente. Questo hardware funziona in combinazione con il componente software WAFL External cache di ONTAP.

In Unified Manager, nella pagina Dettagli evento, l'icona del componente del cluster che rappresenta l'aggregato in conflitto viene evidenziata in rosso. Sotto l'icona, tra parentesi, si trova il nome dell'aggregato, che identifica l'aggregato. È possibile attivare Flash cache sul nodo in cui risiede l'aggregato.

È possibile utilizzare Gestione di sistema di ONTAP o i comandi ONTAP per verificare se Flash cache è installata o attivata e, se non è già attivata, attivarla. Il seguente comando indica se Flash cache è attivata su un nodo specifico: **`cluster::> run local options flexscale.enable`**

Per ulteriori informazioni su Flash cache e sui requisiti per il suo utilizzo, consulta il seguente report tecnico:

"Report tecnico 3832: Guida alle Best practice per la cache flash"

In che modo l'abilitazione di Flash Pool su un aggregato di storage può migliorare le performance dei carichi di lavoro

Puoi migliorare le performance dei carichi di lavoro attivando la funzione Flash Pool su un aggregato. Un Flash Pool è un aggregato che incorpora sia HDD che SSD. Gli HDD vengono utilizzati per lo storage primario e gli SSD forniscono una cache di lettura e scrittura dalle performance elevate per migliorare le performance aggregate.

In Unified Manager, la pagina Dettagli evento visualizza il nome dell'aggregato in conflitto. È possibile utilizzare Gestore di sistema di ONTAP o i comandi ONTAP per verificare se Flash Pool è attivato per un aggregato. Se si dispone di SSD installati, è possibile utilizzare l'interfaccia della riga di comando per attivarla. Se si dispone di SSD installati, è possibile eseguire il seguente comando sull'aggregato per verificare se Flash Pool è attivato: **`cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled`**

In questo comando, *`aggr_name`* è il nome dell'aggregato, ad esempio l'aggregato in conflitto.

Per ulteriori informazioni su Flash Pool e sui requisiti per il suo utilizzo, consulta la *Guida alla gestione dello storage fisico Clustered Data ONTAP*.

Verifica dello stato di salute della configurazione MetroCluster

È possibile utilizzare Unified Manager per esaminare lo stato dei cluster in una configurazione MetroCluster su IP o FC. Lo stato di salute e gli eventi consentono di determinare se vi sono problemi hardware o software che potrebbero influire sulle prestazioni dei carichi di lavoro.

Se si configura Unified Manager per l'invio di avvisi e-mail, è possibile controllare l'e-mail per verificare la presenza di eventuali problemi di salute sul cluster locale o remoto che potrebbero aver contribuito a un evento di performance. Nella GUI di Unified Manager, è possibile selezionare **Gestione eventi** per visualizzare un elenco degli eventi correnti, quindi utilizzare i filtri per visualizzare solo gli eventi di configurazione MetroCluster.

Per ulteriori informazioni, vedere "Verifica dello stato dei cluster in una configurazione MetroCluster"

Verifica della configurazione MetroCluster

È possibile evitare problemi di performance per i carichi di lavoro mirrorati in configurazioni MetroCluster su FC e IP, garantendo che la configurazione MetroCluster sia configurata correttamente. È inoltre possibile migliorare le performance dei carichi di lavoro modificando la configurazione o aggiornando i componenti software o hardware.

Fare riferimento a. "Documentazione MetroCluster" Per istruzioni sulla configurazione dei cluster nella configurazione MetroCluster, inclusi switch Fibre Channel (FC), cavi e ISL (Inter-Switch link). Inoltre, consente di configurare il software MetroCluster in modo che i cluster locali e remoti possano comunicare con i dati del volume mirror. Per informazioni specifiche sulla configurazione MetroCluster over IP, vedere "Installare una configurazione IP MetroCluster".

È possibile confrontare la configurazione di MetroCluster con i requisiti della "Documentazione MetroCluster" Per determinare se la modifica o l'aggiornamento dei componenti nella configurazione MetroCluster potrebbe migliorare le performance dei carichi di lavoro. Questo confronto può aiutarti a rispondere alle seguenti domande:

- I controller sono appropriati per i carichi di lavoro?
- Hai bisogno di aggiornare i bundle ISL a una larghezza di banda più ampia per gestire un throughput maggiore?
- È possibile regolare i crediti buffer-to-buffer (BBC) sugli switch per aumentare la larghezza di banda?
- Se i tuoi carichi di lavoro hanno un elevato throughput di scrittura su storage SSD (Solid state Drive), devi aggiornare i bridge FC-SAS per adattarli al throughput?

Informazioni correlate

- Per informazioni sulla sostituzione o l'aggiornamento dei componenti di MetroCluster, consultare "Documentazione MetroCluster".
- Per informazioni sull'aggiornamento dei controller, vedere "Aggiornamento dei controller in una configurazione MetroCluster FC mediante switchover e switchback" e. "Aggiornamento dei controller in una configurazione MetroCluster IP mediante switchover e switchback"

Spostamento dei carichi di lavoro in un aggregato diverso

È possibile utilizzare Unified Manager per identificare un aggregato meno occupato rispetto all'aggregato in cui risiedono attualmente i carichi di lavoro, quindi è possibile spostare volumi o LUN selezionati in tale aggregato. Lo spostamento di carichi di lavoro dalle performance elevate in un aggregato meno occupato o in un aggregato con storage flash abilitato consente al carico di lavoro di funzionare in modo più efficiente.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- È necessario aver registrato il nome dell'aggregato che ha attualmente un problema di performance.
- È necessario aver registrato la data e l'ora in cui l'aggregato ha ricevuto l'evento.
- Unified Manager deve aver raccolto e analizzato almeno un mese di dati relativi alle performance.

Questi passaggi ti aiutano a identificare le seguenti risorse in modo da poter spostare i carichi di lavoro dalle performance elevate verso un aggregato meno utilizzato:

- Gli aggregati sullo stesso cluster meno utilizzati
- I volumi dalle performance più elevate dell'aggregato corrente

Fasi

1. Identificare l'aggregato nel cluster meno utilizzato:
   a. Nella pagina dei dettagli **evento**, fare clic sul nome del cluster in cui risiede l'aggregato.

      I dettagli del cluster vengono visualizzati nella pagina Landing di Performance/Cluster.

   b. Nella pagina **Riepilogo**, fare clic su **aggregati** dal riquadro **oggetti gestiti**.

      Viene visualizzato l'elenco degli aggregati in questo cluster.

   c. Fare clic sulla colonna **Utilization** (utilizzo) per ordinare gli aggregati in base al minor utilizzo.

      È inoltre possibile identificare gli aggregati che hanno la capacità massima * libera*. In questo modo viene fornito un elenco di potenziali aggregati in cui è possibile spostare i carichi di lavoro.

   d. Annotare il nome dell'aggregato in cui si desidera spostare i carichi di lavoro.
2. Identificare i volumi dalle performance elevate dell'aggregato che ha ricevuto l'evento:
   a. Fare clic sull'aggregato che presenta problemi di performance.

      I dettagli dell'aggregato vengono visualizzati nella pagina Performance/aggregate Explorer (Esplora prestazioni/aggregato).

   b. Dal selettore **intervallo di tempo**, selezionare **ultimi 30 giorni**, quindi fare clic su **Applica intervallo**.

      In questo modo è possibile visualizzare una cronologia delle performance più lunga rispetto alle 72 ore predefinite. Si desidera spostare un volume che utilizza molte risorse in modo coerente, non solo nelle ultime 72 ore.

   c. Dal controllo **View and compare**, selezionare **Volumes on this aggregate** (volumi su questo

aggregato).

Viene visualizzato un elenco di volumi FlexVol e volumi FlexGroup costitutivi su questo aggregato.

d. Ordinare i volumi in base ai MB/s più elevati, quindi in base agli IOPS più elevati, per visualizzare i volumi con le performance più elevate.

e. Annotare i nomi dei volumi che si desidera spostare in un aggregato diverso.

3. Sposta i volumi dalle performance elevate nell'aggregato identificato come a basso utilizzo.

È possibile eseguire l'operazione di spostamento utilizzando Gestione sistema di ONTAP, OnCommand Workflow Automation, comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, verificare se si stanno ricevendo lo stesso tipo di eventi da questo nodo o aggregato.

Spostamento dei carichi di lavoro in un nodo diverso

È possibile utilizzare Unified Manager per identificare un aggregato su un nodo diverso meno occupato rispetto al nodo su cui sono attualmente in esecuzione i carichi di lavoro, quindi è possibile spostare i volumi selezionati in tale aggregato. Lo spostamento di carichi di lavoro dalle performance elevate in un aggregato su un nodo meno occupato consente ai carichi di lavoro su entrambi i nodi di funzionare in modo più efficiente.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- È necessario aver registrato il nome del nodo che sta riscontrando un problema di performance.
- È necessario aver registrato la data e l'ora in cui il nodo ha ricevuto l'evento di performance.
- Unified Manager deve aver raccolto e analizzato i dati delle performance per un mese o più.

Questa procedura consente di identificare le seguenti risorse in modo da spostare i carichi di lavoro dalle performance elevate in un nodo meno utilizzato:

- I nodi dello stesso cluster che hanno la maggiore capacità di performance libera
- Gli aggregati del nuovo nodo che hanno la maggiore capacità di performance libera
- I volumi dalle performance più elevate sul nodo corrente

Fasi

1. Identificare un nodo nel cluster che abbia la capacità di performance libera più elevata:
   a. Nella pagina **Dettagli evento**, fare clic sul nome del cluster in cui risiede il nodo.

      I dettagli del cluster vengono visualizzati nella pagina Landing di Performance/Cluster.

   b. Nella scheda **Riepilogo**, fare clic su **nodi** dal riquadro **oggetti gestiti**.

      Viene visualizzato l'elenco dei nodi di questo cluster.

   c. Fare clic sulla colonna **Performance Capacity used** per ordinare i nodi in base alla percentuale minima utilizzata.

In questo modo viene fornito un elenco dei nodi potenziali in cui è possibile spostare i carichi di lavoro.

d. Annotare il nome del nodo in cui si desidera spostare i carichi di lavoro.

2. Identificare un aggregato sul nuovo nodo meno utilizzato:
   a. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates** e selezionare **Performance** > **All Aggregates** dal menu View.

      Viene visualizzata la vista Performance: All aggregates (prestazioni: Tutti gli aggregati).

   b. Fare clic su **Filtering**, selezionare **Node** dal menu a discesa a sinistra, digitare il nome del nodo nel campo di testo, quindi fare clic su **Apply Filter** (Applica filtro).

      La vista Performance: All aggregates (prestazioni: Tutti gli aggregati) viene visualizzata nuovamente con l'elenco degli aggregati disponibili su questo nodo.

   c. Fare clic sulla colonna **Performance Capacity used** (capacità di performance utilizzata) per ordinare gli aggregati in base ai dati meno utilizzati.

      In questo modo viene fornito un elenco di potenziali aggregati in cui è possibile spostare i carichi di lavoro.

   d. Annotare il nome dell'aggregato in cui si desidera spostare i carichi di lavoro.
3. Identificare i carichi di lavoro dalle performance elevate dal nodo che ha ricevuto l'evento:
   a. Torna alla pagina **Dettagli evento** per l'evento.
   b. Nel campo **volumi interessati**, fare clic sul collegamento relativo al numero di volumi.

      La vista Performance: All Volumes (prestazioni: Tutti i volumi) viene visualizzata con un elenco filtrato dei volumi su quel nodo.

   c. Fare clic sulla colonna **capacità totale** per ordinare i volumi in base allo spazio allocato più grande.

      In questo modo viene visualizzato un elenco dei volumi potenziali che si desidera spostare.

   d. Annotare i nomi dei volumi che si desidera spostare e i nomi degli aggregati correnti in cui risiedono.
4. Sposta i volumi negli aggregati identificati come dotati di capacità di performance massima sul nuovo nodo.

   È possibile eseguire l'operazione di spostamento utilizzando Gestione sistema di ONTAP, OnCommand Workflow Automation, comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, è possibile verificare se si stanno ricevendo lo stesso tipo di eventi da questo nodo o aggregato.

Spostamento dei carichi di lavoro in un aggregato su un nodo diverso

È possibile utilizzare Unified Manager per identificare un aggregato su un nodo diverso meno occupato rispetto al nodo in cui sono attualmente in esecuzione i carichi di lavoro, quindi è possibile spostare volumi selezionati in tale aggregato. Lo spostamento di carichi di lavoro dalle performance elevate in un aggregato su un nodo meno occupato consente ai carichi di lavoro su entrambi i nodi di funzionare in modo più efficiente.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- È necessario aver registrato il nome del nodo che sta riscontrando un problema di performance.
- È necessario aver registrato la data e l'ora in cui il nodo ha ricevuto l'evento di performance.
- Unified Manager deve aver raccolto e analizzato almeno un mese di dati relativi alle performance.

Questi passaggi consentono di identificare le seguenti risorse in modo da poter spostare i carichi di lavoro dalle performance elevate in un nodo meno utilizzato:

- I nodi dello stesso cluster meno utilizzati
- Gli aggregati sul nuovo nodo che sono i meno utilizzati
- I volumi dalle performance più elevate sul nodo corrente

Fasi

1. Identificare un nodo nel cluster meno utilizzato:
   a. Nella pagina dei dettagli **evento**, fare clic sul nome del cluster in cui risiede il nodo.

      I dettagli del cluster vengono visualizzati nella pagina Landing di Performance/Cluster.

   b. Nella pagina **Riepilogo**, fare clic su **nodi** dal riquadro **oggetti gestiti**.

      Viene visualizzato l'elenco dei nodi di questo cluster.

   c. Fare clic sulla colonna **Utilization** (utilizzo) per ordinare i nodi in base ai meno utilizzati.

      È inoltre possibile identificare i nodi che hanno la capacità massima * libera*. In questo modo viene fornito un elenco dei nodi potenziali in cui è possibile spostare i carichi di lavoro.

   d. Annotare il nome del nodo in cui si desidera spostare i carichi di lavoro.
2. Identificare un aggregato sul nuovo nodo meno utilizzato:
   a. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates** e selezionare **Performance** > **All Aggregates** dal menu View.

      Viene visualizzata la vista Performance: All aggregates (prestazioni: Tutti gli aggregati).

   b. Fare clic su **Filtering**, selezionare **Node** dal menu a discesa a sinistra, digitare il nome del nodo nel campo di testo, quindi fare clic su **Apply Filter** (Applica filtro).

      La vista Performance: All aggregates (prestazioni: Tutti gli aggregati) viene visualizzata nuovamente con l'elenco degli aggregati disponibili su questo nodo.

   c. Fare clic sulla colonna **Utilization** (utilizzo) per ordinare gli aggregati in base al minor utilizzo.

      È inoltre possibile identificare gli aggregati che hanno la capacità massima * libera*. In questo modo viene fornito un elenco di potenziali aggregati in cui è possibile spostare i carichi di lavoro.

   d. Annotare il nome dell'aggregato in cui si desidera spostare i carichi di lavoro.
3. Identificare i carichi di lavoro dalle performance elevate dal nodo che ha ricevuto l'evento:

a. Torna alla pagina dei dettagli **evento** per l'evento.
b. Nel campo **volumi interessati**, fare clic sul collegamento relativo al numero di volumi.

   La vista Performance: All Volumes (prestazioni: Tutti i volumi) viene visualizzata con un elenco filtrato dei volumi su quel nodo.

c. Fare clic sulla colonna **capacità totale** per ordinare i volumi in base allo spazio allocato più grande.

   In questo modo viene visualizzato un elenco dei volumi potenziali che si desidera spostare.

d. Annotare i nomi dei volumi che si desidera spostare e i nomi degli aggregati correnti in cui risiedono.

4. Spostare i volumi negli aggregati identificati come a basso utilizzo sul nuovo nodo.

   È possibile eseguire l'operazione di spostamento utilizzando Gestione sistema di ONTAP, OnCommand Workflow Automation, comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, verificare se si stanno ricevendo lo stesso tipo di eventi da questo nodo o aggregato.

Spostamento dei carichi di lavoro in un nodo di una coppia ha diversa

È possibile utilizzare Unified Manager per identificare un aggregato su un nodo in una coppia di ha (High Availability) diversa che ha una capacità di performance libera maggiore rispetto alla coppia di ha in cui i carichi di lavoro sono attualmente in esecuzione. Quindi, è possibile spostare i volumi selezionati negli aggregati della nuova coppia ha.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Il cluster deve essere composto da almeno due coppie ha

  Non è possibile utilizzare questo processo di correzione se nel cluster è presente una sola coppia ha.

- È necessario aver registrato i nomi dei due nodi della coppia ha che attualmente presentano un problema di performance.
- È necessario aver registrato la data e l'ora in cui i nodi hanno ricevuto l'evento di performance.
- Unified Manager deve aver raccolto e analizzato i dati delle performance per un mese o più.

Lo spostamento di carichi di lavoro dalle performance elevate in un aggregato su un nodo con una maggiore capacità di performance libera consente ai carichi di lavoro su entrambi i nodi di funzionare in modo più efficiente. Questa procedura consente di identificare le seguenti risorse in modo da poter spostare i carichi di lavoro dalle performance elevate in un nodo con una capacità di performance più libera su una coppia ha diversa:

- I nodi di una coppia ha diversa sullo stesso cluster che hanno la massima capacità di performance libera
- Gli aggregati sui nuovi nodi che hanno la maggiore capacità di performance libera
- I volumi dalle performance più elevate sui nodi correnti

Fasi

1. Identificare i nodi che fanno parte di una coppia ha diversa sullo stesso cluster:
   a. Nella pagina **Dettagli evento**, fare clic sul nome del cluster su cui risiedono i nodi.

      I dettagli del cluster vengono visualizzati nella pagina Landing di Performance/Cluster.

   b. Nella pagina **Riepilogo**, fare clic su **nodi** dal riquadro **oggetti gestiti**.

      L'elenco dei nodi di questo cluster viene visualizzato nella vista Performance: All Nodes (prestazioni: Tutti i nodi).

   c. Annotare i nomi dei nodi che si trovano in diverse coppie ha rispetto alla coppia ha che attualmente presenta un problema di performance.
2. Identificare un nodo della nuova coppia ha con la massima capacità di performance libera:
   a. Nella vista **Performance: All Nodes** (prestazioni: Tutti i nodi), fare clic sulla colonna **Performance Capacity used** (capacità di performance utilizzata) per ordinare i nodi in base alla percentuale minima utilizzata.

      In questo modo viene fornito un elenco dei nodi potenziali in cui è possibile spostare i carichi di lavoro.

   b. Annotare il nome del nodo su una coppia ha diversa in cui si desidera spostare i carichi di lavoro.
3. Identifica un aggregato sul nuovo nodo che ha la maggiore capacità di performance libera:
   a. Nella vista **Performance: All Nodes** (prestazioni: Tutti i nodi), fare clic sul nodo.

      I dettagli del nodo vengono visualizzati nella pagina Performance/Node Explorer (Esplora prestazioni/nodo).

   b. Nel menu **Visualizza e confronta**, selezionare **aggregati su questo nodo**.

      Gli aggregati su questo nodo vengono visualizzati nella griglia.

   c. Fare clic sulla colonna **Performance Capacity used** (capacità di performance utilizzata) per ordinare gli aggregati in base ai dati meno utilizzati.

      In questo modo viene fornito un elenco di potenziali aggregati in cui è possibile spostare i carichi di lavoro.

   d. Annotare il nome dell'aggregato in cui si desidera spostare i carichi di lavoro.
4. Identificare i carichi di lavoro dalle performance elevate dei nodi che hanno ricevuto l'evento:
   a. Torna alla pagina dei dettagli **evento** per l'evento.
   b. Nel campo **volumi interessati**, fare clic sul collegamento relativo al numero di volumi per il primo nodo.

      La vista Performance: All Volumes (prestazioni: Tutti i volumi) viene visualizzata con un elenco filtrato dei volumi su quel nodo.

   c. Fare clic sulla colonna **capacità totale** per ordinare i volumi in base allo spazio allocato più grande.

      In questo modo viene visualizzato un elenco dei volumi potenziali che si desidera spostare.

   d. Annotare i nomi dei volumi che si desidera spostare e i nomi degli aggregati correnti in cui risiedono.
   e. Eseguire i passaggi 4c e 4d per il secondo nodo che faceva parte di questo evento per identificare

anche i volumi che si desidera spostare da quel nodo.

5. Sposta i volumi negli aggregati identificati come dotati di capacità di performance massima sul nuovo nodo.

   È possibile eseguire l'operazione di spostamento utilizzando Gestione sistema di ONTAP, OnCommand Workflow Automation, comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, è possibile verificare se si stanno ricevendo lo stesso tipo di eventi da questo nodo o aggregato.

Spostamento dei carichi di lavoro in un altro nodo di una coppia ha diversa

È possibile utilizzare Unified Manager per identificare un aggregato su un nodo in una coppia ha diversa che è meno occupata della coppia ha in cui i carichi di lavoro sono attualmente in esecuzione. Quindi, è possibile spostare i volumi selezionati negli aggregati della nuova coppia ha. Lo spostamento di carichi di lavoro dalle performance elevate in un aggregato su un nodo meno occupato consente ai carichi di lavoro su entrambi i nodi di funzionare in modo più efficiente.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Il cluster deve essere composto da almeno due coppie ha; non è possibile utilizzare questo processo di correzione se nel cluster è presente una sola coppia ha.
- È necessario aver registrato i nomi dei due nodi della coppia ha che presentano attualmente un problema di performance.
- È necessario aver registrato la data e l'ora in cui i nodi hanno ricevuto l'evento di performance.
- Unified Manager deve aver raccolto e analizzato almeno un mese di dati relativi alle performance.

Questi passaggi consentono di identificare le seguenti risorse in modo da poter spostare carichi di lavoro dalle performance elevate in un nodo meno utilizzato su una coppia ha diversa:

- I nodi in una coppia ha diversa sullo stesso cluster che sono meno utilizzati
- Gli aggregati sui nuovi nodi che sono i meno utilizzati
- I volumi dalle performance più elevate sui nodi correnti

Fasi

1. Identificare i nodi che fanno parte di una coppia ha diversa sullo stesso cluster:
   a. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Clusters** e selezionare **Performance** > **All Clusters** dal menu View.

      Viene visualizzata la vista Performance: All Clusters (prestazioni: Tutti i cluster).

   b. Fare clic sul numero nel campo **Node Count** del cluster corrente.

      Viene visualizzata la vista Performance: All Nodes (prestazioni: Tutti i nodi).

   c. Annotare i nomi dei nodi che si trovano in diverse coppie ha rispetto alla coppia ha che attualmente

presenta un problema di performance.

2. Identificare un nodo della nuova coppia ha meno utilizzato:
   a. Fare clic sulla colonna **Utilization** (utilizzo) per ordinare i nodi in base ai meno utilizzati.

      È inoltre possibile identificare i nodi che hanno la capacità massima * libera*. In questo modo viene fornito un elenco dei nodi potenziali in cui è possibile spostare i carichi di lavoro.

   b. Annotare il nome del nodo in cui si desidera spostare i carichi di lavoro.
3. Identificare un aggregato sul nuovo nodo meno utilizzato:
   a. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates** e selezionare **Performance** > **All Aggregates** dal menu View.

      Viene visualizzata la vista Performance: All aggregates (prestazioni: Tutti gli aggregati).

   b. Fare clic su **Filtering**, selezionare **Node** dal menu a discesa a sinistra, digitare il nome del nodo nel campo di testo, quindi fare clic su **Apply Filter** (Applica filtro).

      La vista Performance: All aggregates (prestazioni: Tutti gli aggregati) viene visualizzata nuovamente con l'elenco degli aggregati disponibili su questo nodo.

   c. Fare clic sulla colonna **Utilization** (utilizzo) per ordinare gli aggregati in base al minor utilizzo.

      È inoltre possibile identificare gli aggregati che hanno la capacità massima * libera*. In questo modo viene fornito un elenco di potenziali aggregati in cui è possibile spostare i carichi di lavoro.

   d. Annotare il nome dell'aggregato in cui si desidera spostare i carichi di lavoro.
4. Identificare i carichi di lavoro dalle performance elevate dei nodi che hanno ricevuto l'evento:
   a. Torna alla pagina dei dettagli **evento** per l'evento.
   b. Nel campo **volumi interessati**, fare clic sul collegamento relativo al numero di volumi per il primo nodo.

      La vista Performance: All Volumes (prestazioni: Tutti i volumi) viene visualizzata con un elenco filtrato dei volumi su quel nodo.

   c. Fare clic sulla colonna **capacità totale** per ordinare i volumi in base allo spazio allocato più grande.

      In questo modo viene visualizzato un elenco dei volumi potenziali che si desidera spostare.

   d. Annotare i nomi dei volumi che si desidera spostare e i nomi degli aggregati correnti in cui risiedono.
   e. Eseguire i passaggi 4c e 4d per il secondo nodo che faceva parte di questo evento per identificare anche i volumi che si desidera spostare da quel nodo.
5. Spostare i volumi negli aggregati identificati come a basso utilizzo sul nuovo nodo.

   È possibile eseguire l'operazione di spostamento utilizzando Gestione sistema di ONTAP, OnCommand Workflow Automation, comandi ONTAP o una combinazione di questi strumenti.

Dopo alcuni giorni, verificare se si stanno ricevendo lo stesso tipo di eventi da questo nodo o aggregato.

Utilizzare le impostazioni dei criteri QoS per assegnare priorità al lavoro su questo nodo

È possibile impostare un limite su un gruppo di criteri QoS per controllare il limite di throughput di i/o al secondo (IOPS) o Mbps per i carichi di lavoro in esso contenuti. Se i carichi di lavoro si trovano in un gruppo di policy senza limiti impostati, ad esempio il gruppo di policy predefinito, o se il limite impostato non soddisfa le esigenze, è possibile aumentare il limite impostato o spostare i carichi di lavoro in un gruppo di policy nuovo o esistente con il limite desiderato.

Se un evento di performance su un nodo è causato da un eccessivo utilizzo delle risorse del nodo da parte dei carichi di lavoro, la descrizione dell'evento nella pagina Dettagli evento visualizza un collegamento all'elenco dei volumi coinvolti. Nella pagina Performance/Volumes (prestazioni/volumi), è possibile ordinare i volumi interessati in base a IOPS e Mbps per vedere quali carichi di lavoro hanno il massimo utilizzo che potrebbe aver contribuito all'evento.

Assegnando i volumi che stanno utilizzando in eccesso le risorse del nodo a un'impostazione di gruppo di criteri più restrittiva, il gruppo di criteri limita i carichi di lavoro per limitare la loro attività, riducendo così l'utilizzo delle risorse su quel nodo.

È possibile utilizzare Gestione di sistema di ONTAP o i comandi ONTAP per gestire i gruppi di criteri, incluse le seguenti attività:

- Creazione di un gruppo di criteri
- Aggiunta o rimozione di workload in un gruppo di policy
- Spostamento di un workload tra gruppi di policy
- Modifica del limite di throughput di un gruppo di criteri

Rimuovere volumi e LUN inattivi

Una volta identificato lo spazio libero aggregato come un problema, è possibile cercare volumi e LUN inutilizzati ed eliminarli dall'aggregato. Questo può aiutare a ridurre il problema dello spazio su disco insufficiente.

Se un evento di performance su un aggregato è causato da uno spazio su disco insufficiente, esistono alcuni modi per determinare quali volumi e LUN non vengono più utilizzati.

Per identificare i volumi inutilizzati:

- Nella pagina Dettagli evento, il campo **Conteggio oggetti interessati** fornisce un collegamento che visualizza l'elenco dei volumi interessati.

  Fare clic sul collegamento per visualizzare i volumi nella vista Performance: All Volumes (prestazioni: Tutti i volumi). Da qui è possibile ordinare i volumi interessati in base a **IOPS** per vedere quali volumi non sono stati attivi.

Per identificare le LUN inutilizzate:

1. Nella pagina Dettagli evento, annotare il nome dell'aggregato in cui si è verificato l'evento.
2. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **LUN** e selezionare **Performance** > **All LUN**

dal menu View.

3. Fare clic su **Filtering**, selezionare **aggregate** dal menu a discesa a sinistra, digitare il nome dell'aggregato nel campo di testo, quindi fare clic su **Apply Filter** (Applica filtro).
4. Ordinare l'elenco risultante dei LUN interessati in base a **IOPS** per visualizzare i LUN non attivi.

Una volta identificati i volumi e le LUN inutilizzati, è possibile utilizzare Gestione di sistema di ONTAP o i comandi ONTAP per eliminare tali oggetti.

Aggiungere dischi ed eseguire la ricostruzione del layout aggregato

È possibile aggiungere dischi a un aggregato per aumentare la capacità di storage e le performance di tale aggregato. Dopo aver aggiunto i dischi, si vede un miglioramento delle performance solo dopo la ricostruzione dell'aggregato.

Quando si riceve un evento di soglia definito dal sistema nella pagina Dettagli evento, il testo della descrizione dell'evento elenca il nome dell'aggregato che ha il problema. È possibile aggiungere dischi e ricostruire i dati su questo aggregato.

I dischi aggiunti all'aggregato devono già esistere nel cluster. Se il cluster non dispone di dischi aggiuntivi, potrebbe essere necessario contattare l'amministratore o acquistare altri dischi. È possibile utilizzare Gestione di sistema di ONTAP o i comandi ONTAP per aggiungere dischi a un aggregato.

"Report tecnico 3838: Guida alla configurazione del sottosistema di storage"

Impostazione di una connessione tra un server Unified Manager e un provider di dati esterno

La connessione tra un server Unified Manager e un provider di dati esterno consente di inviare i dati delle performance del cluster a un server esterno in modo che i responsabili dello storage possano tracciare le metriche delle performance utilizzando software di terze parti.

La connessione tra un server Unified Manager e un provider di dati esterno viene stabilita tramite l'opzione di menu "External Data Provider" nella console di manutenzione.

Dati sulle performance che possono essere inviati a un server esterno

Unified Manager raccoglie una vasta gamma di dati sulle performance da tutti i cluster monitorati. È possibile inviare gruppi specifici di dati a un server esterno.

A seconda dei dati delle performance che si desidera inserire nel grafico, è possibile scegliere di inviare uno dei seguenti gruppi di statistiche:

Gruppo di statistiche	Dati inclusi	Dettagli
Monitor delle performance	Statistiche delle performance di alto livello per i seguenti oggetti: • LUN • Volumi	Questo gruppo fornisce IOPS totali o latenza per tutte le LUN e i volumi in tutti i cluster monitorati. Questo gruppo fornisce il minor numero di statistiche.
Utilizzo delle risorse	Statistiche di utilizzo delle risorse per i seguenti oggetti: • Nodi • Aggregati	Questo gruppo fornisce le statistiche di utilizzo per il nodo e le risorse fisiche aggregate in tutti i cluster monitorati. Fornisce inoltre le statistiche raccolte nel gruppo Performance Monitor.
Analisi dettagliata	Statistiche di lettura/scrittura e per protocollo di basso livello per tutti gli oggetti monitorati: • Nodi • Aggregati • LUN • Volumi • Dischi • LIF • Porte/NIC	Questo gruppo fornisce i guasti in lettura/scrittura e per protocollo per tutti e sette i tipi di oggetti monitorati in tutti i cluster monitorati. Fornisce inoltre le statistiche raccolte nel gruppo Performance Monitor e nel gruppo Resource Utilization. Questo gruppo fornisce il maggior numero di statistiche.

Se il nome di un cluster, o oggetto cluster, viene modificato nel sistema di storage, sia il vecchio che il nuovo oggetto conterranno i dati sulle prestazioni sul server esterno (chiamato "percorso_elettronico `m`"). I due oggetti non sono correlati allo stesso oggetto. Ad esempio, se si modifica il nome di un volume da “volume1_acct” a “acct_vol1”, verranno visualizzati i vecchi dati sulle prestazioni del volume precedente e i nuovi dati sulle prestazioni del nuovo volume.

Consultare l’articolo della Knowledge base 30096 per l’elenco di tutti i contatori delle prestazioni che possono essere inviati a un provider di dati esterno.

"Contatori delle prestazioni di Unified Manager che possono essere esportati in un provider di dati esterno"

Impostazione di Graphite per ricevere i dati sulle performance da Unified Manager

Graphite è uno strumento software aperto per la raccolta e la rappresentazione grafica dei dati delle performance dai sistemi informatici. Il server e il software Graphite devono essere configurati correttamente per ricevere dati statistici da Unified Manager.

NetApp non verifica o verifica versioni specifiche di Graphite o di altri strumenti di terze parti.

Dopo aver installato Graphite in base alle istruzioni di installazione, è necessario apportare le seguenti modifiche per supportare il trasferimento dei dati statistici da Unified Manager:

- In `/opt/graphite/conf/carbon.conf` File, il numero massimo di file che è possibile creare sul server Graphite al minuto deve essere impostato su *200* (**`MAX_CREATES_PER_MINUTE = 200`**).

  A seconda del numero di cluster nella configurazione e degli oggetti delle statistiche selezionati per l'invio, potrebbero essere necessari migliaia di nuovi file da creare inizialmente. Con 200 file al minuto potrebbero essere necessari 15 minuti o più prima che tutti i file metrici vengano creati inizialmente. Una volta creati tutti i file di metriche univoci, questo parametro non è più rilevante.

- Se si esegue Graphite su un server distribuito utilizzando un indirizzo IPv6, il valore di LINE_RECEIVER_INTERFACE in `/opt/graphite/conf/carbon.conf` il file deve essere modificato da "0.0.0.0" a "::" (**`LINE_RECEIVER_INTERFACE = ::`**)
- In `/opt/graphite/conf/storage-schemas.conf` file, il `retentions` il parametro deve essere utilizzato per impostare la frequenza su 5 minuti e il periodo di conservazione sul numero di giorni rilevanti per l'ambiente.

  Il periodo di conservazione può essere lungo quanto consentito dall'ambiente, ma il valore della frequenza deve essere impostato su 5 minuti per almeno un'impostazione di conservazione. Nell'esempio seguente, viene definita una sezione per Unified Manager utilizzando `pattern` e i valori impostano la frequenza iniziale su 5 minuti e il periodo di conservazione su 100 giorni: **`[OPM]`**

  ```
  pattern = ^netapp-performance\..

  retentions = 5m:100d
  ```

  > Se il tag vendor predefinito viene modificato da "netapp-performance" a qualcosa di diverso, tale modifica deve essere riflessa in `pattern` anche il parametro.

> Se il server Graphite non è disponibile quando il server Unified Manager tenta di inviare i dati relativi alle prestazioni, i dati non vengono inviati e i dati raccolti non sono presenti.

Configurazione di una connessione da un server Unified Manager a un provider di dati esterno

Unified Manager può inviare i dati delle performance del cluster a un server esterno. È possibile specificare il tipo di dati statistici inviati e l'intervallo di invio dei dati.

Cosa ti serve

- È necessario disporre di un ID utente autorizzato per accedere alla console di manutenzione del server Unified Manager.
- È necessario disporre delle seguenti informazioni sul provider di dati esterno:
  - Nome del server o indirizzo IP (IPv4 o IPv6)
  - Porta predefinita del server (se non si utilizza la porta predefinita 2003)
- È necessario aver configurato il server remoto e il software di terze parti in modo che possa ricevere dati statistici dal server Unified Manager.
- È necessario sapere quale gruppo di statistiche si desidera inviare:

- PERFORMANCE_INDICATOR: Statistiche del monitor delle performance
- RESOURCE_UTILIZATION: Statistiche di monitoraggio dell'utilizzo delle risorse e delle performance
- DRILL_DOWN: Tutte le statistiche

- È necessario conoscere l'intervallo di tempo in cui si desidera trasmettere le statistiche: 5, 10 o 15 minuti

  Per impostazione predefinita, Unified Manager raccoglie le statistiche a intervalli di 5 minuti. Se si imposta l'intervallo di trasmissione su 10 (o 15) minuti, la quantità di dati inviati durante ciascuna trasmissione è due (o tre) volte maggiore rispetto all'intervallo predefinito di 5 minuti.

  Se si modifica l'intervallo di raccolta delle prestazioni di Unified Manager su 10 o 15 minuti, è necessario modificare l'intervallo di trasmissione in modo che sia uguale o superiore all'intervallo di raccolta di Unified Manager.

È possibile configurare una connessione tra un server Unified Manager e un server del provider di dati esterno.

Fasi

1. Accedere come utente di manutenzione alla console di manutenzione del server Unified Manager.

   Vengono visualizzati i prompt della console di manutenzione di Unified Manager.

2. Nella console di manutenzione, digitare il numero dell'opzione di menu **External Data Provider**.

   Viene visualizzato il menu connessione server esterno.

3. Digitare il numero dell'opzione di menu **Aggiungi/Modifica connessione server**.

   Vengono visualizzate le informazioni correnti sulla connessione al server.

4. Quando richiesto, digitare `y` per continuare.
5. Quando richiesto, inserire l'indirizzo IP o il nome del server di destinazione e le informazioni sulla porta del server (se diversa dalla porta predefinita 2003).
6. Quando richiesto, digitare `y` per verificare che le informazioni immesse siano corrette.
7. Premere un tasto qualsiasi per tornare al menu connessione server esterno.
8. Digitare il numero dell'opzione di menu **Modify Server Configuration** (Modifica configurazione server).

   Vengono visualizzate le informazioni di configurazione del server corrente.

9. Quando richiesto, digitare `y` per continuare.
10. Quando richiesto, inserire il tipo di statistiche da inviare, l'intervallo di tempo in cui le statistiche vengono inviate e se si desidera attivare la trasmissione delle statistiche:

Per..	Inserisci…
ID gruppo statistiche	`0` - PERFORMANCE_INDICATOR (predefinito) `1` - RESOURCE_UTILIZATION `2` - DRILL_DOWN

Per..	Inserisci…
Tag del vendor	Un nome descrittivo per la cartella in cui verranno memorizzate le statistiche sul server esterno. “netapp-performance” è il nome predefinito, ma è possibile immettere un altro valore. Utilizzando la notazione con punti è possibile definire una struttura gerarchica di cartelle. Ad esempio, immettendo **`stats.performance.netapp`** le statistiche si trovano in **stats** > **performance** > **netapp**.
Intervallo di trasmissione	**`5`** (impostazione predefinita), **`10`**, o. **`15`** minuti
Attiva/disattiva	**`0`** - Disable (Disattiva) **`1`** - Enable (attiva) (impostazione predefinita)

11. Quando richiesto, digitare **`y`** per verificare che le informazioni immesse siano corrette.
12. Premere un tasto qualsiasi per tornare al menu connessione server esterno.
13. Tipo **`x`** per uscire dalla console di manutenzione.

Una volta configurata la connessione, i dati delle prestazioni selezionati vengono inviati al server di destinazione all’intervallo di tempo specificato. Sono necessari alcuni minuti prima che le metriche inizino a comparire nello strumento esterno. Potrebbe essere necessario aggiornare il browser per visualizzare le nuove metriche nella gerarchia delle metriche.

Monitorare e gestire lo stato dei cluster

Introduzione al monitoraggio dello stato di salute di Active IQ Unified Manager

Active IQ Unified Manager (in precedenza Unified Manager di OnCommand) consente di monitorare un gran numero di sistemi che eseguono il software ONTAP attraverso un'interfaccia utente centralizzata. L'infrastruttura server di Unified Manager offre scalabilità, supportabilità e funzionalità avanzate di monitoraggio e notifica.

Le funzionalità chiave di Unified Manager includono il monitoraggio, gli avvisi, la gestione della disponibilità e della capacità dei cluster, la gestione delle funzionalità di protezione e il raggruppamento dei dati diagnostici e l'invio al supporto tecnico.

È possibile utilizzare Unified Manager per monitorare i cluster. Quando si verificano problemi nel cluster, Unified Manager notifica all'utente i dettagli di tali problemi attraverso gli eventi. Alcuni eventi forniscono anche un'azione correttiva che è possibile intraprendere per risolvere i problemi. È possibile configurare gli avvisi per gli eventi in modo che, quando si verificano problemi, si riceva una notifica tramite e-mail e trap SNMP.

È possibile utilizzare Unified Manager per gestire gli oggetti di storage nel proprio ambiente associandoli alle annotazioni. È possibile creare annotazioni personalizzate e associare dinamicamente cluster, storage virtual machine (SVM) e volumi con le annotazioni attraverso le regole.

È inoltre possibile pianificare i requisiti di storage degli oggetti cluster utilizzando le informazioni fornite nei grafici di capacità e integrità per il rispettivo oggetto cluster.

Capacità fisica e logica

Unified Manager utilizza i concetti di spazio fisico e logico utilizzati per gli oggetti di storage ONTAP.

- Capacità fisica: Lo spazio fisico si riferisce ai blocchi fisici di storage utilizzati nel volume. La "capacità fisica utilizzata" è generalmente inferiore alla capacità logica utilizzata a causa della riduzione dei dati dalle funzionalità di efficienza dello storage (come deduplica e compressione).
- Capacità logica: Lo spazio logico si riferisce allo spazio utilizzabile (i blocchi logici) in un volume. Lo spazio logico si riferisce al modo in cui lo spazio teorico può essere utilizzato, senza tenere conto dei risultati della deduplica o della compressione. "Spazio logico utilizzato" è lo spazio fisico utilizzato e i risparmi derivanti dalle funzionalità di efficienza dello storage (come deduplica e compressione) configurate. Questa misurazione appare spesso più grande della capacità fisica utilizzata perché include copie Snapshot, cloni e altri componenti e non riflette la compressione dei dati e altre riduzioni dello spazio fisico. Pertanto, la capacità logica totale potrebbe essere superiore allo spazio fornito.

Unità di misura della capacità

Unified Manager calcola la capacità dello storage in base a unità binarie di 1024 (2^{10}) byte. In ONTAP 9.10.0 e versioni precedenti, queste unità venivano visualizzate come KB, MB, GB, TB e PB. A partire da ONTAP 9.10.1, vengono visualizzati in Unified Manager come KiB, MiB, GiB, TIB e PIB.

Le unità utilizzate per il throughput continuano a essere kilobyte per secondo (Kbps), Megabyte per secondo (Mbps), Gigabyte per secondo (Gbps) o terabyte per secondo (Tbps) e così via, per tutte le versioni di ONTAP.

Unità di capacità visualizzata in Unified Manager per ONTAP 9.10.0 e versioni precedenti	Unità di capacità visualizzata in Unified Manager per ONTAP 9.10.1	Calcolo	Valore in byte
KB	KiB	1024	1024 byte
MB	MIB	1024 * 1024	1,048,576 byte
GB	Gib	1024 * 1024 * 1024	1,073,741,824 byte
TB	TIB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 byte

Funzionalità di monitoraggio dello stato di Unified Manager

Unified Manager si basa su un'infrastruttura server che offre scalabilità, supportabilità e funzionalità avanzate di monitoraggio e notifica. Unified Manager supporta il monitoraggio dei sistemi che eseguono il software ONTAP.

Unified Manager include le seguenti funzionalità:

- Rilevamento, monitoraggio e notifiche per i sistemi installati con il software ONTAP:
  - Oggetti fisici: Nodi, dischi, shelf di dischi, coppie SFO, porte, E Flash cache
  - Oggetti logici: Cluster, storage virtual machine (SVM), aggregati, volumi, LUN, namespace, Qtree, LIF, copie Snapshot, percorsi di giunzione, condivisioni NFS, Condivisioni SMB, quote utente e gruppo, gruppi di criteri QoS e gruppi iniziatori
  - Protocolli: CIFS, NFS, FC, iSCSI, NVMe, E FCoE
  - Efficienza dello storage: Aggregati di SSD, aggregati di Flash Pool, aggregati di FabricPool, deduplica e compressione
  - Protezione: Relazioni SnapMirror (sincrone e asincrone) e relazioni SnapVault
- Visualizzazione dello stato di rilevamento e monitoraggio del cluster
- Configurazioni MetroCluster su FC e IP: Visualizzazione e monitoraggio della configurazione, dei problemi e dello stato di connettività dei componenti del cluster. Switch e bridge MetroCluster per configurazioni MetroCluster over FC
- Miglioramento dell'infrastruttura di avvisi, eventi e soglie
- LDAP, LDAPS, autenticazione SAML e supporto utente locale
- RBAC (per un set predefinito di ruoli)
- AutoSupport e bundle di supporto
- Dashboard migliorato per mostrare capacità, disponibilità, protezione e performance dell'ambiente
- Interoperabilità dello spostamento del volume, cronologia dello spostamento del volume e cronologia delle modifiche del percorso di giunzione
- Area di impatto che visualizza graficamente le risorse interessate da eventi come alcuni dischi non riusciti, mirroring aggregato MetroCluster degradato e dischi di riserva MetroCluster lasciati indietro

- Possibile area di effetto che visualizza l'effetto degli eventi MetroCluster
- Area azioni correttive consigliate che visualizza le azioni che possono essere eseguite per affrontare eventi come alcuni dischi non riusciti, mirroring aggregato MetroCluster degradato e dischi di riserva MetroCluster lasciati indietro
- Area delle risorse che potrebbero essere interessate da questo problema che visualizza le risorse che potrebbero essere interessate da eventi come l'evento Volume Offline, l'evento Volume Restricted e l'evento Thin-Provised Volume Space at Risk
- Supporto per SVM con volumi FlexVol o FlexGroup
- Supporto per il monitoraggio dei volumi root dei nodi
- Monitoraggio avanzato delle copie Snapshot, incluso il calcolo dello spazio recuperabile e l'eliminazione delle copie Snapshot
- Annotazioni per gli oggetti di storage
- Creazione di report e gestione di informazioni sugli oggetti storage come capacità fisica e logica, utilizzo, risparmi di spazio, performance ed eventi correlati
- Integrazione con OnCommand Workflow Automation per l'esecuzione dei flussi di lavoro

  Il negozio di automazione dello storage contiene pacchetti di workflow automatizzati per lo storage certificati da NetApp sviluppati per l'utilizzo con OnCommand Workflow Automation (WFA). È possibile scaricare i pacchetti e importarli in WFA per eseguirli. I flussi di lavoro automatizzati sono disponibili qui:

  "Storage Automation Store"

Interfacce di Unified Manager utilizzate per gestire lo stato di salute del sistema storage

Queste sezioni contengono informazioni sulle due interfacce utente fornite da Active IQ Unified Manager per la risoluzione dei problemi di capacità, disponibilità e protezione dello storage dei dati. Le due interfacce utente sono l'interfaccia utente Web di Unified Manager e la console di manutenzione.

Se si desidera utilizzare le funzioni di protezione di Unified Manager, è necessario installare e configurare anche OnCommand Workflow Automation (Wfa).

UI Web di Unified Manager

L'interfaccia utente Web di Unified Manager consente a un amministratore di monitorare e risolvere i problemi del cluster relativi a capacità, disponibilità e protezione dello storage dei dati.

Queste sezioni descrivono alcuni flussi di lavoro comuni che un amministratore può seguire per risolvere i problemi di capacità dello storage, disponibilità dei dati o protezione visualizzati nell'interfaccia utente Web di Unified Manager.

Console di manutenzione

La console di manutenzione di Unified Manager consente a un amministratore di monitorare, diagnosticare e risolvere i problemi del sistema operativo, i problemi di aggiornamento della versione, i problemi di accesso degli utenti e i problemi di rete relativi al server Unified Manager stesso. Se l'interfaccia utente Web di Unified Manager non è disponibile, la console di manutenzione è l'unica forma di accesso a Unified Manager.

È possibile utilizzare queste informazioni per accedere alla console di manutenzione e utilizzarla per risolvere i problemi relativi al funzionamento del server Unified Manager.

Gestione e monitoraggio dei cluster e dello stato degli oggetti del cluster

Unified Manager utilizza query API periodiche e un motore di raccolta dati per raccogliere i dati dai cluster. Aggiungendo cluster al database di Unified Manager, è possibile monitorare e gestire questi cluster per rilevare eventuali rischi di disponibilità e capacità.

Comprendere il monitoraggio dei cluster

È possibile aggiungere cluster al database di Unified Manager per monitorare la disponibilità, la capacità e altri dettagli, come l'utilizzo della CPU, le statistiche dell'interfaccia, lo spazio libero su disco, l'utilizzo di qtree e l'ambiente dello chassis.

Gli eventi vengono generati se lo stato è anomalo o quando viene superata una soglia predefinita. Se configurato in questo modo, Unified Manager invia una notifica a un destinatario specificato quando un evento attiva un avviso.

Comprensione dei volumi root dei nodi

È possibile monitorare il volume root del nodo utilizzando Unified Manager. La Best practice consiste nel fatto che il volume root del nodo deve avere una capacità sufficiente a impedire il downdown del nodo.

Quando la capacità utilizzata del volume root del nodo supera il 80% della capacità totale del volume root del nodo, viene generato l'evento Node Root Volume Space quasi Full. È possibile configurare un avviso per l'evento per ricevere una notifica. È possibile intraprendere le azioni appropriate per impedire che il nodo si blocchi utilizzando Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

Informazioni su eventi e soglie per gli aggregati root di nodi

È possibile monitorare l'aggregato root del nodo utilizzando Unified Manager. La Best practice consiste nel fornire in maniera spessa il volume root nell'aggregato root per evitare che il nodo si arresti.

Per impostazione predefinita, gli eventi di capacità e performance non vengono generati per gli aggregati root. Inoltre, i valori di soglia utilizzati da Unified Manager non sono applicabili agli aggregati root del nodo. Solo un rappresentante del supporto tecnico può modificare le impostazioni per questi eventi da generare. Quando le impostazioni vengono modificate dal rappresentante del supporto tecnico, i valori di soglia della capacità vengono applicati all'aggregato root del nodo.

È possibile intraprendere le azioni appropriate per impedire l'arresto del nodo utilizzando Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

Comprensione del quorum e dell'epsilon

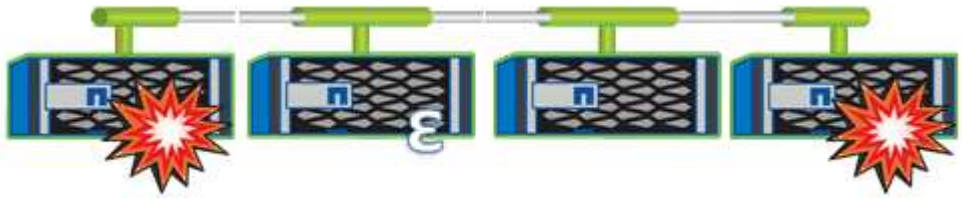
Il quorum e l'epsilon sono misure importanti per lo stato e la funzione dei cluster che indicano insieme come i cluster affrontano le potenziali sfide di comunicazione e

connettività.

Quorum è una condizione preliminare per un cluster completamente funzionante. Quando un cluster si trova in quorum, la maggior parte dei nodi è in buone condizioni e può comunicare tra loro. In caso di perdita del quorum, il cluster perde la capacità di eseguire le normali operazioni del cluster. Solo un insieme di nodi può avere il quorum alla volta, perché tutti i nodi condividono collettivamente una singola vista dei dati. Pertanto, se a due nodi non comunicanti è consentito modificare i dati in modo divergente, non è più possibile riconciliare i dati in una singola vista dati.

Ogni nodo del cluster partecipa a un protocollo di voting che sceglie un nodo master; ogni nodo rimanente è un nodo secondario. Il nodo master è responsabile della sincronizzazione delle informazioni nel cluster. Una volta formato, il quorum viene mantenuto con il voto continuo. Se il nodo master non è in linea e il cluster è ancora in quorum, viene selezionato un nuovo master dai nodi che rimangono in linea.

Poiché esiste la possibilità di un legame in un cluster con un numero pari di nodi, un nodo ha un peso di voto frazionario aggiuntivo chiamato epsilon. Se la connettività tra due parti uguali di un cluster di grandi dimensioni non riesce, il gruppo di nodi che contiene epsilon mantiene il quorum, presupponendo che tutti i nodi siano integri. Ad esempio, la seguente illustrazione mostra un cluster a quattro nodi in cui due dei nodi sono guasti. Tuttavia, poiché uno dei nodi sopravvissuti contiene epsilon, il cluster rimane in quorum anche se non esiste una semplice maggioranza di nodi sani.



Epsilon viene assegnato automaticamente al primo nodo al momento della creazione del cluster. Se il nodo che contiene epsilon diventa inintegro, assume il controllo del partner ad alta disponibilità o viene sostituito dal partner ad alta disponibilità, epsilon viene automaticamente riassegnato a un nodo integro in una coppia ha diversa.

L'utilizzo offline di un nodo può influire sulla capacità del cluster di rimanere in quorum. Pertanto, ONTAP emette un messaggio di avviso se si tenta di eseguire un'operazione che toglie il quorum al cluster o se si mette fuori servizio un'operazione per evitare la perdita del quorum. È possibile disattivare i messaggi di avviso del quorum utilizzando il comando cluster quorum-service options modify al livello di privilegio avanzato.

In generale, supponendo una connettività affidabile tra i nodi del cluster, un cluster più grande è più stabile di un cluster più piccolo. Il requisito di quorum di una semplice maggioranza della metà dei nodi più epsilon è più semplice da gestire in un cluster di 24 nodi che in un cluster di due nodi.

Un cluster a due nodi presenta alcune sfide specifiche per il mantenimento del quorum. I cluster a due nodi utilizzano il cluster ha, in cui nessuno dei due nodi contiene epsilon; invece, entrambi i nodi vengono continuamente interrogati per garantire che, in caso di guasto di un nodo, l'altro disponga dell'accesso completo in lettura/scrittura ai dati, nonché dell'accesso alle interfacce logiche e alle funzioni di gestione.

Visualizzazione dell'elenco e dei dettagli del cluster

È possibile utilizzare la vista Health: All Clusters (Salute: Tutti i cluster) per visualizzare l'inventario dei cluster. La vista capacità: Tutti i cluster consente di visualizzare informazioni riepilogative sulla capacità e sull'utilizzo dello storage in tutti i cluster.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

È inoltre possibile visualizzare i dettagli dei singoli cluster, ad esempio lo stato del cluster, la capacità, la configurazione, le LIF, i nodi, E dischi in quel cluster utilizzando la pagina Cluster / Health Details.

I dettagli nella vista Health: All Clusters (Salute: Tutti i cluster), Capacity: All Clusters (capacità: Tutti i cluster) e nella pagina Cluster / Health Details (Dettagli cluster/integrità) consentono di pianificare lo storage. Ad esempio, prima di eseguire il provisioning di un nuovo aggregato, è possibile selezionare un cluster specifico dalla vista Health: All Clusters (Salute: Tutti i cluster) e ottenere i dettagli della capacità per determinare se il cluster dispone dello spazio richiesto.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Clusters**.
2. Nel menu View (Visualizza), selezionare la vista **Health: All Clusters** (Salute: Tutti i cluster) per visualizzare le informazioni sullo stato di salute oppure la vista **Capacity: All Clusters** (capacità: Tutti i cluster) per visualizzare i dettagli sulla capacità e sull'utilizzo dello storage in tutti i cluster.
3. Fare clic sul nome di un cluster per visualizzare i dettagli completi del cluster nella pagina dei dettagli **Cluster / Health**.

Informazioni correlate

- "Pagina dei dettagli del cluster/stato di salute"
- "Performance: Vista di tutti i cluster"
- "Monitoraggio delle configurazioni MetroCluster"
- "Visualizzazione dello stato di sicurezza per cluster e VM di storage"
- "Quali criteri di sicurezza vengono valutati"

Verifica dello stato dei cluster in una configurazione MetroCluster

È possibile utilizzare Active IQ Unified Manager (Unified Manager) per controllare lo stato operativo dei cluster e dei relativi componenti nelle configurazioni MetroCluster over FC e MetroCluster over IP. Se i cluster sono stati coinvolti in un evento di performance rilevato da Unified Manager, lo stato di salute può aiutare a determinare se un problema hardware o software ha contribuito all'evento.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- È necessario aver analizzato un evento di performance per una configurazione MetroCluster e avere ottenuto il nome del cluster interessato.
- Entrambi i cluster nella configurazione MetroCluster su FC e IP devono essere monitorati dalla stessa istanza di Unified Manager.

Determinazione dello stato del cluster nella configurazione MetroCluster over FC

Per determinare lo stato del cluster in una configurazione MetroCluster su FC, procedere come segue.

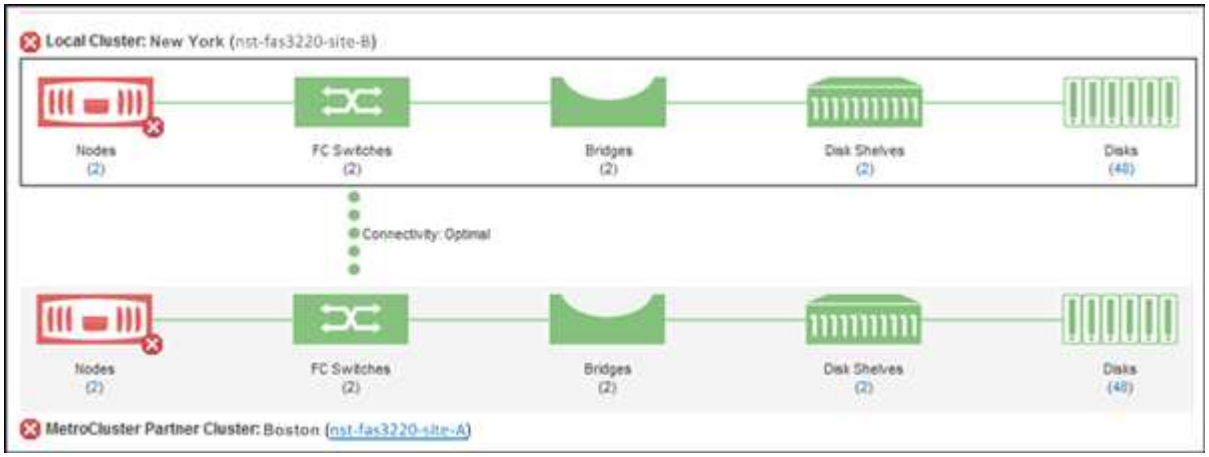
Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi** per visualizzare l'elenco degli eventi.
2. Nel pannello dei filtri, selezionare All MetroCluster filters (tutti i filtri) nella categoria **Source Type** (tipo di origine). Vengono visualizzati tutti gli eventi generati nel proprio ambiente per tutte le configurazioni MetroCluster.
3. Accanto a un evento MetroCluster, fare clic sul nome del cluster.

   Se non viene visualizzato alcun evento MetroCluster, è possibile utilizzare la barra di ricerca per cercare il nome del cluster coinvolto nell'evento correlato alla configurazione MetroCluster over FC.

   Viene visualizzata la vista Health: All Clusters (Salute: Tutti i cluster) con informazioni dettagliate sull'evento.

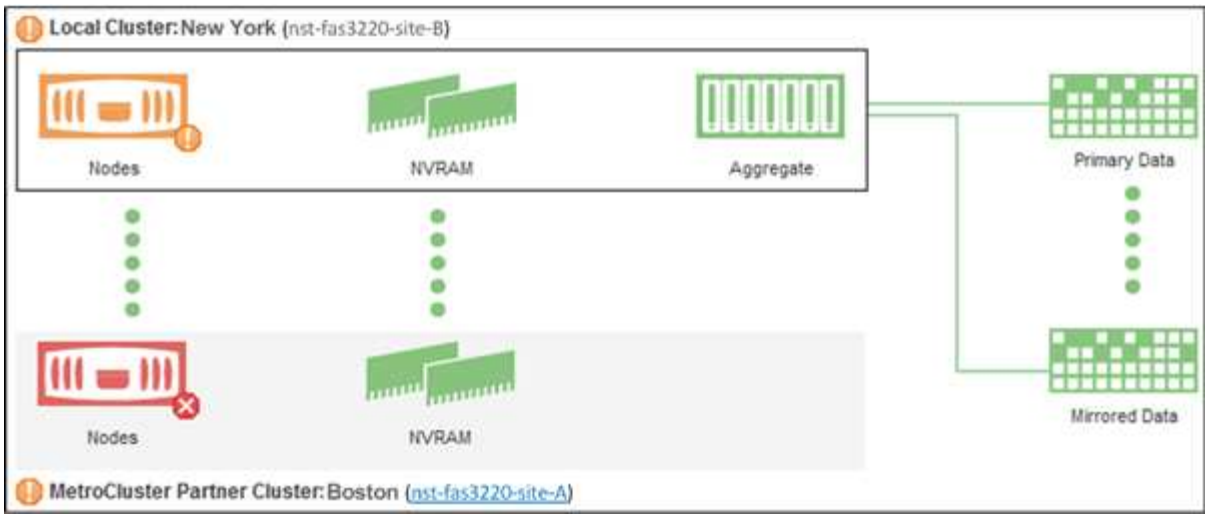
4. Selezionare la scheda **connettività MetroCluster** per visualizzare lo stato della connessione tra il cluster selezionato e il cluster partner.



   In questo esempio, vengono visualizzati i nomi e i componenti del cluster locale e del cluster partner. Un'icona gialla o rossa indica un evento di integrità per il componente evidenziato. L'icona Connectivity (connettività) rappresenta il collegamento tra i cluster. È possibile puntare il cursore del mouse su un'icona per visualizzare le informazioni sull'evento o fare clic sull'icona per visualizzare gli eventi. Un problema di integrità su entrambi i cluster potrebbe aver contribuito all'evento delle performance.

   Unified Manager monitora il componente NVRAM del collegamento tra i cluster. Se l'icona FC Switches (interruttori FC) sul cluster locale o partner o l'icona Connectivity (connettività) è rossa, potrebbe essere stato causato un problema di stato del collegamento.

5. Selezionare la scheda **Replica MetroCluster**.



In questo esempio, se l'icona NVRAM sul cluster locale o partner è gialla o rossa, un problema di integrità della NVRAM potrebbe aver causato l'evento delle prestazioni. Se sulla pagina non sono presenti icone rosse o gialle, un problema di performance sul cluster partner potrebbe aver causato l'evento di performance.

Determinazione dello stato del cluster nella configurazione MetroCluster over IP

Per determinare lo stato del cluster in una configurazione MetroCluster over IP, procedere come segue.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi** per visualizzare l'elenco degli eventi.
2. Nel pannello del filtro, sotto la categoria **Source Type** (tipo di origine), selezionare `MetroCluster Relationship` filtro. Vengono visualizzati tutti gli eventi generati nel proprio ambiente per tutte le configurazioni MetroCluster.

   Se non è possibile visualizzare gli eventi MetroCluster segnalati, utilizzare la barra di ricerca per cercare in base al nome del cluster coinvolto nell'evento correlato alla configurazione MetroCluster over IP.

3. Accanto all'evento MetroCluster pertinente, fare clic sul nome del cluster. Viene visualizzata la pagina Clusters con i dettagli del cluster. Per informazioni sulla determinazione dei problemi di salute, vedere "Monitorare i problemi di connettività nella configurazione MetroCluster over IP".

Visualizzazione dello stato di salute e capacità di tutti i cluster di array SAN

È possibile utilizzare le pagine di inventario del cluster per visualizzare lo stato di salute e capacità dei cluster All SAN Array.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

È possibile visualizzare le informazioni generali per tutti i cluster array SAN nella vista Health: All Clusters (Salute: Tutti i cluster) e Capacity: All Clusters (capacità: Tutti i cluster). Inoltre, è possibile visualizzare i dettagli nella pagina Cluster / Health Details.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Clusters**.
2. Assicurarsi che la colonna “Personality” sia visualizzata nella vista **Health: Tutti i cluster** oppure aggiungerla utilizzando il controllo **Show / Hide**.

   In questa colonna viene visualizzato “All SAN Array” (tutti gli array SAN) per tutti i cluster di array SAN.
3. Esaminare le informazioni.
4. Per visualizzare informazioni sulla capacità dello storage in questi cluster, selezionare la vista capacità: Tutti i cluster.
5. Per visualizzare informazioni dettagliate sullo stato di salute e sulla capacità dello storage in tali cluster, fare clic sul nome di un cluster All SAN Array.

   Visualizzare i dettagli nelle schede Health (Stato), Capacity (capacità) e Nodes (nodi) nella pagina Cluster / Health details (Dettagli cluster/salute)

Visualizzazione dell’elenco dei nodi e dei dettagli

È possibile utilizzare la vista Health: All Nodes (Salute: Tutti i nodi) per visualizzare l’elenco dei nodi nei cluster. È possibile utilizzare la pagina Cluster / Health Details per visualizzare informazioni dettagliate sui nodi che fanno parte del cluster monitorato.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell’applicazione o amministratore dello storage.

È possibile visualizzare dettagli quali lo stato del nodo, il cluster che contiene il nodo, i dettagli della capacità aggregata (utilizzata e totale) e i dettagli della capacità raw (utilizzabile, spare e totale). È inoltre possibile ottenere informazioni su coppie ha, shelf di dischi e porte.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Nodes**.
2. Nella vista **Health: All Nodes** (Salute: Tutti i nodi), fare clic sul nodo di cui si desidera visualizzare i dettagli.

   Le informazioni dettagliate per il nodo selezionato vengono visualizzate nella pagina Cluster / Health details (Dettagli cluster/salute). Nel riquadro di sinistra viene visualizzato l’elenco delle coppie ha. Per impostazione predefinita, l’opzione ha Details (Dettagli ha) è aperta, che visualizza i dettagli dello stato ha e gli eventi correlati alla coppia ha selezionata.
3. Per visualizzare altri dettagli sul nodo, eseguire l’azione appropriata:

Per visualizzare…	**Fare clic su…**
Dettagli sugli shelf di dischi	**Shelf di dischi**.
Informazioni relative alla porta	**Porte**.

Per ulteriori informazioni, consulta:

- "Performance: Vista di tutti i nodi"

- "Visualizzazione dei valori IOPS disponibili di nodo e aggregazione"
- "Visualizzazione dei valori utilizzati per la capacità di nodo e le performance aggregate"

Generazione di un report sull'inventario hardware per il rinnovo del contratto

È possibile generare un report che contiene un elenco completo di informazioni su cluster e nodi, ad esempio numeri di modello e di serie dell'hardware, tipi di dischi e conteggi, licenze installate e altro ancora. Questo report è utile per il rinnovo del contratto all'interno di siti sicuri ("siti `dARK`") non connessi alla piattaforma NetAppActive IQ.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Nodes**.
2. Accedere alla vista **Health: All Nodes** (Salute: Tutti i nodi) o **Performance: All Nodes** (prestazioni: Tutti i nodi).
3. Selezionare **Report** > ***** > Report inventario hardware*.

   Il report dell'inventario hardware viene scaricato come file .csv con informazioni complete alla data corrente.

4. Fornisci queste informazioni al tuo contatto del supporto NetApp per il rinnovo del contratto.

Visualizzazione dell'elenco e dei dettagli di Storage VM

Dalla vista Health: All Storage VM (Salute: Tutte le macchine virtuali dello storage), è possibile monitorare l'inventario delle macchine virtuali dello storage (SVM). È possibile utilizzare la pagina Storage VM / Health Details per visualizzare informazioni dettagliate sulle SVM monitorate.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

È possibile visualizzare i dettagli di SVM, ad esempio la capacità, l'efficienza e la configurazione di una SVM. È inoltre possibile visualizzare informazioni sui dispositivi correlati e sugli avvisi correlati per la SVM.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Storage VMS**.
2. Scegliere uno dei seguenti modi per visualizzare i dettagli SVM:
   - Per visualizzare le informazioni sullo stato di tutte le SVM in tutti i cluster, nel menu View (Visualizza), selezionare Health: All Storage VMS view (Stato: Vista di tutte le VM di storage).
   - Per visualizzare i dettagli completi, fare clic sul nome della Storage VM.

     È inoltre possibile visualizzare i dettagli completi facendo clic su **View Details** (Visualizza dettagli) nella finestra di dialogo Minimal Details (Dettagli minimi).

3. Visualizzare gli oggetti correlati alla SVM facendo clic su **Visualizza correlati** nella finestra di dialogo Dettagli minimi.

Informazioni correlate

- "Storage VM: Pagina dei dettagli sullo stato di salute"
- "Performance: Vista di tutte le VM di storage"
- "Sicurezza: Vista anti-ransomware"
- "Visualizzazione dello stato di sicurezza per cluster e VM di storage"
- "Relazione: Vista tutte le relazioni"

Visualizzazione dell'elenco aggregato e dei dettagli

Dalla vista Health: All aggregates (Salute: Tutti gli aggregati), è possibile monitorare l'inventario degli aggregati. La vista capacità: Tutti gli aggregati consente di visualizzare informazioni sulla capacità e sull'utilizzo degli aggregati in tutti i cluster.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

È possibile visualizzare dettagli come la capacità aggregata e la configurazione e informazioni sui dischi dalla pagina aggregata/Dettagli sullo stato di salute. È possibile utilizzare questi dettagli prima di configurare le impostazioni di soglia, se necessario.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates**.
2. Scegliere uno dei seguenti modi per visualizzare i dettagli dell'aggregato:
   - Per visualizzare le informazioni sullo stato di tutti gli aggregati in tutti i cluster, nel menu View (Visualizza), selezionare Health: All aggregates view (Salute: Vista di tutti gli aggregati).
   - Per visualizzare informazioni sulla capacità e sull'utilizzo di tutti gli aggregati in tutti i cluster, nel menu View (Visualizza), selezionare Capacity: All aggregates view (capacità: Vista di tutti gli aggregati).
   - Per visualizzare i dettagli completi, fare clic sul nome dell'aggregato.

     È inoltre possibile visualizzare i dettagli completi facendo clic su **View Details** (Visualizza dettagli) nella finestra di dialogo Minimal Details (Dettagli minimi).
3. Visualizzare gli oggetti correlati all'aggregato facendo clic su **Visualizza correlati** nella finestra di dialogo Dettagli minimi.

Informazioni correlate

- "Pagina aggregata/Dettagli salute"
- "Performance: Vista di tutti gli aggregati"
- "Personalizzazione dei report sulla capacità aggregata"

Visualizzazione delle informazioni sulla capacità FabricPool

È possibile visualizzare le informazioni sulla capacità di FabricPool per cluster, aggregati

e volumi nelle pagine dell'inventario capacità e performance e dei dettagli per questi oggetti. Queste pagine visualizzano anche le informazioni del mirror FabricPool quando è stato configurato un Tier mirror.

In queste pagine vengono visualizzate informazioni quali la capacità disponibile sul Tier di performance locale e sul Tier cloud, la capacità utilizzata in entrambi i Tier, gli aggregati collegati a un Tier cloud, E quali volumi stanno implementando le funzionalità di FabricPool spostando determinate informazioni nel Tier cloud.

Quando un livello cloud viene mirrorato su un altro provider cloud (il "mlivello di orrore"), entrambi i livelli cloud vengono visualizzati nella pagina aggregato/Dettagli salute.

Fasi

1. Eseguire una delle seguenti operazioni:

Per visualizzare le informazioni sulla capacità per…	**Eseguire questa operazione…**
Cluster	a. Nella vista capacità: Tutti i cluster, fare clic su un cluster. b. Nella pagina Cluster / Health details (Dettagli cluster/integrità), fare clic sulla scheda **Configuration** (Configurazione). Il display mostra i nomi dei Tier cloud a cui è connesso il cluster.
Aggregati	a. Nella vista capacità: Tutti gli aggregati, fare clic su un aggregato in cui il campo tipo indica "SSD (FabricPool)" o "HDD (FabricPool)". b. Nella pagina aggregato/Dettagli salute, fare clic sulla scheda **capacità**. Il display mostra la capacità totale utilizzata nel Tier cloud. c. Fare clic sulla scheda **Disk Information** (informazioni disco). Il display mostra il nome del livello cloud e la capacità utilizzata. d. Fare clic sulla scheda **Configurazione**. Il display mostra il nome del livello cloud e altre informazioni dettagliate sul livello cloud.

Per visualizzare le informazioni sulla capacità per…	Eseguire questa operazione…
Volumi	a. Nella vista capacità: Tutti i volumi, fare clic su un volume in cui viene visualizzato il nome di un criterio nel campo “Tiering Policy”. b. Nella pagina Volume / Health details (Dettagli volume/salute), fare clic sulla scheda **Configuration** (Configurazione). Sul display viene visualizzato il nome del criterio di tiering FabricPool assegnato al volume.

2. Nella pagina **analisi del carico di lavoro** è possibile selezionare “Cloud Tier View” nell’area **Capacity Trend** per visualizzare la capacità utilizzata nel Performance Tier locale e nel Cloud Tier nel mese precedente.

Per ulteriori informazioni sugli aggregati FabricPool, vedere "Panoramica su dischi e aggregati".

Visualizzazione dei dettagli del pool di storage

È possibile visualizzare i dettagli del pool di storage per monitorare lo stato del pool di storage, la cache totale e disponibile e le allocazioni utilizzate e disponibili.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell’applicazione o amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates**.
2. Fare clic su un nome aggregato.

   Vengono visualizzati i dettagli dell’aggregato selezionato.

3. Fare clic sulla scheda **Disk Information** (informazioni disco).

   Vengono visualizzate informazioni dettagliate sul disco.

   La tabella cache viene visualizzata solo quando l’aggregato selezionato utilizza un pool di storage.

4. Nella tabella cache, spostare il puntatore sul nome del pool di storage richiesto.

   Vengono visualizzati i dettagli del pool di storage.

Visualizzazione dell’elenco e dei dettagli dei volumi

Dalla vista Health: All Volumes (Salute: Tutti i volumi), è possibile monitorare l’inventario dei volumi. La vista Capacity: All Volumes (capacità: Tutti i volumi) consente di visualizzare informazioni sulla capacità e sull’utilizzo dei volumi in un cluster.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

È inoltre possibile utilizzare la pagina dei dettagli relativi a volume/salute per visualizzare informazioni dettagliate sui volumi monitorati, tra cui capacità, efficienza, configurazione e protezione dei volumi. È inoltre possibile visualizzare informazioni sulle periferiche correlate e sugli avvisi correlati per un volume specifico.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Scegliere uno dei seguenti metodi per visualizzare i dettagli del volume:
   - Per visualizzare informazioni dettagliate sullo stato dei volumi in un cluster, nel menu View (Visualizza), selezionare Health: All Volumes view (Salute: Vista di tutti i volumi).
   - Per visualizzare informazioni dettagliate sulla capacità e sull'utilizzo dei volumi in un cluster, nel menu View (Visualizza), selezionare Capacity: All Volumes view (capacità: Vista tutti i volumi).
   - Per visualizzare i dettagli completi, fare clic sul nome del volume.

     È inoltre possibile visualizzare i dettagli completi facendo clic su **View Details** (Visualizza dettagli) nella finestra di dialogo Minimal Details (Dettagli minimi).
3. **Opzionale:** visualizzare gli oggetti correlati al volume facendo clic su **Visualizza correlati** nella finestra di dialogo Dettagli minimi.

Informazioni correlate

- "Volume: Pagina dei dettagli sullo stato di salute"
- "Performance (prestazioni): Vista di tutti i volumi"
- "Sicurezza: Vista anti-ransomware"
- "Visualizzazione delle relazioni di protezione dei volumi"
- "Creazione di un report per visualizzare i grafici della capacità dei volumi disponibili"

Visualizzazione dei dettagli sulle condivisioni NFS

È possibile visualizzare i dettagli di tutte le condivisioni NFS, ad esempio il relativo stato, il percorso associato al volume (volumi FlexGroup o volumi FlexVol), i livelli di accesso dei client alle condivisioni NFS e la policy di esportazione definita per i volumi esportati. Utilizzare la vista Health: All NFS shares per visualizzare tutte le condivisioni NFS su tutti i cluster monitorati e utilizzare la pagina Storage VM / Health details per visualizzare tutte le condivisioni NFS su una specifica macchina virtuale di storage (SVM).

Cosa ti serve

- La licenza NFS deve essere attivata sul cluster.
- Le interfacce di rete che servono le condivisioni NFS devono essere configurate.
- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Fase

1. Nel riquadro di navigazione a sinistra, seguire i passaggi riportati di seguito a seconda che si desideri visualizzare tutte le condivisioni NFS o solo le condivisioni NFS per una specifica SVM.

Per…	Attenersi alla procedura descritta di seguito…
Visualizza tutte le condivisioni NFS	Fare clic su **Storage** > **NFS shares**
Visualizza condivisioni NFS per SVM singola	a. Fare clic su **Storage** > **Storage VM** b. Fare clic sulla SVM per la quale si desidera visualizzare i dettagli delle condivisioni NFS. c. Nella pagina Storage VM / Health details (Dettagli sullo stato di salute/VM di storage), fare clic sulla scheda **NFS Shares** (condivisioni NFS).

Per ulteriori informazioni, vedere "Provisioning dei volumi di condivisione dei file" e. "Provisioning delle condivisioni di file CIFS e NFS tramite API".

Visualizzazione dei dettagli sulle condivisioni SMB/CIFS

È possibile visualizzare i dettagli di tutte le condivisioni SMB/CIFS, ad esempio il nome della condivisione, il percorso di giunzione, gli oggetti contenenti, le impostazioni di sicurezza e i criteri di esportazione definiti per la condivisione. Utilizzare la vista Health: All SMB shares per visualizzare tutte le condivisioni SMB su tutti i cluster monitorati e utilizzare la pagina Storage VM / Health details per visualizzare tutte le condivisioni SMB su una specifica macchina virtuale di storage (SVM).

Cosa ti serve

- La licenza CIFS deve essere attivata sul cluster.
- È necessario configurare le interfacce di rete che servono le condivisioni SMB/CIFS.
- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Le condivisioni nelle cartelle non vengono visualizzate.

Fase

1. Nel riquadro di navigazione a sinistra, seguire la procedura riportata di seguito a seconda che si desideri visualizzare tutte le condivisioni SMB/CIFS o solo le condivisioni di una specifica SVM.

Per…	Attenersi alla procedura descritta di seguito…
Visualizza tutte le condivisioni SMB/CIFS	Fare clic su **Storage** > **SMB shares**

Per…	Attenersi alla procedura descritta di seguito…
Visualizza le condivisioni SMB/CIFS per SVM singola	a. Fare clic su **Storage** > **Storage VM** b. Fare clic sulla SVM per la quale si desidera visualizzare i dettagli della condivisione SMB/CIFS. c. Nella pagina Storage VM / Health details (Dettagli stato/VM storage), fare clic sulla scheda **SMB shares** (condivisioni SMB).

Per ulteriori informazioni, vedere "Provisioning delle condivisioni di file CIFS e NFS tramite API".

Visualizzazione dell'elenco delle copie Snapshot

È possibile visualizzare l'elenco delle copie Snapshot per un volume selezionato. È possibile utilizzare l'elenco delle copie Snapshot per calcolare la quantità di spazio su disco che è possibile recuperare se una o più copie Snapshot vengono eliminate ed è possibile eliminare le copie Snapshot, se necessario.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Il volume contenente le copie Snapshot deve essere online.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nella vista **Health: All Volumes**, selezionare il volume contenente le copie Snapshot che si desidera visualizzare.
3. Nella pagina dei dettagli **Volume / Health**, fare clic sulla scheda **Capacity**.
4. Nel riquadro **Dettagli** della scheda **capacità**, nella sezione altri dettagli, fare clic sul collegamento accanto a **copie Snapshot**.

   Il numero di copie Snapshot è un collegamento che visualizza l'elenco delle copie Snapshot.

Informazioni correlate

"Pagina Health/Volumes"

Eliminazione delle copie Snapshot

È possibile eliminare una copia Snapshot per risparmiare spazio o liberare spazio su disco, oppure eliminare la copia Snapshot se non è più necessaria.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Il volume deve essere online.

Per eliminare una copia Snapshot occupata o bloccata, è necessario rilasciare la copia Snapshot dall'applicazione che la stava utilizzando.

- Non è possibile eliminare la copia Snapshot di base in un volume padre se un volume FlexClone utilizza tale copia Snapshot.

  La copia Snapshot di base è la copia Snapshot utilizzata per creare il volume FlexClone e visualizzare lo stato `Busy` E dipendenza dell'applicazione come `Busy, Vclone` nel volume padre.

- Non è possibile eliminare una copia Snapshot bloccata utilizzata in una relazione SnapMirror.

  La copia Snapshot è bloccata ed è necessaria per il prossimo aggiornamento.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nella vista **Health: All Volumes**, selezionare il volume contenente le copie Snapshot che si desidera visualizzare.

   Viene visualizzato l'elenco delle copie Snapshot.

3. Nella pagina dei dettagli **Volume / Health**, fare clic sulla scheda **Capacity**.
4. Nel riquadro **Dettagli** della scheda **capacità**, nella sezione altri dettagli, fare clic sul collegamento accanto a **copie Snapshot**.

   Il numero di copie Snapshot è un collegamento che visualizza l'elenco delle copie Snapshot.

5. Nella vista **Snapshot Copies**, selezionare le copie Snapshot che si desidera eliminare, quindi fare clic su **Delete Selected** (Elimina selezionati).

Calcolo dello spazio recuperabile per le copie Snapshot

È possibile calcolare la quantità di spazio su disco che è possibile recuperare se una o più copie Snapshot vengono eliminate.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- Il volume deve essere online.
- Il volume deve essere un volume FlexVol; questa funzionalità non è supportata con i volumi FlexGroup.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nella vista **Health: All Volumes**, selezionare il volume contenente le copie Snapshot che si desidera visualizzare.

   Viene visualizzato l'elenco delle copie Snapshot.

3. Nella pagina dei dettagli **Volume / Health**, fare clic sulla scheda **Capacity**.

4. Nel riquadro **Dettagli** della scheda **capacità**, nella sezione altri dettagli, fare clic sul collegamento accanto a **copie Snapshot**.

   Il numero di copie Snapshot è un collegamento che visualizza l'elenco delle copie Snapshot.

5. Nella vista **Snapshot Copies**, selezionare le copie Snapshot per cui si desidera calcolare lo spazio recuperabile.
6. Fare clic su **Calcola**.

   Viene visualizzato lo spazio recuperabile (in percentuale e KB, MB, GB e così via) sul volume.

7. Per ricalcolare lo spazio recuperabile, selezionare le copie Snapshot richieste e fare clic su **Ricalcola**.

Descrizione delle finestre di dialogo e degli oggetti del cluster

È possibile visualizzare tutti i cluster e gli oggetti cluster dalla pagina degli oggetti di storage corrispondenti. È inoltre possibile visualizzare i dettagli dalla pagina dei dettagli dell'oggetto di storage corrispondente. È ora possibile avviare l'interfaccia utente di System Manager dalle seguenti sezioni RELATIVE ALLO STORAGE e ALLA PROTEZIONE dell'INVENTARIO.

- Inventario dei cluster, stato dei cluster e prestazioni dei cluster
- Pagine di inventario aggregato, salute aggregata e performance aggregate
- Pagine Volume Inventory, Volume Health e Volume Performance
- Pagine Node Inventory e Node Performance
- Pagine StorageVM Inventory, StorageVM Health e StorageVM Performance
- Pagine delle relazioni di protezione

Flussi di lavoro e attività comuni per lo stato di salute di Unified Manager

Alcuni dei flussi di lavoro e delle attività amministrative più comuni associati a Unified Manager includono la selezione dei cluster di storage da monitorare, la diagnosi di condizioni che influiscono negativamente sulla disponibilità, la capacità e la protezione dei dati, il ripristino dei dati persi, la configurazione e la gestione dei volumi, il raggruppamento e l'invio di dati diagnostici al supporto tecnico (se necessario).

Unified Manager consente agli amministratori dello storage di visualizzare una dashboard, valutare la capacità complessiva, la disponibilità e lo stato di protezione dei cluster di storage gestiti, quindi identificare, individuare, diagnosticare e assegnare rapidamente eventuali problemi specifici che potrebbero insorgere.

I problemi più importanti relativi a un cluster, a una macchina virtuale di storage, a un volume o a un volume FlexGroup che influiscono sulla capacità di storage o sulla disponibilità dei dati degli oggetti storage gestiti vengono visualizzati nei grafici di stato del sistema e negli eventi della pagina Dashboard. Quando vengono identificati problemi critici, questa pagina fornisce collegamenti a supporto dei flussi di lavoro appropriati per la risoluzione dei problemi.

Unified Manager può anche essere incluso nei flussi di lavoro che includono i relativi strumenti di gestione, ad

esempio OnCommand Workflow Automation (Wfa), per supportare la configurazione diretta delle risorse di storage.

I flussi di lavoro comuni relativi alle seguenti attività amministrative sono descritti in questo documento:

- Diagnosi e gestione dei problemi di disponibilità

  Se un guasto hardware o problemi di configurazione delle risorse di storage causano la visualizzazione degli eventi di disponibilità dei dati nella pagina Dashboard, gli amministratori dello storage possono seguire i collegamenti integrati per visualizzare le informazioni di connettività relative alla risorsa di storage interessata, visualizzare consigli per la risoluzione dei problemi e assegnare la risoluzione dei problemi ad altri amministratori.

- Configurazione e monitoraggio degli incidenti relativi alle performance

  L'amministratore può monitorare e gestire le performance delle risorse del sistema di storage monitorate. Vedere "Introduzione al monitoraggio delle performance di Active IQ Unified Manager" per ulteriori informazioni.

- Diagnosi e gestione dei problemi di capacità del volume

  Se nella pagina Dashboard vengono visualizzati problemi di capacità dello storage del volume, gli amministratori dello storage possono seguire i collegamenti integrati per visualizzare i trend attuali e storici relativi alla capacità dello storage del volume interessato, visualizzare consigli per la risoluzione dei problemi e assegnare la risoluzione dei problemi ad altri amministratori.

- Configurazione, monitoraggio e diagnosi dei problemi relativi alle relazioni di protezione

  Dopo aver creato e configurato le relazioni di protezione, gli amministratori dello storage possono visualizzare i potenziali problemi relativi alle relazioni di protezione, lo stato corrente delle relazioni di protezione, le informazioni attuali e storiche sul successo dei lavori di protezione sulle relazioni interessate e i consigli per la risoluzione dei problemi. Vedere "Creazione, monitoraggio e risoluzione dei problemi delle relazioni di protezione" per ulteriori informazioni.

- Creazione di file di backup e ripristino dei dati dai file di backup.
- Associazione di oggetti storage con annotazioni

  Associando gli oggetti storage alle annotazioni, gli amministratori dello storage possono filtrare e visualizzare gli eventi correlati agli oggetti storage, consentendo agli amministratori dello storage di assegnare priorità e risolvere i problemi associati agli eventi.

- Utilizzo delle API REST per gestire i cluster visualizzando le informazioni su stato, capacità e performance acquisite da Unified Manager. Vedere "Introduzione alle API REST di Active IQ Unified Manager" per ulteriori informazioni.
- Invio di un pacchetto di supporto al supporto tecnico

  Gli amministratori dello storage possono recuperare e inviare un pacchetto di supporto al supporto tecnico utilizzando la console di manutenzione. I pacchetti di supporto devono essere inviati al supporto tecnico quando il problema richiede una diagnosi e una risoluzione dei problemi più dettagliate rispetto a quanto viene fornito da un messaggio AutoSupport.

Monitoraggio e troubleshooting della disponibilità dei dati

Unified Manager monitora l'affidabilità con cui gli utenti autorizzati possono accedere ai dati memorizzati, avvisa l'utente in caso di condizioni che bloccano o impediscono tale accesso e consente di diagnosticare tali condizioni e assegnarne e monitorarne la risoluzione.

Gli argomenti relativi al workflow di disponibilità in questa sezione descrivono esempi di come un amministratore dello storage può utilizzare l'interfaccia utente Web di Unified Manager per rilevare, diagnosticare e assegnare condizioni hardware e software di risoluzione che influiscono negativamente sulla disponibilità dei dati.

Scansione e risoluzione delle condizioni di inattività del collegamento di interconnessione per il failover dello storage

Questo flusso di lavoro fornisce un esempio di come è possibile eseguire la scansione, valutare e risolvere le condizioni di collegamento di interconnessione di failover dello storage downed. In questo scenario, sei un amministratore che utilizza Unified Manager per cercare i rischi di failover dello storage prima di avviare un aggiornamento della versione di ONTAP sui nodi.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Se le interconnessioni di failover dello storage tra i nodi di coppia ha si guastano durante un tentativo di aggiornamento senza interruzioni, l'aggiornamento non riesce. Pertanto, l'amministratore deve monitorare e confermare l'affidabilità del failover dello storage sui nodi del cluster destinati all'aggiornamento prima dell'avvio di un aggiornamento.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**.
2. Nella pagina di inventario **Gestione eventi**, selezionare **Eventi disponibilità attivi**.
3. Nella parte superiore della colonna **Nome** della pagina di inventario **Gestione eventi**, fare clic su e invio `*failover` nella casella di testo per limitare l'evento da visualizzare agli eventi relativi al failover dello storage.

   Vengono visualizzati tutti gli eventi precedenti relativi alle condizioni di failover dello storage.

   In questo scenario, Unified Manager visualizza l'evento, "Storage failover Interconnect one or more links down" nella sezione Availability Incidents.

4. Se uno o più eventi relativi al failover dello storage vengono visualizzati nella pagina di inventario **Gestione eventi**, attenersi alla seguente procedura:

   a. Fare clic sul collegamento relativo al titolo dell'evento per visualizzare i dettagli dell'evento.

      In questo esempio, fare clic sul titolo dell'evento "Storage failover Interconnect one or more links down".

   Viene visualizzata la pagina Dettagli evento relativa all'evento.

a. Nella pagina Dettagli evento, è possibile eseguire una o più delle seguenti attività:
   - Esaminare il messaggio di errore nel campo cause e valutare il problema.
   - Assegnare l'evento a un amministratore.
   - Riconoscere l'evento.

Informazioni correlate

"Pagina dei dettagli dell'evento"

"Ruoli e funzionalità degli utenti di Unified Manager"

Esecuzione di un'azione correttiva per i collegamenti di interconnessione per il failover dello storage

Quando si visualizza la pagina Dettagli evento di un evento correlato al failover dello storage, è possibile esaminare le informazioni riepilogative della pagina per determinare l'urgenza dell'evento, la possibile causa del problema e la possibile risoluzione del problema.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

In questo scenario di esempio, il riepilogo degli eventi fornito nella pagina Dettagli evento contiene le seguenti informazioni sulla condizione di inattività del collegamento di interconnessione per il failover dello storage:

```
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)
```

Le informazioni sull'evento di esempio indicano che un collegamento di interconnessione di failover dello storage, Link1, tra i nodi di coppia ha aardvark e bonobo è inattivo, ma che il collegamento 0 tra Apple e Boy è attivo. Poiché un collegamento è attivo, l'accesso remoto alla memoria dinamica (RDMA) è ancora in funzione e un processo di failover dello storage può ancora avere successo.

Tuttavia, per garantire che la protezione del failover dello storage e i collegamenti non siano attivi sia

completamente disattivata, si decide di diagnosticare ulteriormente il motivo per cui il collegamento 1 non funziona.

Fasi

1. Dalla pagina dei dettagli **evento**, è possibile fare clic sul collegamento all'evento specificato nel campo origine per ottenere ulteriori dettagli su altri eventi che potrebbero essere correlati alla condizione di inattività del collegamento di interconnessione per il failover dello storage.

   In questo esempio, l'origine dell'evento è il nodo denominato aardvark. Facendo clic sul nome del nodo vengono visualizzati i dettagli ha per la coppia ha interessata, aardvark e bonobo, nella scheda nodi della pagina Cluster / Health Details (Dettagli cluster/salute) e gli altri eventi che si sono verificati di recente sulla coppia ha interessata.

2. Per ulteriori informazioni sull'evento, consultare i **Dettagli ha**.

   In questo esempio, le informazioni rilevanti sono nella tabella Eventi. La tabella mostra l'evento "torage failover Connection one or More link Down `S`", l'ora in cui è stato generato l'evento e, ancora una volta, il nodo da cui ha avuto origine l'evento.

Utilizzando le informazioni sulla posizione del nodo in ha Details (Dettagli ha), richiedere o completare personalmente un'ispezione fisica e la riparazione del problema di failover dello storage sui nodi di coppia ha interessati.

Informazioni correlate

"Pagina dei dettagli dell'evento"

"Ruoli e funzionalità degli utenti di Unified Manager"

Risoluzione dei problemi di volume offline

Questo flusso di lavoro fornisce un esempio di come è possibile valutare e risolvere un evento offline di un volume che Unified Manager potrebbe visualizzare nella pagina di inventario di Event Management. In questo scenario, l'amministratore utilizza Unified Manager per risolvere uno o più eventi offline di un volume.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

I volumi potrebbero essere segnalati offline per diversi motivi:

- L'amministratore di SVM ha deliberatamente portato il volume offline.
- Il nodo del cluster di hosting del volume è inattivo e il failover dello storage verso il partner ha Pair ha si è guastato.
- La SVM (Storage Virtual Machine) di hosting del volume viene arrestata perché il nodo che ospita il volume root di tale SVM non è attivo.
- L'aggregato di hosting del volume è inattivo a causa di un guasto simultaneo di due dischi RAID.

Per confermare o eliminare una o più di queste possibilità, è possibile utilizzare la pagina dell'inventario di gestione degli eventi e le pagine dei dettagli di Cluster/Health, Storage VM/Health e Volume/Health.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**.
2. Nella pagina di inventario **Gestione eventi**, selezionare **Eventi disponibilità attivi**.
3. Fare clic sul collegamento ipertestuale visualizzato per l'evento Volume Offline.

   Viene visualizzata la pagina Dettagli evento per l'incidente di disponibilità.

4. In questa pagina, consultare le note per verificare se l'amministratore di SVM ha portato il volume in questione offline.
5. Nella pagina dei dettagli **evento**, è possibile esaminare le informazioni relative a una o più delle seguenti attività:
   - Esaminare le informazioni visualizzate nel campo cause per ottenere una possibile guida diagnostica.

     In questo esempio, le informazioni nel campo cause informano solo che il volume non è in linea.

   - Controllare l'area Note e aggiornamenti per verificare se l'amministratore di SVM ha deliberatamente portato il volume in questione offline.
   - Fare clic sull'origine dell'evento, in questo caso il volume riportato offline, per ottenere ulteriori informazioni su tale volume.
   - Assegnare l'evento a un amministratore.
   - Riconoscere l'evento o, se necessario, contrassegnarlo come risolto.

Esecuzione di azioni diagnostiche per condizioni di volume offline

Dopo aver effettuato la navigazione nella pagina dei dettagli relativi al volume/salute di un volume che risulta offline, è possibile cercare ulteriori informazioni utili per la diagnosi della condizione di volume offline.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Se il volume segnalato offline non è stato portato deliberatamente offline, il volume potrebbe essere offline per diversi motivi.

A partire dalla pagina dei dettagli relativi a volume/salute del volume offline, è possibile accedere ad altre pagine e riquadri per confermare o eliminare le possibili cause:

- Fare clic sui collegamenti della pagina dei dettagli **Volume / Health** per determinare se il volume non è in linea perché il nodo host è inattivo e se si è verificato un errore anche nel failover dello storage verso il partner ha Pair.

  Vedere "Determinare se una condizione di volume offline è causata da un nodo inattivo".

- Fare clic sui collegamenti della pagina dei dettagli **Volume / Health** per determinare se il volume non è in linea e se la relativa SVM (host Storage Virtual Machine) viene arrestata a causa della disattivazione del nodo che ospita il volume root di tale SVM.

  Vedere "Determinare se un volume è offline e SVM viene arrestato perché un nodo non è attivo".

- Fare clic sui collegamenti della pagina dei dettagli **Volume / Health** per determinare se il volume non è in

linea a causa di dischi rotti nel relativo aggregato host.

Vedere "Determinare se un volume è offline a causa di dischi rotti in un aggregato".

Informazioni correlate

"Ruoli e funzionalità degli utenti di Unified Manager"

Determinare se un volume non è in linea perché il nodo host non è attivo

È possibile utilizzare l'interfaccia utente Web di Unified Manager per confermare o eliminare la possibilità che un volume non sia in linea perché il nodo host non è attivo e che il failover dello storage verso il partner ha Pair non sia riuscito.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Per determinare se la condizione offline del volume è causata da un guasto del nodo di hosting e da un successivo failover dello storage non riuscito, eseguire le seguenti operazioni:

Fasi

1. Individuare e fare clic sul collegamento ipertestuale visualizzato sotto SVM nel riquadro **Related Devices** (dispositivi correlati) della pagina dei dettagli **Volume / Health** del volume offline.

   La pagina Storage VM / Health Details (Dettagli stato/VM di storage) visualizza informazioni sulla SVM (Storage Virtual Machine) di hosting del volume offline.

2. Nel riquadro **Related Devices** (periferiche correlate) della pagina dei dettagli **Storage VM / Health**, individuare e fare clic sul collegamento ipertestuale visualizzato in Volumes (volumi).

   La vista Health: All Volumes (Salute: Tutti i volumi) visualizza una tabella di informazioni su tutti i volumi ospitati dalla SVM.

3. Nell'intestazione della colonna **Health: All Volumes** view state (Stato: Tutti i volumi), fare clic sul simbolo del filtro , Quindi selezionare l'opzione **non in linea**.

   Vengono elencati solo i volumi SVM in stato offline.

4. Nella vista Health: All Volumes (Salute: Tutti i volumi), fare clic sul simbolo della griglia , Quindi selezionare l'opzione **Cluster Nodes** (nodi cluster).

   Potrebbe essere necessario scorrere la casella di selezione della griglia per individuare l'opzione **Cluster Nodes** (nodi cluster).

   La colonna Cluster Nodes (nodi cluster) viene aggiunta all'inventario dei volumi e visualizza il nome del nodo che ospita ciascun volume offline.

5. Nella vista **Health: All Volumes** (Salute: Tutti i volumi), individuare l'elenco del volume offline e, nella colonna Cluster Node (nodo cluster), fare clic sul nome del nodo di hosting.

   La scheda Nodes (nodi) nella pagina Cluster / Health Details (Dettagli cluster/integrità) visualizza lo stato della coppia di nodi ha a cui appartiene il nodo di hosting. Lo stato del nodo di hosting e il successo di qualsiasi operazione di failover del cluster sono indicati sul display.

Dopo aver confermato che la condizione di volume offline esiste perché il nodo host è inattivo e che il failover dello storage verso il partner ha Pair non è riuscito, contattare l'amministratore o l'operatore appropriato per riavviare manualmente il nodo inattivo e risolvere il problema di failover dello storage.

Determinare se un volume non è in linea e se il relativo SVM viene arrestato perché un nodo non è attivo

È possibile utilizzare l'interfaccia utente Web di Unified Manager per confermare o eliminare la possibilità che un volume non sia in linea perché la sua SVM (host Storage Virtual Machine) viene arrestata a causa del nodo che ospita il volume root di tale SVM.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Per determinare se la condizione di volume offline ha causato l'arresto della SVM host perché il nodo che ospita il volume root di tale SVM non è attivo, eseguire le seguenti operazioni:

Fasi

1. Individuare e fare clic sul collegamento ipertestuale visualizzato sotto SVM nel riquadro **Related Devices** (dispositivi correlati) della pagina dei dettagli **Volume / Health** del volume offline.

   La pagina Storage VM / Health details (Dettagli stato di integrità/VM di storage) visualizza lo stato "running" (in esecuzione) o "sracked" (superato) della SVM di hosting. Se lo stato SVM è in esecuzione, la condizione offline del volume non è causata dal nodo che ospita il volume root di tale SVM.

2. Se lo stato SVM viene arrestato, fare clic su **View SVM** (Visualizza SVM) per identificare ulteriormente la causa dell'arresto della SVM in hosting.
3. Nell'intestazione della colonna **Health: All Storage VM** view SVM (Stato: Tutte le macchine virtuali storage), fare clic sul simbolo del filtro Quindi digitare il nome della SVM interrotta.

   Le informazioni relative a tale SVM vengono visualizzate in una tabella.

4. Nella vista **Health: All Storage VMS**, fare clic su Quindi selezionare l'opzione **Volume root**.

   La colonna Volume root viene aggiunta all'inventario SVM e visualizza il nome del volume root della SVM interrotta.

5. Nella colonna Root Volume (Volume principale), fare clic sul nome del volume root per visualizzare la pagina dei dettagli **Storage VM / Health** relativa a tale volume.

   Se lo stato del volume root SVM è (Online), la condizione offline del volume originale non viene causata perché il nodo che ospita il volume root di tale SVM non è attivo.

6. Se lo stato del volume root SVM è (Offline), individuare e fare clic sul collegamento ipertestuale visualizzato sotto aggregato nel riquadro Related Devices (dispositivi correlati) della pagina Volume / Health Details (Dettagli volume/salute) del volume root SVM.
7. Individuare e fare clic sul collegamento ipertestuale visualizzato sotto nodo nel riquadro **Related Devices** (dispositivi correlati) della pagina dei dettagli **aggregate / Health** dell'aggregato.

   La scheda Nodes (nodi) nella pagina Cluster / Health Details (Dettagli cluster/integrità) visualizza lo stato della coppia di nodi ha a cui appartiene il nodo di hosting del volume root SVM. Lo stato del nodo viene indicato nel display.

Dopo aver confermato che la condizione di offline del volume è causata dalla condizione di offline SVM host del volume, causata dal nodo che ospita il volume root di tale SVM, contattare l'amministratore o l'operatore appropriato per riavviare manualmente il nodo inattivo.

Determinare se un volume è offline a causa di dischi rotti in un aggregato

È possibile utilizzare l'interfaccia utente Web di Unified Manager per confermare o eliminare la possibilità che un volume sia offline perché i problemi del disco RAID hanno portato l'aggregato host offline.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Per determinare se la condizione di volume offline è causata da problemi del disco RAID che stanno portando l'aggregato di hosting offline, eseguire le seguenti operazioni:

Fasi

1. Individuare e fare clic sul collegamento ipertestuale visualizzato sotto aggregato nel riquadro **Related Devices** (dispositivi correlati) della pagina dei dettagli **Volume / Health**.

   La pagina aggregato/Dettagli salute visualizza lo stato online o offline dell'aggregato di hosting. Se lo stato aggregato è online, i problemi del disco RAID non sono la causa della offline del volume.

2. Se lo stato aggregato non è in linea, fare clic su **Disk Information** (informazioni disco) e cercare gli eventi del disco guasti nell'elenco **Events** (Eventi) nella scheda **Disk Information** (informazioni disco).
3. Per identificare ulteriormente i dischi rotti, fare clic sul collegamento ipertestuale visualizzato sotto nodo nel riquadro **dispositivi correlati**.

   Viene visualizzata la pagina Cluster / Health details (Dettagli cluster / stato).

4. Fare clic su **Disks**, quindi selezionare **Broken** nel pannello **Filters** per visualizzare tutti i dischi in stato di rottura.

   Se i dischi in stato interrotto hanno causato lo stato offline dell'aggregato host, il nome dell'aggregato viene visualizzato nella colonna aggregato interessato.

Dopo aver confermato che la condizione di volume offline è causata da dischi RAID rotti e dal conseguente aggregato di host offline, contattare l'amministratore o l'operatore appropriato per sostituire manualmente i dischi rotti e riportare l'aggregato online.

Risoluzione dei problemi di capacità

Questo flusso di lavoro fornisce un esempio di come risolvere un problema di capacità. In questo scenario, si è un amministratore o un operatore e si accede alla pagina Unified ManagerDashboard per verificare se uno degli oggetti di storage monitorati presenta problemi di capacità. Si desidera determinare la possibile causa del problema e risolverlo.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Nella pagina Dashboard, cercare un evento di errore “Volume Space Full” nel pannello Capacity (capacità) sotto l’elenco a discesa degli eventi.

Fasi

1. Nel pannello **Capacity** della pagina **Dashboard**, fare clic sul nome dell’evento di errore Volume Space Full.

   Viene visualizzata la pagina Dettagli evento relativa all’errore.

2. Dalla pagina dei dettagli **evento**, è possibile eseguire una o più delle seguenti attività:
   - Esaminare il messaggio di errore nel campo cause (causa) e fare clic sui suggerimenti nella sezione Suggested Remedial Actions (azioni correttive suggerite) per esaminare le descrizioni delle possibili soluzioni.
   - Fare clic sul nome dell’oggetto, in questo caso un volume, nel campo Source (origine) per ottenere i dettagli sull’oggetto.
   - Cercare le note che potrebbero essere state aggiunte a questo evento.
   - Aggiungere una nota all’evento.
   - Assegnare l’evento a un altro utente.
   - Riconoscere l’evento.
   - Contrassegnare l’evento come risolto.

Informazioni correlate

"Pagina dei dettagli dell’evento"

Esecuzione delle azioni correttive suggerite per un volume completo

Dopo aver ricevuto un evento di errore “Volume Space Full”, esaminare le azioni correttive suggerite nella pagina Dettagli evento e decidere di eseguire una delle azioni suggerite.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell’applicazione o di amministratore dello storage.

Un utente con qualsiasi ruolo può eseguire tutte le attività di questo flusso di lavoro che utilizzano Unified Manager.

In questo esempio, è stato visualizzato un evento di errore Volume Space Full nella pagina di inventario di Unified ManagerEvent Management e si è fatto clic sul nome dell’evento.

Le possibili azioni correttive che è possibile eseguire per un volume completo includono quanto segue:

- Attivazione della crescita automatica, della deduplica o della compressione sul volume
- Ridimensionamento o spostamento del volume
- Eliminazione o spostamento dei dati dal volume

Sebbene tutte queste azioni debbano essere eseguite da Gestore di sistema di ONTAP o dall’interfaccia utente di ONTAP, è possibile utilizzare Unified Manager per trovare le informazioni necessarie per determinare le azioni da intraprendere.

Fasi

1. Nella pagina dei dettagli **evento**, fare clic sul nome del volume nel campo origine per visualizzare i dettagli sul volume interessato.
2. Nella pagina dei dettagli **Volume / Health**, fare clic su **Configuration** e verificare che deduplica e compressione siano già attivate sul volume.

   Si decide di ridimensionare il volume.
3. Nel riquadro **Related Devices** (periferiche correlate), fare clic sul nome dell'aggregato di hosting per vedere se l'aggregato può ospitare un volume più grande.
4. Nella pagina dei dettagli **aggregato/integrità**, l'aggregato che ospita l'intero volume ha una capacità non impegnata sufficiente, pertanto è possibile utilizzare Gestione di sistema di ONTAP per ridimensionare il volume, offrendo una maggiore capacità.

Informazioni correlate

"Pagina dei dettagli dell'evento"

Gestione delle soglie di integrità

È possibile configurare i valori delle soglie di integrità globali per tutti gli aggregati, i volumi e i qtree per tenere traccia di eventuali violazioni delle soglie di integrità.

Quali sono le soglie di stato della capacità dello storage

Una soglia di stato della capacità di storage è il punto in cui il server Unified Manager genera eventi per segnalare qualsiasi problema di capacità con gli oggetti di storage. È possibile configurare gli avvisi in modo che inviino notifiche ogni volta che si verificano tali eventi.

Le soglie di integrità della capacità di storage per tutti gli aggregati, i volumi e i qtree sono impostate sui valori predefiniti. È possibile modificare le impostazioni in base alle esigenze di un oggetto o di un gruppo di oggetti.

Configurazione delle impostazioni della soglia di integrità globale

È possibile configurare le condizioni delle soglie di integrità globali per capacità, crescita, Snapshot Reserve, quote e inode per monitorare in modo efficace le dimensioni di aggregato, volume e qtree. È inoltre possibile modificare le impostazioni per la generazione di eventi per il superamento delle soglie di ritardo.

Le impostazioni della soglia di integrità globale si applicano a tutti gli oggetti a cui sono associati, ad esempio aggregati, volumi e così via. Quando vengono superate le soglie, viene generato un evento e, se sono configurati avvisi, viene inviata una notifica di avviso. Le soglie predefinite sono impostate sui valori consigliati, ma è possibile modificarle in modo da generare eventi a intervalli per soddisfare le esigenze specifiche. Quando le soglie vengono modificate, gli eventi vengono generati o resi obsoleti nel ciclo di monitoraggio successivo.

È possibile accedere alle impostazioni della soglia di integrità globale dalla sezione soglie evento del menu di navigazione a sinistra. È inoltre possibile modificare le impostazioni di soglia per singoli oggetti, dalla pagina di inventario o dalla pagina dei dettagli dell'oggetto.

- Per ulteriori informazioni, vedere "Configurazione dei valori globali di soglia di integrità degli aggregati".

  È possibile configurare le impostazioni della soglia di integrità per capacità, crescita e copie Snapshot per tutti gli aggregati per tenere traccia di qualsiasi violazione di soglia.

- Per ulteriori informazioni, vedere "Configurazione dei valori delle soglie globali di integrità del volume".

  È possibile modificare le impostazioni della soglia di integrità per capacità, copie Snapshot, quote qtree, crescita del volume, spazio di riserva di sovrascrittura, e inode per tutti i volumi per tenere traccia di qualsiasi violazione di soglia.

- Per ulteriori informazioni, vedere "Configurazione dei valori globali delle soglie di integrità del qtree".

  È possibile modificare le impostazioni della soglia di integrità per la capacità di tutti i qtree per tenere traccia di qualsiasi violazione di soglia.

- Per ulteriori informazioni, vedere "Modifica delle impostazioni della soglia di integrità del ritardo per le relazioni di protezione non gestite".

  È possibile aumentare o ridurre la percentuale di tempo di avviso o ritardo degli errori in modo che gli eventi vengano generati a intervalli più adatti alle proprie esigenze.

Configurazione dei valori globali di soglia di integrità degli aggregati

È possibile configurare i valori delle soglie globali di integrità per tutti gli aggregati per tenere traccia di qualsiasi violazione di soglia. Gli eventi appropriati vengono generati per le violazioni di soglia ed è possibile adottare misure preventive in base a tali eventi. È possibile configurare i valori globali in base alle impostazioni delle Best practice per le soglie applicabili a tutti gli aggregati monitorati.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Quando si configurano le opzioni a livello globale, i valori predefiniti degli oggetti vengono modificati. Tuttavia, se i valori predefiniti sono stati modificati a livello di oggetto, i valori globali non vengono modificati.

Le opzioni di soglia hanno valori predefiniti per un migliore monitoraggio, tuttavia è possibile modificare i valori in base ai requisiti dell'ambiente.

Quando la funzione di crescita automatica è attivata sui volumi che risiedono nell'aggregato, le soglie della capacità aggregata vengono considerate violate in base alle dimensioni massime del volume impostate dalla funzione di crescita automatica, non in base alle dimensioni originali del volume.

I valori della soglia di integrità non sono applicabili all'aggregato root del nodo.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **soglie evento** > **aggregato**.
2. Configurare i valori di soglia appropriati per capacità, crescita e copie Snapshot.
3. Fare clic su **Save** (Salva).

Informazioni correlate

"Aggiunta di utenti"

Configurazione dei valori delle soglie globali di integrità del volume

È possibile configurare i valori della soglia di integrità globale per tutti i volumi per tenere traccia di qualsiasi violazione di soglia. Gli eventi appropriati vengono generati per le violazioni delle soglie di salute ed è possibile adottare misure preventive in base a tali eventi. È possibile configurare i valori globali in base alle impostazioni delle Best practice per le soglie applicabili a tutti i volumi monitorati.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

La maggior parte delle opzioni di soglia dispone di valori predefiniti per un migliore monitoraggio. Tuttavia, è possibile modificare i valori in base ai requisiti del proprio ambiente.

Si noti che quando la funzione di crescita automatica è attivata su un volume, le soglie di capacità vengono considerate violate in base alle dimensioni massime del volume impostate dalla crescita automatica, non in base alle dimensioni originali del volume.

> Il valore predefinito di 1000 copie Snapshot è applicabile solo ai volumi FlexVol quando la versione di ONTAP è 9.4 o superiore e ai volumi FlexGroup quando la versione di ONTAP è 9.8 o superiore. Per i cluster installati con versioni precedenti del software ONTAP, il numero massimo è 250 copie Snapshot per volume. Per queste versioni precedenti, Unified Manager interpreta questo numero 1000 (e qualsiasi numero compreso tra 1000 e 250) come 250; ciò significa che continuerai a ricevere eventi quando il numero di copie Snapshot raggiunge 250. Se si desidera impostare questa soglia su un valore inferiore a 250 per queste versioni precedenti, è necessario impostare la soglia su 250 o inferiore nella vista Health: All Volumes (Salute: Tutti i volumi) o nella pagina Volume / Health Details (Dettagli volume/salute).

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **soglie evento** > **Volume**.
2. Configurare i valori di soglia appropriati per capacità, copie Snapshot, quote qtree, crescita del volume e inode.
3. Fare clic su **Save** (Salva).

Informazioni correlate

"Aggiunta di utenti"

Configurazione dei valori globali delle soglie di integrità del qtree

È possibile configurare i valori della soglia di integrità globale per tutti i qtree per tenere traccia di qualsiasi violazione di soglia. Gli eventi appropriati vengono generati per le violazioni delle soglie di salute ed è possibile adottare misure preventive in base a tali eventi. È possibile configurare i valori globali in base alle impostazioni delle Best practice per le soglie applicabili a tutti i qtree monitorati.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Le opzioni di soglia hanno valori predefiniti per un migliore monitoraggio, tuttavia è possibile modificare i valori in base ai requisiti dell'ambiente.

Gli eventi vengono generati per un qtree solo quando è stata impostata una quota Qtree o una quota predefinita nel qtree. Gli eventi non vengono generati se lo spazio definito in una quota utente o di gruppo ha superato la soglia.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **soglie evento** > **Qtree**.
2. Configurare i valori di soglia della capacità appropriati.
3. Fare clic su **Save** (Salva).

Configurazione delle impostazioni delle soglie di ritardo per le relazioni di protezione non gestite

È possibile modificare le impostazioni globali predefinite di avviso di ritardo e soglia di stato degli errori per le relazioni di protezione non gestite in modo che gli eventi vengano generati a intervalli appropriati alle proprie esigenze.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Il tempo di ritardo non deve superare l'intervallo di pianificazione del trasferimento definito. Ad esempio, se la pianificazione del trasferimento è oraria, il tempo di ritardo non deve essere superiore a un'ora. La soglia di ritardo specifica una percentuale che il tempo di ritardo non deve superare. Utilizzando l'esempio di un'ora, se la soglia di ritardo è definita come 150%, si riceverà un evento quando il tempo di ritardo è superiore a 1.5 ore.

Le impostazioni descritte in questa attività vengono applicate globalmente a tutte le relazioni di protezione non gestite. Le impostazioni non possono essere specificate e applicate esclusivamente a una relazione di protezione non gestita.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **soglie evento** > **relazione**.
2. Aumentare o ridurre la percentuale di tempo di avviso o ritardo degli errori predefinita globale, secondo necessità.
3. Per disattivare l'attivazione di un evento di avviso o di errore da qualsiasi valore di soglia di ritardo, deselezionare la casella accanto a **Enabled** (attivato).
4. Fare clic su **Save** (Salva).

Informazioni correlate

"Aggiunta di utenti"

Modifica delle impostazioni delle singole soglie di integrità aggregate

È possibile modificare le impostazioni della soglia di integrità per capacità aggregata, crescita e copie Snapshot di uno o più aggregati. Quando viene superata una soglia, vengono generati avvisi e vengono ricevute notifiche. Queste notifiche consentono di adottare misure preventive in base all'evento generato.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

In base alle modifiche apportate ai valori di soglia, gli eventi vengono generati o resi obsoleti nel ciclo di monitoraggio successivo.

Quando la funzione di crescita automatica è attivata sui volumi che risiedono nell'aggregato, le soglie della capacità aggregata vengono considerate violate in base alle dimensioni massime del volume impostate dalla funzione di crescita automatica, non in base alle dimensioni originali del volume.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates**.
2. Nella vista **Health: Tutti gli aggregati**, selezionare uno o più aggregati, quindi fare clic su **Edit thresholds** (Modifica soglie).
3. Nella finestra di dialogo **Edit aggregate thresholds** (Modifica soglie aggregate), modificare le impostazioni di una delle seguenti soglie: Capacità, crescita o copie Snapshot selezionando la casella di controllo appropriata e modificando le impostazioni.
4. Fare clic su **Save** (Salva).

Informazioni correlate

"Aggiunta di utenti"

Modifica delle impostazioni delle soglie di integrità dei singoli volumi

È possibile modificare le impostazioni della soglia di integrità per capacità del volume, crescita, quota e riserva di spazio di uno o più volumi. Quando viene superata una soglia, vengono generati avvisi e vengono ricevute notifiche. Queste notifiche consentono di adottare misure preventive in base all'evento generato.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

In base alle modifiche apportate ai valori di soglia, gli eventi vengono generati o resi obsoleti nel ciclo di monitoraggio successivo.

Si noti che quando la funzione di crescita automatica è attivata su un volume, le soglie di capacità vengono considerate violate in base alle dimensioni massime del volume impostate dalla crescita automatica, non in base alle dimensioni originali del volume.

> Il valore predefinito di 1000 copie Snapshot è applicabile solo ai volumi FlexVol quando la versione di ONTAP è 9.4 o superiore e ai volumi FlexGroup quando la versione di ONTAP è 9.8 o superiore. Per i cluster installati con versioni precedenti del software ONTAP, il numero massimo è 250 copie Snapshot per volume. Per queste versioni precedenti, Unified Manager interpreta questo numero 1000 (e qualsiasi numero compreso tra 1000 e 250) come 250; ciò significa che continuerai a ricevere eventi quando il numero di copie Snapshot raggiunge 250. Se si desidera impostare questa soglia su un valore inferiore a 250 per queste versioni precedenti, è necessario impostare la soglia su 250 o inferiore nella vista Health: All Volumes (Salute: Tutti i volumi) o nella pagina Volume / Health Details (Dettagli volume/salute).

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nella vista **Health: All Volumes** (Salute: Tutti i volumi), selezionare uno o più volumi, quindi fare clic su **Edit Thresholds** (Modifica soglie).
3. Nella finestra di dialogo **Edit Volume Thresholds** (Modifica soglie volume), modificare le impostazioni di soglia di una delle seguenti opzioni: Capacità, copie Snapshot, quota qtree, crescita o inode selezionando la casella di controllo appropriata e modificando le impostazioni.
4. Fare clic su **Save** (Salva).

Informazioni correlate

"Aggiunta di utenti"

Modifica delle singole impostazioni delle soglie di integrità di qtree

È possibile modificare le impostazioni della soglia di integrità per la capacità di qtree per uno o più qtree. Quando viene superata una soglia, vengono generati avvisi e vengono ricevute notifiche. Queste notifiche consentono di adottare misure preventive in base all'evento generato.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

In base alle modifiche apportate ai valori di soglia, gli eventi vengono generati o resi obsoleti nel ciclo di monitoraggio successivo.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Qtree**.
2. Nella vista **capacità: Tutti i Qtree**, selezionare uno o più qtree, quindi fare clic su **Modifica soglie**.
3. Nella finestra di dialogo **Edit Qtree thresholds** (Modifica soglie Qtree), modificare le soglie di capacità per il qtree o i qtree selezionati e fare clic su **Save** (Salva).

> È inoltre possibile impostare singole soglie qtree dalla scheda Qtree nella pagina Storage VM / Health details.

Gestione degli obiettivi di sicurezza del cluster

Unified Manager offre una dashboard che identifica la sicurezza dei cluster ONTAP, delle macchine virtuali di storage e dei volumi in base ai consigli definiti nella *Guida per l'aumento della sicurezza NetApp per ONTAP 9*.

L'obiettivo della dashboard di sicurezza è mostrare le aree in cui i cluster ONTAP non sono allineati con le linee guida consigliate da NetApp, in modo da poter risolvere questi potenziali problemi. Nella maggior parte dei casi, è possibile risolvere i problemi utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP. La tua organizzazione potrebbe non seguire tutti i consigli, quindi in alcuni casi non sarà necessario apportare modifiche.

Per consigli e risoluzioni dettagliate, vedere "Guida al rafforzamento della sicurezza di NetApp per ONTAP 9"

(TR-4569).

Oltre a segnalare lo stato di sicurezza, Unified Manager genera anche eventi di sicurezza per qualsiasi cluster o SVM che presenta violazioni della sicurezza. È possibile tenere traccia di questi problemi nella pagina di inventario di Event Management ed è possibile configurare gli avvisi per questi eventi in modo che l'amministratore dello storage riceva una notifica quando si verificano nuovi eventi di sicurezza.

Per ulteriori informazioni, vedere "Quali criteri di sicurezza vengono valutati".

Quali criteri di sicurezza vengono valutati

In generale, i criteri di sicurezza per i cluster ONTAP, le macchine virtuali di storage (SVM) e i volumi vengono valutati in base ai consigli definiti nella *Guida per l'aumento della protezione di NetApp per ONTAP 9*.

Alcuni dei controlli di sicurezza includono:

- Se un cluster utilizza un metodo di autenticazione sicuro, ad esempio SAML
- se i cluster peered hanno la loro comunicazione crittografata
- Se una VM storage ha attivato il registro di controllo
- sia che i volumi dispongano della crittografia software o hardware abilitata

Per informazioni dettagliate, vedere gli argomenti relativi alle categorie di conformità e "Guida al rafforzamento della sicurezza di NetApp per ONTAP 9" .

> Anche gli eventi di upgrade riportati dalla piattaforma Active IQ sono considerati eventi di sicurezza. Questi eventi identificano i problemi in cui la risoluzione richiede l'aggiornamento del software ONTAP, del firmware del nodo o del software del sistema operativo (per gli avvisi di sicurezza). Questi eventi non vengono visualizzati nel pannello sicurezza, ma sono disponibili nella pagina inventario gestione eventi.

Per ulteriori informazioni, vedere "Gestione degli obiettivi di sicurezza del cluster".

Categorie di compliance del cluster

Questa tabella descrive i parametri di conformità della sicurezza del cluster che Unified Manager valuta, i consigli di NetApp e se il parametro influisce sulla determinazione generale del cluster che presenta un reclamo o meno.

La presenza di SVM non conformi su un cluster influisce sul valore di conformità del cluster. Pertanto, in alcuni casi potrebbe essere necessario risolvere problemi di sicurezza con una SVM prima che la sicurezza del cluster venga considerata conforme.

Si noti che non tutti i parametri elencati di seguito vengono visualizzati per tutte le installazioni. Ad esempio, se non si dispone di cluster peered o se AutoSupport è stato disattivato su un cluster, gli elementi di peering cluster o trasporto HTTPS AutoSupport non verranno visualizzati nella pagina dell'interfaccia utente.

Parametro	Descrizione	Consiglio	Influisce sulla conformità del cluster
FIPS globale	Indica se la modalità di conformità Global FIPS (Federal Information Processing Standard) 140-2 è attivata o disattivata. Quando FIPS è attivato, TLSv1 e SSLv3 sono disattivati e sono consentiti solo TLSv1.1 e TLSv1.2.	Attivato	Sì
Telnet	Indica se l'accesso Telnet al sistema è attivato o disattivato. NetApp consiglia Secure Shell (SSH) per un accesso remoto sicuro.	Disattivato	Sì
Impostazioni SSH non sicure	Indica se SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con *cbc.	No	Sì
Banner di accesso	Indica se il banner di accesso è attivato o disattivato per gli utenti che accedono al sistema.	Attivato	Sì
Peering dei cluster	Indica se la comunicazione tra i cluster in peering è crittografata o non crittografata. La crittografia deve essere configurata sia sul cluster di origine che su quello di destinazione affinché questo parametro sia considerato conforme.	Crittografato	Sì
Network Time Protocol	Indica se il cluster dispone di uno o più server NTP configurati. Per la ridondanza e il miglior servizio, NetApp consiglia di associare almeno tre server NTP al cluster.	Configurato	Sì

Parametro	Descrizione	Consiglio	Influisce sulla conformità del cluster
OCSP	Indica se in ONTAP sono presenti applicazioni non configurate con OCSP (Online Certificate Status Protocol) e quindi le comunicazioni non sono crittografate. Vengono elencate le applicazioni non conformi.	Attivato	No
Log di controllo remoto	Indica se l'inoltro dei log (Syslog) è crittografato o meno.	Crittografato	Sì
Trasporto HTTPS AutoSupport	Indica se HTTPS è utilizzato come protocollo di trasporto predefinito per l'invio di messaggi AutoSupport al supporto NetApp.	Attivato	Sì
Admin User predefinito	Indica se l'utente amministratore predefinito (incorporato) è attivato o disattivato. NetApp consiglia di bloccare (disabilitare) gli account integrati non necessari.	Disattivato	Sì
Utenti SAML	Indica se SAML è configurato. SAML consente di configurare l'autenticazione a più fattori (MFA) come metodo di accesso per il single sign-on.	No	No
Utenti di Active Directory	Indica se Active Directory è configurato. Active Directory e LDAP sono i meccanismi di autenticazione preferiti per gli utenti che accedono ai cluster.	No	No

Parametro	Descrizione	Consiglio	Influisce sulla conformità del cluster
Utenti LDAP	Indica se LDAP è configurato. Active Directory e LDAP sono i meccanismi di autenticazione preferiti per gli utenti che gestiscono i cluster su utenti locali.	No	No
Utenti certificati	Indica se un utente certificato è configurato per accedere al cluster.	No	No
Utenti locali	Indica se gli utenti locali sono configurati per l'accesso al cluster.	No	No
Shell remota	Indica se RSH è attivato. Per motivi di sicurezza, RSH deve essere disattivato. È preferibile utilizzare Secure Shell (SSH) per un accesso remoto sicuro.	Disattivato	Sì
MD5 in uso	Indica se gli account utente ONTAP utilizzano una funzione hash MD5 meno sicura. Si preferisce la migrazione degli account utente con hash MD5 alla funzione hash crittografica più sicura come SHA-512.	No	Sì
Tipo di autorità di certificazione	Indica il tipo di certificato digitale utilizzato.	Firma CA	No

Categorie di conformità delle VM di storage

Questa tabella descrive i criteri di conformità della sicurezza SVM (Storage Virtual Machine) che Unified Manager valuta, i consigli di NetApp e se il parametro influisce sulla determinazione generale della SVM che presenta un reclamo o meno.

Parametro	Descrizione	Consiglio	Influisce sulla conformità SVM
Log di audit	Indica se la registrazione dell'audit è attivata o disattivata.	Attivato	Sì
Impostazioni SSH non sicure	Indica se SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con `cbc*`.	No	Sì
Banner di accesso	Indica se il banner di accesso è attivato o disattivato per gli utenti che accedono alle SVM sul sistema.	Attivato	Sì
Crittografia LDAP	Indica se la crittografia LDAP è attivata o disattivata.	Attivato	No
Autenticazione NTLM	Indica se l'autenticazione NTLM è attivata o disattivata.	Attivato	No
Firma del payload LDAP	Indica se la firma del payload LDAP è attivata o disattivata.	Attivato	No
Impostazioni CHAP	Indica se CHAP è attivato o disattivato.	Attivato	No
Kerberos V5	Indica se l'autenticazione Kerberos V5 è attivata o disattivata.	Attivato	No
Autenticazione NIS	Indica se è configurato l'utilizzo dell'autenticazione NIS.	Disattivato	No
Stato FPolicy attivo	Indica se FPolicy è stato creato o meno.	Sì	No
Crittografia SMB attivata	Indica se SMB -signing & sealing non è abilitato.	Sì	No
Firma SMB abilitata	Indica se la firma SMB non è abilitata.	Sì	No

Categorie di compliance ai volumi

Questa tabella descrive i parametri di crittografia del volume che Unified Manager valuta per determinare se i dati sui volumi sono adeguatamente protetti dall'accesso da parte di utenti non autorizzati.

Si noti che i parametri di crittografia del volume non influiscono sul fatto che la VM del cluster o dello storage sia considerata conforme.

Parametro	Descrizione
Software crittografato	Visualizza il numero di volumi protetti mediante le soluzioni di crittografia software NetApp Volume Encryption (NVE) o NetApp aggregate Encryption (NAE).
Crittografia hardware	Visualizza il numero di volumi protetti mediante la crittografia hardware NetApp Storage Encryption (NSE).
Crittografia software e hardware	Visualizza il numero di volumi protetti dalla crittografia software e hardware.
Non crittografato	Visualizza il numero di volumi non crittografati.

Cosa significa non conformità

I cluster e le macchine virtuali di storage (SVM) sono considerati non conformi quando uno qualsiasi dei criteri di sicurezza valutati in base alle raccomandazioni definite nella *Guida per l'hardware di sicurezza NetApp per ONTAP 9* non viene soddisfatto. Inoltre, un cluster viene considerato non conforme quando una SVM viene contrassegnata come non conforme.

Le icone di stato nelle schede di sicurezza hanno i seguenti significati in relazione alla loro conformità:

- - Il parametro viene configurato come consigliato.
- - Il parametro non è configurato come consigliato.
- - La funzionalità non è attivata sul cluster o il parametro non è configurato come consigliato, ma questo parametro non contribuisce alla compliance dell'oggetto.

Si noti che lo stato di crittografia del volume non contribuisce a stabilire se il cluster o la SVM sono considerati conformi.

Visualizzazione dello stato di sicurezza per cluster e VM di storage

Active IQ Unified Manager consente di visualizzare lo stato di sicurezza degli oggetti di storage nell'ambiente da diversi punti dell'interfaccia. È possibile raccogliere e analizzare informazioni e report in base a parametri definiti e rilevare comportamenti sospetti o modifiche di sistema non autorizzate sui cluster monitorati e sulle VM di storage.

Per i consigli sulla protezione, consultare la "Guida al rafforzamento della sicurezza di NetApp per ONTAP 9"

Visualizzare lo stato di sicurezza a livello di oggetto nella pagina Security

In qualità di amministratore di sistema, è possibile utilizzare la pagina **sicurezza** per ottenere visibilità sul livello di sicurezza dei cluster ONTAP e delle VM di storage a livello di data center e sito. Gli oggetti supportati sono cluster, VM di storage e volumi. Attenersi alla seguente procedura:

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Dashboard**.
2. A seconda che si desideri visualizzare lo stato di sicurezza per tutti i cluster monitorati o per un singolo cluster, selezionare **tutti i cluster** o selezionare un singolo cluster dal menu a discesa.
3. Fare clic sulla freccia destra nel pannello **Security**. Viene visualizzata la pagina Security (sicurezza).

Facendo clic sui grafici a barre, sui conteggi e. `View Reports` I collegamenti consentono di accedere alla pagina Volumes (volumi), Clusters (Clusters) o Storage VM (Storage VM) per visualizzare i dettagli corrispondenti o generare report, in base alle esigenze.

La pagina Security (sicurezza) visualizza i seguenti pannelli:

- **Cluster Compliance**: Stato di sicurezza (numero di cluster conformi o non conformi) di tutti i cluster di un data center
- **Storage VM Compliance**: Lo stato di sicurezza (numero di storage VM conformi o non conformi) per tutte le storage VM del data center
- **Volume Encryption**: Stato della crittografia del volume (numero di volumi crittografati o non crittografati) di tutti i volumi dell'ambiente
- **Volume Anti-ransomware Status**: Stato di sicurezza (numero di volumi con anti-ransomware attivato o disattivato) di tutti i volumi nel tuo ambiente
- **Cluster Authentication and Certificates**: Numero di cluster che utilizzano ciascun tipo di metodo di autenticazione, ad esempio SAML, Active Directory o tramite certificati e autenticazione locale. Il pannello visualizza anche il numero di cluster i cui certificati sono scaduti o stanno per scadere tra 60 giorni.

Visualizza i dettagli di sicurezza di tutti i cluster nella pagina Clusters

La pagina dei dettagli **Clusters / Security** consente di visualizzare lo stato di conformità della sicurezza a livello di cluster.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage > Clusters**.
2. Selezionare **Visualizza > sicurezza > tutti i cluster**.

Parametri di sicurezza predefiniti, come Global FIPS, Telnet, impostazioni SSH non sicure, banner di accesso, protocollo temporale di rete, Vengono visualizzati trasporto HTTPS AutoSupport e lo stato della scadenza del certificato del cluster.

Fare clic su ⋮ Pulsante More options (altre opzioni) e scegliere di visualizzare i dettagli di sicurezza nella pagina **Security** di Unified Manager o in System Manager. È necessario disporre di credenziali valide per visualizzare i dettagli in System Manager.

Se un cluster dispone di un certificato scaduto, fare clic su `expired` Sotto **Cluster Certificate Valid**, e rinnovarlo da System Manager (9.10.1 e versioni successive). Non è possibile fare clic su `expired` Se l'istanza di System Manager è di una release precedente alla 9.10.1.

Visualizza i dettagli di sicurezza di tutti i cluster dalla pagina delle VM di storage

La pagina dei dettagli **Storage VM / Security** consente di visualizzare lo stato di conformità della sicurezza a livello di storage VM.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage > Storage VM**.
2. Selezionare **Visualizza > sicurezza > tutte le macchine virtuali storage**. Viene visualizzato un elenco di cluster con i parametri di sicurezza.

È possibile avere una vista predefinita della conformità di sicurezza delle VM di storage controllando i parametri di sicurezza, come le VM di storage, il cluster, il banner di accesso, il log di audit e le impostazioni SSH non sicure.

Fare clic su ⋮ Pulsante More options (altre opzioni) e scegliere di visualizzare i dettagli di sicurezza nella pagina **Security** di Unified Manager o in System Manager. È necessario disporre di credenziali valide per visualizzare i dettagli in System Manager.

Per informazioni sulla sicurezza anti-ransomware per volumi e macchine virtuali storage, vedere "Visualizzazione dello stato anti-ransomware di tutti i volumi e le VM di storage".

Visualizzazione di eventi di sicurezza che potrebbero richiedere aggiornamenti software o firmware

Alcuni eventi di sicurezza hanno un'area di impatto di "Upgrade". Questi eventi vengono segnalati dalla piattaforma Active IQ e identificano i problemi in cui la risoluzione richiede l'aggiornamento del software ONTAP, del firmware del nodo o del software del sistema operativo (per gli avvisi di sicurezza).

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Potrebbe essere necessario eseguire un'azione correttiva immediata per alcuni di questi problemi, mentre altri potrebbero essere in grado di attendere la successiva manutenzione pianificata. È possibile visualizzare tutti questi eventi e assegnarli agli utenti in grado di risolvere i problemi. Inoltre, se esistono alcuni eventi di aggiornamento della protezione che non si desidera ricevere notifiche, questo elenco può aiutare a identificare tali eventi in modo da poterli disattivare.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**.

   Per impostazione predefinita, tutti gli eventi attivi (nuovi e riconosciuti) vengono visualizzati nella pagina di inventario Gestione eventi.

2. Dal menu View (Visualizza), selezionare **Upgrade events** (Aggiorna eventi).

   Nella pagina vengono visualizzati tutti gli eventi di protezione dell'aggiornamento attivi.

Visualizzazione del modo in cui viene gestita l'autenticazione dell'utente su tutti i cluster

La pagina Security (sicurezza) visualizza i tipi di autenticazione utilizzati per autenticare gli utenti su ciascun cluster e il numero di utenti che accedono al cluster utilizzando ciascun tipo. In questo modo è possibile verificare che l'autenticazione dell'utente venga eseguita in modo sicuro, come definito dall'organizzazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Dashboard**.
2. Nella parte superiore della dashboard, selezionare **tutti i cluster** dal menu a discesa.
3. Fare clic sulla freccia destra nel pannello **Security** (sicurezza) per visualizzare la pagina **Security** (protezione).
4. Visualizzare la scheda **Cluster Authentication** per visualizzare il numero di utenti che accedono al sistema utilizzando ciascun tipo di autenticazione.
5. Visualizzare la scheda **Cluster Security** per visualizzare i meccanismi di autenticazione utilizzati per autenticare gli utenti su ciascun cluster.

Se alcuni utenti accedono al sistema utilizzando un metodo non sicuro o utilizzando un metodo non consigliato da NetApp, è possibile disattivare il metodo.

Visualizzazione dello stato di crittografia di tutti i volumi

È possibile visualizzare un elenco di tutti i volumi e il relativo stato di crittografia corrente per determinare se i dati presenti nei volumi sono adeguatamente protetti dall'accesso da parte di utenti non autorizzati.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

I tipi di crittografia che è possibile applicare a un volume sono:

- Software - volumi protetti mediante le soluzioni di crittografia software NetApp Volume Encryption (NVE) o NetApp aggregate Encryption (NAE).
- Hardware - volumi protetti mediante crittografia hardware NetApp Storage Encryption (NSE).
- Software e hardware - volumi protetti dalla crittografia software e hardware.
- None (Nessuno) - volumi non crittografati.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu View (Visualizza), selezionare **Health** > **Volumes Encryption** (crittografia volumi)
3. Nella vista **Health: Volumes Encryption**, ordinare il campo **Encryption Type** oppure utilizzare il filtro per visualizzare i volumi con un tipo di crittografia specifico o che non sono crittografati (tipo di crittografia "None").

Visualizzazione dello stato anti-ransomware di tutti i volumi e le VM di storage

È possibile visualizzare un elenco di tutti i volumi e le VM di storage (SVM) e il relativo

stato anti-ransomware corrente per determinare se i dati sui volumi e sulle SVM sono adeguatamente protetti da attacchi ransomware.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Per ulteriori informazioni sui diversi stati anti-ransomware, vedere "ONTAP: Attiva l'anti-ransomware".

Visualizza i dettagli di sicurezza di tutti i volumi con rilevamento anti-ransomware

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu Visualizza, selezionare **Health** > **Security** > **Anti-ransomware**
3. Nella vista **Security: Anti-ransomware**, è possibile ordinare in base ai diversi campi o utilizzare il filtro.

> L'anti-ransomware non è supportato per volumi offline, volumi limitati, volumi SnapLock, volumi FlexGroup, volumi FlexCache, Volumi solo SAN, volumi di macchine virtuali storage bloccate, volumi root di macchine virtuali storage o volumi di protezione dei dati.

Visualizza i dettagli di sicurezza di tutte le VM storage con rilevamento anti-ransomware

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage > Storage VM**.
2. Selezionare **Visualizza > sicurezza > Anti-ransomware**. Viene visualizzato un elenco di SVM con lo stato anti-ransomware.

> Il monitoraggio anti-ransomware non è supportato sulle macchine virtuali storage che non hanno attivato il protocollo NAS.

Visualizzazione di tutti gli eventi di sicurezza attivi

È possibile visualizzare tutti gli eventi di protezione attivi e assegnarli a un utente in grado di risolvere il problema. Inoltre, se alcuni eventi di protezione non si desidera ricevere, questo elenco può aiutare a identificare gli eventi che si desidera disattivare.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Gestione eventi**.

   Per impostazione predefinita, gli eventi nuovi e confermati vengono visualizzati nella pagina di inventario Gestione eventi.

2. Dal menu View (Visualizza), selezionare **Active Security events** (Eventi di sicurezza attivi).

   La pagina visualizza tutti gli eventi New e Acknowledged Security generati negli ultimi 7 giorni.

Aggiunta di avvisi per eventi di sicurezza

È possibile configurare gli avvisi per singoli eventi di sicurezza come qualsiasi altro evento ricevuto da Unified Manager. Inoltre, se si desidera trattare tutti gli eventi di sicurezza allo stesso modo e inviare messaggi e-mail alla stessa persona, è possibile creare un singolo avviso per notificare l'attivazione di qualsiasi evento di sicurezza.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

L'esempio seguente mostra come creare un avviso per l'evento di protezione "Telnet Protocol enabled". In questo modo viene inviato un avviso se l'accesso Telnet è configurato per l'accesso amministrativo remoto al cluster. È possibile utilizzare questa stessa metodologia per creare avvisi per tutti gli eventi di sicurezza.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina **Alert Setup**, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo **Aggiungi avviso**, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.
4. Fare clic su **Resources** (risorse) e selezionare il cluster o il cluster in cui si desidera attivare l'avviso.
5. Fare clic su **Eventi** ed eseguire le seguenti operazioni:
   a. Nell'elenco gravità evento, selezionare **Avviso**.
   b. Nell'elenco Eventi corrispondenti, selezionare **protocollo Telnet attivato**.
6. Fare clic su **azioni**, quindi selezionare il nome dell'utente che riceverà l'e-mail di avviso nel campo **Avvisa questi utenti**.
7. Configurare le altre opzioni di questa pagina per la frequenza di notifica, l'emissione di tap SNMP e l'esecuzione di uno script.
8. Fare clic su **Save** (Salva).

Disattivazione di eventi di sicurezza specifici

Tutti gli eventi sono attivati per impostazione predefinita. È possibile disattivare eventi specifici per impedire la generazione di notifiche per gli eventi che non sono importanti nel proprio ambiente. È possibile attivare gli eventi disattivati se si desidera riprendere la ricezione delle notifiche.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Quando si disattivano gli eventi, gli eventi precedentemente generati nel sistema vengono contrassegnati come obsoleti e gli avvisi configurati per tali eventi non vengono attivati. Quando si abilitano eventi disattivati, le notifiche per questi eventi vengono generate a partire dal ciclo di monitoraggio successivo.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Event Setup**.
2. Nella pagina impostazione **evento**, disattivare o attivare gli eventi scegliendo una delle seguenti opzioni:

Se si desidera…	Quindi…
Disattivare gli eventi	a. Fare clic su **Disable** (Disattiva). b. Nella finestra di dialogo Disable Events (Disattiva eventi), selezionare la severità **Warning**. Questa è la categoria per tutti gli eventi di sicurezza. c. Nella colonna Eventi corrispondenti, selezionare gli eventi di protezione che si desidera disattivare, quindi fare clic sulla freccia destra per spostarli nella colonna Disable Events (Disattiva eventi). d. Fare clic su **Save and Close** (Salva e chiudi). e. Verificare che gli eventi disattivati siano visualizzati nella vista elenco della pagina impostazione eventi.
Attivare gli eventi	a. Dall'elenco degli eventi disattivati, selezionare la casella di controllo corrispondente all'evento o agli eventi che si desidera riabilitare. b. Fare clic su **Enable** (attiva).

Eventi di sicurezza

Gli eventi di sicurezza forniscono informazioni sullo stato di sicurezza dei cluster ONTAP, delle macchine virtuali di storage e dei volumi in base ai parametri definiti nella *Guida al rafforzamento della sicurezza NetApp per ONTAP 9*. Questi eventi notificano potenziali problemi in modo da poterne valutare la severità e, se necessario, risolvere il problema.

Gli eventi di sicurezza sono raggruppati per tipo di origine e includono il nome dell'evento e del trap, il livello di impatto e la severità. Questi eventi vengono visualizzati nelle categorie di eventi delle macchine virtuali del cluster e dello storage.

Gestione delle operazioni di backup e ripristino

È possibile creare backup di Active IQ Unified Manager e utilizzare la funzione di ripristino per ripristinare il backup sullo stesso sistema (locale) o su un nuovo sistema (remoto) in caso di guasto del sistema o perdita di dati.

Esistono tre metodi di backup e ripristino a seconda del sistema operativo su cui è stato installato Unified Manager e in base al numero di cluster e nodi gestiti:

Sistema operativo	Dimensione dell'implementazione	Metodo di backup consigliato
VMware vSphere	Qualsiasi	Snapshot VMware dell'appliance virtuale Unified Manager

Sistema operativo	Dimensione dell'implementazione	Metodo di backup consigliato
Red Hat Enterprise Linux o CentOS Linux	Piccolo	Dump del database MySQL di Unified Manager
	Grande	NetApp Snapshot del database Unified Manager
Microsoft Windows	Piccolo	Dump del database MySQL di Unified Manager
	Grande	NetApp Snapshot del database Unified Manager con protocollo iSCSI

Questi diversi metodi sono descritti nelle sezioni che seguono.

Backup e ripristino per Unified Manager su appliance virtuali

Il modello di backup e ripristino per Unified Manager installato su un'appliance virtuale consiste nell'acquisire e ripristinare un'immagine dell'applicazione virtuale completa.

Le seguenti attività consentono di completare un backup dell'appliance virtuale:

1. Spegnere la macchina virtuale e acquisire un'istantanea VMware dell'appliance virtuale Unified Manager.
2. Creare una copia Snapshot di NetApp sul datastore per acquisire lo snapshot di VMware.

   Se il datastore non è ospitato su un sistema che esegue il software ONTAP, seguire le linee guida del vendor dello storage per creare un backup dello snapshot VMware.

3. Replicare la copia Snapshot di NetApp, o snapshot equivalente, su uno storage alternativo.
4. Eliminare lo snapshot VMware.

È necessario implementare una pianificazione di backup utilizzando queste attività per garantire che l'appliance virtuale Unified Manager sia protetta in caso di problemi.

Per ripristinare la macchina virtuale, è possibile utilizzare lo snapshot VMware creato per ripristinare la macchina virtuale allo stato point-in-time di backup.

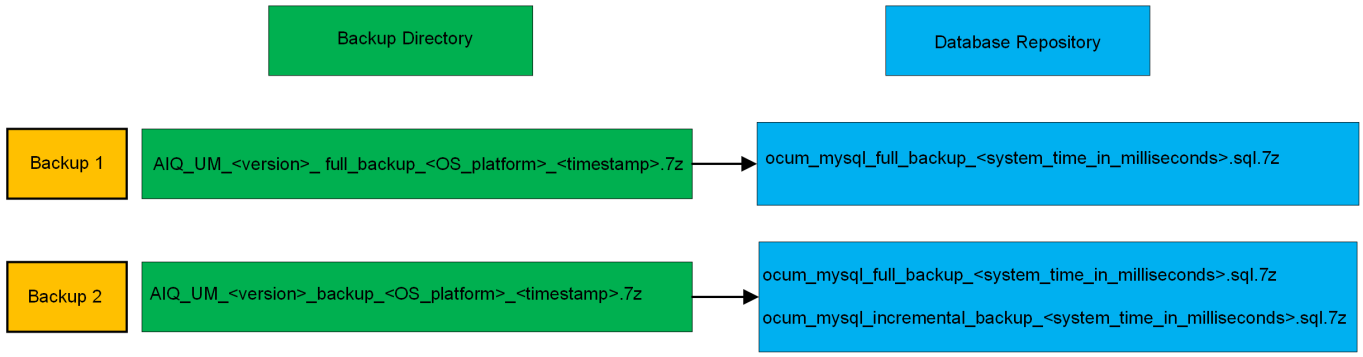
Backup e ripristino utilizzando un dump del database MySQL

Un backup dump del database MySQL è una copia del database Active IQ Unified Manager e dei file di configurazione che è possibile utilizzare in caso di guasto del sistema o perdita di dati. È possibile pianificare la scrittura di un backup in una destinazione locale o remota. Si consiglia di definire una postazione remota esterna al sistema host Active IQ Unified Manager.

Il dump del database MySQL è il meccanismo di backup predefinito quando Unified Manager viene installato su un server Linux e Windows. Tuttavia, se Unified Manager gestisce un gran numero di cluster e nodi o se il completamento dei backup MySQL dura molte ore, è possibile eseguire il backup utilizzando le copie Snapshot. Questa funzionalità è disponibile sui sistemi Red Hat Enterprise Linux, CentOS Linux e Windows.

Un backup del dump del database è costituito da un singolo file nella directory di backup e da uno o più file nella directory del repository del database. Il file nella directory di backup è molto piccolo perché contiene solo un puntatore ai file che si trovano nella directory del repository del database necessari per ricreare il backup.

La prima volta che si genera un backup del database, viene creato un singolo file nella directory di backup e viene creato un file di backup completo nella directory del repository del database. Alla successiva generazione di un backup, nella directory di backup viene creato un singolo file e nella directory del repository del database viene creato un file di backup incrementale che contiene le differenze rispetto al file di backup completo. Questo processo continua con la creazione di backup aggiuntivi, fino all'impostazione di conservazione massima, come mostrato nella figura seguente.



Non rinominare o rimuovere i file di backup in queste due directory, altrimenti le successive operazioni di ripristino non avranno esito positivo.

Se si scrivono i file di backup nel sistema locale, è necessario avviare un processo per copiare i file di backup in una posizione remota in modo che siano disponibili in caso di problemi di sistema che richiedono un ripristino completo.

Prima di iniziare un'operazione di backup, Active IQ Unified Manager esegue un controllo di integrità per verificare che tutti i file di backup e le directory di backup richiesti esistano e siano scrivibili. Inoltre, verifica che vi sia spazio sufficiente nel sistema per creare il file di backup.

Configurazione della destinazione e della pianificazione per i backup dei dump del database

È possibile configurare le impostazioni di backup del dump del database di Unified Manager per impostare il percorso di backup del database, il numero di conservazione e la pianificazione di backup. È possibile attivare backup pianificati giornalieri o settimanali. Per impostazione predefinita, i backup pianificati sono disattivati, ma è necessario impostare una pianificazione di backup.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

- È necessario disporre di almeno 150 GB di spazio disponibile nella posizione definita come percorso di backup.

  Si consiglia di utilizzare una postazione remota esterna al sistema host di Unified Manager.

- Quando Unified Manager viene installato su un sistema Linux e si utilizza il backup MySQL, assicurarsi che nella directory di backup siano impostate le seguenti autorizzazioni e proprietà.

  Permissions: 0750, Ownership: jboss:maintenance

- Quando Unified Manager viene installato su un sistema Windows e si utilizza il backup MySQL, assicurarsi che solo l'amministratore abbia accesso alla directory di backup.

La prima volta che viene eseguito un backup è necessario più tempo rispetto ai backup successivi, poiché il primo backup è un backup completo. Un backup completo può superare 1 GB e può richiedere da tre a quattro ore. I backup successivi sono incrementali e richiedono meno tempo.

- Se il numero di file di backup incrementali risulta troppo grande per lo spazio allocato per i backup, è possibile eseguire periodicamente un backup completo per sostituire il backup precedente e i relativi file incrementali. Come alternativa, è possibile eseguire un backup utilizzando le copie Snapshot.
- Il backup eseguito durante i primi 15 giorni di aggiunta di un nuovo cluster potrebbe non essere sufficientemente accurato per ottenere i dati storici delle performance.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **General** > **Database Backup**.
2. Nella pagina **Database Backup**, fare clic su **Backup Settings**.
3. Configurare i valori appropriati per un percorso di backup, un numero di conservazione e una pianificazione.

   Il valore predefinito per il conteggio di conservazione è 10; è possibile utilizzare 0 per creare backup illimitati.

4. Selezionare il pulsante **pianificato giornaliero** o **pianificato settimanale**, quindi specificare i dettagli della pianificazione.
5. Fare clic su **Apply** (Applica).

I file di backup del dump del database vengono creati in base alla pianificazione. I file di backup disponibili sono disponibili nella pagina Database Backup.

Che cos'è un ripristino del database

Un ripristino del database MySQL è il processo di ripristino di un file di backup di Unified Manager esistente sullo stesso server o su un altro server Unified Manager. L'operazione di ripristino viene eseguita dalla console di manutenzione di Unified Manager.

Se si esegue un'operazione di ripristino sullo stesso sistema (locale) e i file di backup vengono memorizzati in locale, è possibile eseguire l'opzione di ripristino utilizzando il percorso predefinito. Se si esegue un'operazione di ripristino su un sistema Unified Manager diverso (un sistema remoto), è necessario copiare il file di backup, o i file, dallo storage secondario al disco locale prima di eseguire l'opzione di ripristino.

Durante il processo di ripristino, l'utente viene disconnesso da Unified Manager. Una volta completato il

processo di ripristino, è possibile accedere al sistema.

Se si sta ripristinando l'immagine di backup su un nuovo server, al termine dell'operazione di ripristino è necessario generare un nuovo certificato di protezione HTTPS e riavviare il server Unified Manager. Sarà inoltre necessario riconfigurare le impostazioni di autenticazione SAML, se necessarie, quando si ripristina l'immagine di backup su un nuovo server.

I file di backup precedenti non possono essere utilizzati per ripristinare un'immagine dopo che Unified Manager è stato aggiornato a una versione più recente del software. Per risparmiare spazio, tutti i vecchi file di backup, ad eccezione del file più recente, vengono rimossi automaticamente quando si aggiorna Unified Manager.

Informazioni correlate

"Generazione di un certificato di protezione HTTPS"

"Attivazione dell'autenticazione SAML"

"Autenticazione con Active Directory o OpenLDAP"

Ripristino di un backup del database MySQL su un sistema Linux

In caso di perdita o danneggiamento dei dati, è possibile ripristinare Unified Manager allo stato stabile precedente con una perdita minima di dati. È possibile ripristinare il database di Unified Manager su un sistema Red Hat Enterprise Linux o CentOS locale o remoto utilizzando la console di manutenzione di Unified Manager.

Cosa ti serve

- È necessario disporre delle credenziali dell'utente root per l'host Linux su cui è installato Unified Manager.
- Per accedere alla console di manutenzione del server Unified Manager, è necessario disporre di un ID utente e di una password autorizzati.
- È necessario aver copiato il file di backup di Unified Manager e il contenuto della directory del repository del database nel sistema su cui verrà eseguita l'operazione di ripristino.

  Si consiglia di copiare il file di backup nella directory predefinita `/data/ocum`-backup. I file del repository del database devono essere copiati in `/database-dumps-repo` sotto la sottodirectory `/ocum-backup` directory.

- I file di backup devono essere di `.7z` tipo.

La funzionalità di ripristino è specifica della piattaforma e della versione. È possibile ripristinare un backup di Unified Manager solo sulla stessa versione di Unified Manager. È possibile ripristinare un file di backup Linux o un file di backup di un'appliance virtuale su un sistema Red Hat Enterprise Linux o CentOS.

Se il nome della cartella di backup contiene uno spazio, è necessario includere il percorso assoluto o relativo tra virgolette doppie.

Fasi

1. Se si esegue un ripristino su un nuovo server, dopo aver installato Unified Manager non avviare l'interfaccia utente né configurare cluster, utenti o impostazioni di autenticazione al termine dell'installazione. Il file di backup inserisce queste informazioni durante il processo di ripristino.

2. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo del sistema Unified Manager.
3. Accedere al sistema con il nome utente di manutenzione (umadmin) e la password.
4. Immettere il comando `maintenance_console` E premere Invio.
5. Nella console di manutenzione **Menu principale**, inserire il numero dell'opzione **Backup Restore**.
6. Inserire il numero per il backup * Restore MySQL.
7. Quando richiesto, immettere il percorso assoluto del file di backup.

   ```
   Bundle to restore from: /data/ocum-
   backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
   ```

   Una volta completata l'operazione di ripristino, è possibile accedere a Unified Manager.

Dopo aver ripristinato il backup, se il server OnCommand Workflow Automation non funziona, attenersi alla seguente procedura:

1. Sul server Workflow Automation, modificare l'indirizzo IP del server Unified Manager in modo che punti alla macchina più recente.
2. Nel server Unified Manager, reimpostare la password del database se l'acquisizione non riesce nel passaggio 1.

Ripristino di un backup del database MySQL su Windows

In caso di perdita o danneggiamento dei dati, è possibile utilizzare la funzione di ripristino per ripristinare Unified Manager allo stato stabile precedente con una perdita minima. È possibile ripristinare il database MySQL di Unified Manager su un sistema Windows locale o su un sistema Windows remoto utilizzando la console di manutenzione di Unified Manager.

Cosa ti serve

- È necessario disporre dei privilegi di amministratore di Windows.
- È necessario aver copiato il file di backup di Unified Manager e il contenuto della directory del repository del database nel sistema su cui verrà eseguita l'operazione di ripristino.

  Si consiglia di copiare il file di backup nella directory predefinita `\ProgramData\NetApp\OnCommandAppData\ocum\backup`. I file del repository del database devono essere copiati in `\database_dumps_repo` sotto la sottodirectory `\backup` directory.

- I file di backup devono essere di `.7z` tipo.

La funzionalità di ripristino è specifica della piattaforma e della versione. È possibile ripristinare un backup MySQL di Unified Manager solo sulla stessa versione di Unified Manager e un backup di Windows può essere ripristinato solo su una piattaforma Windows.

Se i nomi delle cartelle contengono uno spazio, è necessario includere il percorso assoluto o relativo del file di backup tra virgolette doppie.

Fasi

1. Se si esegue un ripristino su un nuovo server, dopo aver installato Unified Manager non avviare l'interfaccia utente né configurare cluster, utenti o impostazioni di autenticazione al termine dell'installazione. Il file di backup inserisce queste informazioni durante il processo di ripristino.
2. Accedere al sistema Unified Manager con le credenziali di amministratore.
3. Avviare PowerShell o il prompt dei comandi come amministratore di Windows.
4. Immettere il comando `maintenance_console` E premere Invio.
5. Nella console di manutenzione **Menu principale**, inserire il numero dell'opzione **Backup Restore**.
6. Inserire il numero per il backup * Restore MySQL.
7. Quando richiesto, immettere il percorso assoluto del file di backup.

   ```
   Bundle to restore from:
   \ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac
   kup_windows_02-20-2020-02-51.7z
   ```

   Una volta completata l'operazione di ripristino, è possibile accedere a Unified Manager.

Dopo aver ripristinato il backup, se il server OnCommand Workflow Automation non funziona, attenersi alla seguente procedura:

1. Sul server Workflow Automation, modificare l'indirizzo IP del server Unified Manager in modo che punti alla macchina più recente.
2. Nel server Unified Manager, reimpostare la password del database se l'acquisizione non riesce nel passaggio 1.

Backup e ripristino con NetApp Snapshots

Una copia Snapshot di NetApp crea un'immagine point-in-time del database e dei file di configurazione di Unified Manager che è possibile utilizzare per il ripristino in caso di guasto al sistema o perdita di dati. È necessario pianificare periodicamente la scrittura di una copia Snapshot su un volume di uno dei cluster ONTAP in modo da disporre sempre di una copia corrente.

Questa funzionalità non è disponibile per Active IQ Unified Manager installato su un'appliance virtuale.

Configurazione del backup su Linux

Se Active IQ Unified Manager è installato su una macchina Linux, puoi decidere di configurare il backup e il ripristino utilizzando NetApp Snapshots.

Le copie Snapshot richiedono pochissimo tempo, in genere solo pochi minuti, e il database di Unified Manager viene bloccato per un periodo di tempo molto breve, pertanto l'installazione non è più disgregazione. L'immagine consuma uno spazio di storage minimo e comporta un overhead delle performance trascurabile, in quanto registra solo le modifiche apportate ai file dall'ultima copia Snapshot. Poiché Snapshot viene creato su un cluster ONTAP, è possibile sfruttare altre funzionalità NetApp, come SnapMirror, per creare una protezione

secondaria, se necessario.

Prima di iniziare un'operazione di backup, Unified Manager esegue un controllo dell'integrità per verificare che il sistema di destinazione sia disponibile.

- È possibile ripristinare una copia Snapshot solo sulla stessa versione di Active IQ Unified Manager.

  Ad esempio, se è stato creato un backup su Unified Manager 9.12, il backup può essere ripristinato solo sui sistemi Unified Manager 9.12.

- In caso di modifiche nella configurazione di Snapshot, lo snapshot potrebbe non essere valido.

Configurazione della posizione della copia Snapshot

È possibile configurare il volume in cui memorizzare le copie Snapshot in uno dei cluster ONTAP utilizzando Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP.

Cosa ti serve

Il cluster, la VM di storage e il volume devono soddisfare i seguenti requisiti:

- Requisiti del cluster:
  - È necessario installare ONTAP 9.3 o versione successiva
  - Deve essere geograficamente vicino al server Unified Manager
  - Può essere monitorato da Unified Manager, ma non è necessario
- Requisiti delle macchine virtuali per lo storage:
  - Il nome e la mappatura dei nomi devono essere impostati per utilizzare "Files"
  - Utenti locali creati per corrispondere agli utenti lato client
  - Assicurarsi che sia selezionata l'opzione All Read/Write access (tutti gli accessi in lettura/scrittura
  - Assicurarsi che l'opzione accesso superutente sia impostata su "any" nel criterio di esportazione
  - NFS per NetApp Snapshot per Linux
  - NFSv4 deve essere attivato sul server NFS e sul dominio ID NFSv4 specificato sulla macchina virtuale del client e dello storage
  - Il volume deve avere una dimensione almeno doppia rispetto alla directory Unified Manager/OPT/netapp/dati

    Utilizzare il comando du -sh /opt/netapp/data/ per controllare la dimensione corrente.
- Requisiti di volume:
  - Il volume deve avere una dimensione almeno doppia rispetto alla directory di Unified Manager /opt/netapp/dati
  - Lo stile di protezione deve essere impostato su UNIX
  - Il criterio locale di snapshot deve essere disattivato
  - La funzione di dimensionamento automatico del volume deve essere attivata

- Il livello di servizio delle performance deve essere impostato su una policy con IOPS elevati e bassa latenza, ad esempio “Extreme”

Per informazioni dettagliate sulla creazione del volume NFS, vedere "Come configurare NFSv4 in ONTAP 9" e a. "Guida rapida alla configurazione NFS di ONTAP 9".

Specifica del percorso di destinazione per le copie Snapshot

È necessario configurare la posizione di destinazione per le copie Snapshot di Active IQ Unified Manager su un volume già configurato in uno dei cluster ONTAP. Per definire la posizione, utilizzare la console di manutenzione.

- È necessario disporre delle credenziali dell’utente root per l’host Linux su cui è installato Active IQ Unified Manager.
- Per accedere alla console di manutenzione del server Unified Manager, è necessario disporre di un ID utente e di una password autorizzati.
- È necessario disporre dell’indirizzo IP di Cluster Management, del nome della VM di storage, del nome del volume e del nome utente e della password del sistema di storage.
- È necessario aver montato il volume sull’host Active IQ Unified Manager e disporre del percorso di montaggio.

Fasi

1. Utilizzare Secure Shell per connettersi all’indirizzo IP o all’FQDN del sistema Active IQ Unified Manager.
2. Accedere al sistema con il nome utente di manutenzione (umadmin) e la password.
3. Immettere il comando `maintenance_console` E premere Invio.
4. Nella console di manutenzione **Menu principale**, inserire il numero dell’opzione **Backup Restore**.
5. Inserire il numero per **Configure NetApp Snapshot Backup**.
6. Inserire il numero per configurare NFS.
7. Esaminare le informazioni da fornire, quindi inserire il numero **Enter Backup Configuration Details** (Immetti dettagli configurazione backup).
8. Per identificare il volume in cui verrà scritta l’istantanea, inserire l’indirizzo IP dell’interfaccia di gestione del cluster, il nome della VM di storage, il nome del volume, il nome del LUN, il nome utente e la password del sistema di storage e il percorso di montaggio.
9. Verificare queste informazioni e immettere `y`.

   Il sistema esegue le seguenti operazioni:

   - Stabilisce la connessione al cluster
   - Interrompe tutti i servizi
   - Crea una nuova directory nel volume e copia i file di configurazione del database Active IQ Unified Manager
   - Elimina i file da Active IQ Unified Manager e crea un collegamento simbolico alla nuova directory del database
   - Riavvia tutti i servizi
10. Uscire dalla console di manutenzione e avviare l’interfaccia di Active IQ Unified Manager per creare una pianificazione per la copia Snapshot, se non è già stata eseguita questa operazione.

Configurazione del backup su Windows

Active IQ Unified Manager supporta il backup e il ripristino utilizzando le istantanee NetApp sul sistema operativo Windows con l'aiuto del LUN che utilizza il protocollo iSCSI.

È possibile eseguire il backup basato su Snapshot mentre tutti i servizi di Unified Manager sono in esecuzione. Lo stato coerente del database viene acquisito come parte di Snapshot, poiché il backup inserisce un blocco di lettura globale nell'intero database che impedisce qualsiasi scrittura simultanea. Affinché il sistema Unified Manager installato sul sistema operativo Windows esegua il backup e il ripristino utilizzando NetApp Snapshots, è necessario configurare il backup di Unified Manager su Snapshot in base alla console di manutenzione.

Prima di configurare Unified Manager per la creazione di copie Snapshot, è necessario eseguire le seguenti attività di configurazione.

- Configurare il cluster ONTAP
- Configurare il computer host di Windows

Configurazione della posizione di backup per Windows

È necessario configurare il volume per la memorizzazione delle copie Snapshot dopo il backup di Unified Manager su Windows.

Cosa ti serve

Il cluster, la VM di storage e il volume devono soddisfare i seguenti requisiti:

- Requisiti del cluster:
  - È necessario installare ONTAP 9.3 o versione successiva
  - Deve essere geograficamente vicino al server Unified Manager
  - Viene monitorato da Unified Manager
- Requisiti delle macchine virtuali per lo storage:
  - Connettività iSCSI sul cluster ONTAP
  - Il protocollo iSCSI deve essere attivato per la macchina configurata
  - Per la configurazione del backup, è necessario disporre di un volume e di un LUN dedicati. Il volume selezionato deve contenere un solo LUN e nient'altro.
  - La dimensione del LUN deve essere almeno il doppio della dimensione dei dati prevista per la gestione in 9.9 Active IQ Unified Manager.

    In questo modo vengono impostati anche gli stessi requisiti di dimensione sul volume.

  - Assicurarsi che sia selezionata l'opzione All Read/Write access (tutti gli accessi in lettura/scrittura
  - Assicurarsi che l'opzione accesso superutente sia impostata su "any" nel criterio di esportazione
- Requisiti di volume e LUN:
  - Il volume deve avere una dimensione almeno doppia rispetto alla directory dei dati MySQL di Unified Manager.
  - Lo stile di protezione deve essere impostato su Windows
  - Il criterio locale di snapshot deve essere disattivato

- La funzione di dimensionamento automatico del volume deve essere attivata
- Il livello di servizio delle performance deve essere impostato su una policy con IOPS elevati e bassa latenza, ad esempio “Extreme”

Configurazione del cluster ONTAP

Prima di eseguire il backup e il ripristino di Active IQ Unified Manager utilizzando la copia Snapshot sui sistemi ONTAP, è necessario eseguire alcune operazioni di preconfigurazione sui cluster.

È possibile configurare il cluster ONTAP utilizzando il prompt dei comandi o l’interfaccia utente di Gestore di sistema. La configurazione del cluster ONTAP prevede la configurazione dei file di dati di base disponibili per l’assegnazione come file di base iSCSI alla VM di storage. Il passaggio successivo consiste nel configurare una VM di storage abilitata iSCSI utilizzando l’interfaccia utente di System Manager. Sarà necessario configurare un percorso di rete statico per questa VM di storage per controllare il modo in cui i file LIF utilizzano la rete per il traffico in uscita.

Per la configurazione del backup, è necessario disporre di un volume dedicato e di un LUN. Il volume selezionato deve includere un solo LUN. La dimensione del LUN deve essere almeno il doppio della dimensione dei dati prevista per la gestione da parte di Active IQ Unified Manager.

È necessario eseguire la seguente configurazione:

Fasi

1. Configurare una VM di storage abilitata iSCSI o utilizzare una VM di storage esistente con la stessa configurazione.
2. Configurare un percorso di rete per la VM di storage configurata.
3. Configurare un volume di capacità appropriata e un singolo LUN all’interno, assicurandosi che il volume sia dedicato solo per questo LUN.

   In uno scenario in cui il LUN viene creato in System Manager, la rimozione della mappatura del LUN potrebbe eliminare il igroup e il ripristino potrebbe non riuscire. Per evitare questo scenario, assicurarsi che durante la creazione di un LUN venga creato in modo esplicito e non venga cancellato quando il LUN viene dismappato.

4. Configurare un gruppo di iniziatori nella VM di storage.
5. Configurare un set di porte.
6. Integrare l’igroup con il portset.
7. Mappare il LUN sull’igroup.

Configurazione del computer host di Windows

È necessario configurare il computer host Windows prima di poter utilizzare NetApp Snapshot per eseguire il backup e il ripristino di Active IQ Unified Manager. Per avviare Microsoft iSCSI Initiator su un computer host Windows, digitare “iscsi” nella barra di ricerca e fare clic su **iSCSI Initiator**.

Cosa ti serve

È necessario ripulire le configurazioni precedenti sul computer host.

Se si sta tentando di avviare iSCSI Initiator in una nuova installazione di Windows, viene richiesta una conferma e, al momento della conferma, viene visualizzata la finestra di dialogo iSCSI Properties (Proprietà iSCSI). Se si tratta di un'installazione Windows esistente, viene visualizzata la finestra di dialogo delle proprietà iSCSI con una destinazione inattiva o che tenta di connettersi. Pertanto, è necessario assicurarsi che tutte le configurazioni precedenti sull'host Windows siano state rimosse.

Fasi

1. Ripulire le configurazioni precedenti sul computer host.
2. Scopri il portale di destinazione.
3. Connettersi al portale di destinazione.
4. Connettersi utilizzando multipath al portale di destinazione.
5. Scopri entrambi i LIF.
6. Individuare il LUN configurato nel computer Windows come dispositivo.
7. Configurare il LUN rilevato come nuovo disco di volume in Windows.

Specifica del percorso di destinazione per le copie Snapshot in Windows

È necessario configurare la posizione di destinazione per le copie Snapshot di Active IQ Unified Manager su un volume già configurato in uno dei cluster ONTAP. Per definire la posizione, utilizzare la console di manutenzione.

- È necessario disporre del privilegio di amministratore per l'host Windows su cui è installato Active IQ Unified Manager.
- Per accedere alla console di manutenzione del server Unified Manager, è necessario disporre di un ID utente e di una password autorizzati.
- È necessario disporre dell'indirizzo IP di Cluster Management, del nome della VM di storage, del nome del volume, del nome del LUN, del nome utente e della password del sistema di storage.
- È necessario aver montato il volume come unità di rete sull'host Active IQ Unified Manager e disporre dell'unità di montaggio.

Fasi

1. Utilizzando Power Shell, connettersi all'indirizzo IP o al nome di dominio completo del sistema Active IQ Unified Manager.
2. Accedere al sistema con il nome utente di manutenzione (umadmin) e la password.
3. Immettere il comando `maintenance_console` E premere Invio.
4. Nella console di manutenzione **Menu principale**, inserire il numero dell'opzione **Backup Restore**.
5. Inserire il numero per **Configure NetApp Snapshot Backup**.
6. Inserire il numero per configurare iSCSI.
7. Esaminare le informazioni da fornire, quindi inserire il numero **Enter Backup Configuration Details** (Immetti dettagli configurazione backup).
8. Per identificare il volume in cui verrà scritta l'istantanea, inserire l'indirizzo IP dell'interfaccia di gestione del cluster, il nome della VM di storage, il nome del volume, il nome del LUN, il nome utente e la password del sistema di storage e l'unità di montaggio.

9. Verificare queste informazioni e immettere `y`.

   Il sistema esegue le seguenti operazioni:

   - Storage VM validato
   - Il volume viene validato
   - Montare il disco e verificare che lo stato sia validato
   - Esistenza e stato del LUN
   - Esistenza di un disco di rete
   - Viene convalidata l'esistenza di spazio consigliato (più del doppio della directory di dati mysql) nel volume montato
   - Percorso LUN corrispondente al LUN dedicato nel volume
   - nome igroup
   - GUID del volume su cui è montato il disco di rete
   - ISCSI Initiator utilizzato per comunicare con ONTAP

10. Uscire dalla console di manutenzione e avviare l'interfaccia Active IQ Unified Manager per creare una pianificazione per le copie Snapshot.

Configurazione del backup mediante copia Snapshot dalla console di manutenzione

Per eseguire il backup di Active IQ Unified Manager utilizzando la copia Snapshot, è necessario eseguire alcuni passaggi di configurazione dalla console di manutenzione.

Cosa ti serve

Per il sistema in uso, è necessario disporre dei seguenti dettagli:

- Indirizzo IP del cluster
- Nome della VM di storage
- Nome del volume
- Nome del LUN
- Percorso di montaggio
- Credenziali del sistema storage

Fasi

1. Accedere alla console di manutenzione di Unified Manager.
2. Immettere 4 per selezionare **Backup Restore**.
3. Inserire 2 per selezionare **Backup e ripristino utilizzando NetApp Snapshot**.

   Se si desidera modificare la configurazione di backup, immettere 3 per selezionare **Update NetApp Snapshot Backup Configuration**. È possibile solo aggiornare la password.

4. Dal menu, immettere 1 per selezionare **Configure NetApp Snapshot Backup**.
5. Inserire 1 per fornire le informazioni richieste.

6. Fornire il nome utente e la password per la console di manutenzione, quindi fornire la conferma che il LUN è montato sull'host.

   Il processo verifica quindi che la directory dei dati, il percorso del LUN, la VM dello storage, i volumi, la disponibilità dello spazio, il disco e così via forniti dall'utente sono corretti. Le operazioni che procedono in background sono:

   - I servizi vengono arrestati
   - La directory del database viene spostata sullo storage montato
   - La directory del database viene eliminata e vengono stabiliti i symlink
   - I servizi vengono riavviati dopo il completamento della configurazione nell'interfaccia Active IQ Unified Manager, il tipo di backup viene modificato in NetApp Snapshot e si riflette nell'interfaccia utente come backup del database (basato su Snapshot).

Prima di iniziare un'operazione di backup, è necessario verificare se sono state apportate modifiche alla configurazione di Snapshot, in quanto potrebbero causare l'invalidità dello snapshot. Supponiamo di aver configurato il backup in G Drive e Snapshot taken. In seguito, è stato riconfigurato il backup sul disco e e i dati vengono salvati sul disco e in base alla nuova configurazione. Se si tenta di ripristinare l'istantanea acquisita mentre si trovava nel disco G, si verifica un errore con l'errore che il disco G non esiste.

Definizione di una pianificazione di backup per Linux e Windows

È possibile configurare la pianificazione con cui vengono create le copie Snapshot di Unified Manager utilizzando l'interfaccia utente di Unified Manager.

Cosa ti serve

- È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
- È necessario aver configurato le impostazioni per la creazione di copie Snapshot dalla console di manutenzione per identificare la destinazione in cui verranno create le snapshot.

Le copie Snapshot vengono create in pochi minuti e il database di Unified Manager viene bloccato solo per pochi secondi.

> Il backup eseguito durante i primi 15 giorni di aggiunta di un nuovo cluster potrebbe non essere sufficientemente accurato per ottenere i dati storici delle performance.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **General** > **Database Backup**.
2. Nella pagina **Database Backup**, fare clic su **Backup Settings**.
3. Inserire il numero massimo di copie Snapshot che si desidera conservare nel campo **Conteggio conservazione**.

   Il valore predefinito per Conteggio conservazione è 10. Il numero massimo di copie Snapshot è determinato dalla versione del software ONTAP sul cluster. È possibile lasciare vuoto questo campo per implementare il valore massimo indipendentemente dalla versione di ONTAP.

4. Selezionare il pulsante **pianificato giornaliero** o **pianificato settimanale**, quindi specificare i dettagli della pianificazione.

5. Fare clic su **Apply** (Applica).

Le copie Snapshot vengono create in base alla pianificazione. I file di backup disponibili sono disponibili nella pagina Database Backup.

A causa dell'importanza di questo volume e degli snapshot, è possibile creare uno o due avvisi per questo volume in modo da ricevere una notifica quando:

- Lo spazio del volume è pieno al 90%. Utilizzare l'evento **Volume Space Full** per impostare l'avviso.

  È possibile aggiungere capacità al volume utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP in modo che il database di Unified Manager non esaurisca lo spazio disponibile.

- Il numero di snapshot è prossimo al raggiungimento del numero massimo. Utilizzare l'evento **troppe copie Snapshot** per impostare l'avviso.

  È possibile eliminare le snapshot meno recenti utilizzando Gestione di sistema di ONTAP o l'interfaccia utente di ONTAP, in modo da avere sempre spazio per le nuove copie Snapshot.

Gli avvisi vengono configurati nella pagina Configurazione avvisi.

Ripristino di Unified Manager utilizzando le copie Snapshot

In caso di perdita o danneggiamento dei dati, è possibile ripristinare Unified Manager allo stato stabile precedente con una perdita minima di dati. È possibile ripristinare il database Snapshot di Unified Manager su un sistema operativo locale o remoto utilizzando la console di manutenzione di Unified Manager.

Cosa ti serve

- È necessario disporre delle credenziali dell'utente root per l'host Linux e dei privilegi amministrativi per il computer host Windows su cui è installato Unified Manager.
- Per accedere alla console di manutenzione del server Unified Manager, è necessario disporre di un ID utente e di una password autorizzati.

La funzionalità di ripristino è specifica della piattaforma e della versione. È possibile ripristinare un backup di Unified Manager solo sulla stessa versione di Unified Manager.

Fasi

1. Connettersi all'indirizzo IP o al nome di dominio completo del sistema Unified Manager.
   - Linux: Shell sicura
   - Windows: Power Shell
2. Accedere al sistema con le credenziali dell'utente root.
3. Immettere il comando `maintenance_console` E premere Invio.
4. Nella console di manutenzione **Menu principale**, inserire 4 per l'opzione **Backup Restore**.
5. Inserire 2 per selezionare **Backup e ripristino utilizzando NetApp Snapshot**.

   Se si esegue un ripristino su un nuovo server, dopo aver installato Unified Manager non avviare l'interfaccia utente né configurare cluster, utenti o impostazioni di autenticazione al termine dell'installazione. Inserire 1 per selezionare **Configure NetApp Snapshot Backup** e configurare le

impostazioni per le copie Snapshot così come si trovano sul sistema originale.

6. Inserire 3 per selezionare **Restore using NetApp Snapshot** (Ripristina con NetApp Snapshot*).
7. Selezionare la copia Snapshot da cui si desidera ripristinare Unified Manager. Premere **Invio**.
8. Una volta completato il processo di ripristino, accedere all'interfaccia utente di Unified Manager.

Dopo aver ripristinato il backup, se il server Workflow Automation non funziona, attenersi alla seguente procedura:

1. Sul server Workflow Automation, modificare l'indirizzo IP del server Unified Manager in modo che punti alla macchina più recente.
2. Nel server Unified Manager, reimpostare la password del database se l'acquisizione non riesce nel passaggio 1.

Modifica del tipo di backup

Se si desidera modificare il tipo di backup per il sistema Active IQ Unified Manager, è possibile utilizzare le opzioni della console di manutenzione. L'opzione **Unconfigure NetApp Snapshot Backup** consente di tornare al backup basato su MySQL.

Cosa ti serve

Per accedere alla console di manutenzione del server Unified Manager, è necessario disporre di un ID utente e di una password autorizzati.

Fasi

1. Accedere alla console di manutenzione.
2. Selezionare 4 dal menu principale per il backup e il ripristino.
3. Selezionare 2 dal menu **Backup and Restore (Backup e ripristino)**.
4. Selezionare 4 per **Unconfigure NetApp Snapshot Backup**.

   Vengono visualizzate le azioni eseguite, ovvero arrestare i servizi, interrompere il collegamento simbolico, spostare i dati dallo storage alla directory, quindi riavviare i servizi.

   Una volta modificato il metodo di backup, il meccanismo di backup viene modificato da Snapshot copy a MySQL backup predefinito. Questa modifica viene visualizzata nella sezione Database Backup (Backup database) delle impostazioni generali.

Backup on-demand per Unified Manager

È possibile utilizzare l'interfaccia utente di Active IQ Unified Manager per generare backup on-demand quando necessario. Il backup on-demand consente di creare istantaneamente un backup utilizzando il metodo di backup esistente. Il backup on-demand non differenzia tra il backup basato su MySQL o NetApp Snapshot.

È possibile eseguire il backup on-demand utilizzando il pulsante **Backup Now** nella pagina Database Backup. Il backup on-demand non dipende dalle pianificazioni configurate per Active IQ Unified Manager.

Migrazione di un'appliance virtuale Unified Manager a un sistema Linux

Se si desidera modificare il sistema operativo host su cui è in esecuzione Unified Manager, è possibile ripristinare un backup del dump del database MySQL di Unified Manager da un'appliance virtuale a un sistema Red Hat Enterprise Linux o CentOS Linux.

Cosa ti serve

- Sull'appliance virtuale:
  - È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.
  - È necessario conoscere il nome dell'utente di manutenzione di Unified Manager per l'operazione di ripristino.
- Sul sistema Linux:
  - Unified Manager deve essere installato su un server Linux seguendo le istruzioni riportate in "Installazione di Unified Manager su sistemi Linux".
  - La versione di Unified Manager su questo server deve essere uguale a quella dell'appliance virtuale da cui si utilizza il file di backup.
  - Non avviare l'interfaccia utente né configurare cluster, utenti o impostazioni di autenticazione sul sistema Linux dopo l'installazione. Il file di backup inserisce queste informazioni durante il processo di ripristino.
  - È necessario disporre delle credenziali dell'utente root per l'host Linux.

Questi passaggi descrivono come creare un file di backup sull'appliance virtuale, copiare i file di backup nel sistema Red Hat Enterprise Linux o CentOS e ripristinare il backup del database nel nuovo sistema.

Fasi

1. Sull'appliance virtuale, fare clic su **Management** > **Database Backup**.
2. Nella pagina **Database Backup**, fare clic su **Backup Settings**.
3. Modificare il percorso di backup in /jail/support.
4. Nella sezione Schedule (programma), selezionare **Scheduled Daily** (giornaliero pianificato) e inserire un intervallo di tempo che deve trascorrere alcuni minuti prima dell'ora corrente, in modo che il backup venga creato a breve.
5. Fare clic su **Apply** (Applica).
6. Attendere alcune ore per la creazione del backup.

   Un backup completo può superare 1 GB e può richiedere da tre a quattro ore per il completamento.

7. Accedere come utente root all'host Linux su cui è installato Unified Manager e copiare i file di backup da /support sull'appliance virtuale utilizzando SCP.`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

   ```
   root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
   ```

   Assicurarsi di aver copiato il file di backup .7z e tutti i file repository .7z nella sottodirectory /database-dump-repo.

8. Al prompt dei comandi, ripristinare il backup: `um backup restore -f /<backup_file_path>/<backup_file_name>`

   ```
   um backup restore -f /UM_9.7.N151113.1348_backup_unix_02-12-2019-04-16.7z
   ```

9. Al termine dell'operazione di ripristino, accedere all'interfaccia utente Web di Unified Manager.

È necessario eseguire le seguenti operazioni:

- Generare un nuovo certificato di sicurezza HTTPS e riavviare il server Unified Manager.
- Modificare il percorso di backup sull'impostazione predefinita per il sistema Linux (/data/ocum-backup) o su un nuovo percorso di propria scelta, perché non esiste un percorso /jail/support sul sistema Linux.
- Riconfigurare entrambi i lati della connessione di Workflow Automation, se si utilizza WFA.
- Riconfigurare le impostazioni di autenticazione SAML, se si utilizza SAML.

Dopo aver verificato che tutto funziona come previsto sul sistema Linux, è possibile arrestare e rimuovere l'appliance virtuale Unified Manager.

Gestione degli script

È possibile utilizzare gli script per modificare o aggiornare automaticamente più oggetti di storage in Unified Manager. Lo script è associato a un avviso. Quando un evento attiva un avviso, lo script viene eseguito. È possibile caricare script personalizzati e testarne l'esecuzione quando viene generato un avviso.

Per impostazione predefinita, è attivata la possibilità di caricare gli script in Unified Manager ed eseguirli. Se l'organizzazione non desidera consentire questa funzionalità per motivi di sicurezza, è possibile disattivarla da **Storage Management** > **Feature Settings**.

Come funzionano gli script con gli avvisi

È possibile associare un avviso allo script in modo che venga eseguito quando viene generato un avviso per un evento in Unified Manager. È possibile utilizzare gli script per risolvere i problemi relativi agli oggetti di storage o identificare gli oggetti di storage che generano gli eventi.

Quando viene generato un avviso per un evento in Unified Manager, viene inviata un'email di avviso ai destinatari specificati. Se è stato associato un avviso a uno script, lo script viene eseguito. È possibile ottenere i dettagli degli argomenti passati allo script dall'e-mail di avviso.

> Se è stato creato uno script personalizzato e lo si è associato a un avviso per un tipo di evento specifico, le azioni vengono eseguite in base allo script personalizzato per quel tipo di evento e le azioni **Fix it** non sono disponibili per impostazione predefinita nella pagina delle azioni di gestione o nella dashboard di Unified Manager.

Lo script utilizza i seguenti argomenti per l'esecuzione:

- `-eventID`
- `-eventName`

- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

È possibile utilizzare gli argomenti negli script e raccogliere informazioni relative agli eventi o modificare gli oggetti di storage.

Esempio per ottenere argomenti dagli script

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

Quando viene generato un avviso, questo script viene eseguito e viene visualizzato il seguente output:

```
-eventID : 290
-eventSourceID : 4138
```

Aggiunta di script

È possibile aggiungere script in Unified Manager e associarli agli avvisi. Questi script vengono eseguiti automaticamente quando viene generato un avviso e consentono di ottenere informazioni sugli oggetti di storage per i quali viene generato l'evento.

Cosa ti serve

- È necessario aver creato e salvato gli script che si desidera aggiungere al server Unified Manager.
- I formati di file supportati per gli script sono Perl, Shell, PowerShell, Python e. `.bat` file.

Piattaforma su cui è installato Unified Manager	Lingue supportate
VMware	Script Perl e Shell
Linux	Script Perl, Python e Shell
Windows	Script PowerShell, Perl, Python e .bat

  - Per gli script Perl, Perl deve essere installato sul server Unified Manager. Per le installazioni VMware, Perl 5 viene installato per impostazione predefinita e gli script supportano solo ciò che Perl 5 supporta. Se Perl è stato installato dopo Unified Manager, è necessario riavviare il server Unified Manager.
  - Per gli script PowerShell, è necessario impostare il criterio di esecuzione PowerShell appropriato sul server Windows in modo che gli script possano essere eseguiti.

Se lo script crea file di log per tenere traccia dell'avanzamento dello script di avviso, è necessario assicurarsi che i file di log non vengano creati in alcun punto della cartella di installazione di Unified Manager.

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile caricare script personalizzati e raccogliere i dettagli dell'evento relativi all'avviso.

Se questa funzionalità non viene visualizzata nell'interfaccia utente, è perché è stata disattivata dall'amministratore. Se necessario, è possibile attivare questa funzionalità da **Storage Management** > **Feature Settings**.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage Management** > **Scripts**.
2. Nella pagina **script**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi script**, fare clic su **Sfoglia** per selezionare il file script.
4. Inserire una descrizione per lo script selezionato.
5. Fare clic su **Aggiungi**.

Eliminazione degli script

È possibile eliminare uno script da Unified Manager quando lo script non è più necessario o valido.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- Lo script non deve essere associato a un avviso.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage Management** > **Scripts**.
2. Nella pagina **script**, selezionare lo script che si desidera eliminare, quindi fare clic su **Elimina**.
3. Nella finestra di dialogo **Avviso**, confermare l'eliminazione facendo clic su **Sì**.

Esecuzione di test dello script

È possibile verificare che lo script venga eseguito correttamente quando viene generato un avviso per un oggetto di storage.

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver caricato uno script nel formato di file supportato in Unified Manager.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage Management** > **Scripts**.
2. Nella pagina script, aggiungere lo script di test.
3. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
4. Nella pagina **Alert Setup**, eseguire una delle seguenti operazioni:

Per…	Eseguire questa operazione…
Aggiungere un avviso	a. Fare clic su **Aggiungi**. b. Nella sezione Actions (azioni), associare l'avviso allo script di test.
Modificare un avviso	a. Selezionare un avviso, quindi fare clic su **Modifica**. b. Nella sezione Actions (azioni), associare l'avviso allo script di test.

5. Fare clic su **Save** (Salva).
6. Nella pagina **Alert Setup**, selezionare l'avviso aggiunto o modificato, quindi fare clic su **Test**.

   Lo script viene eseguito con l'argomento "-test" e viene inviato un avviso di notifica agli indirizzi e-mail specificati al momento della creazione dell'avviso.

Gestione e monitoraggio dei gruppi

È possibile creare gruppi in Unified Manager per gestire gli oggetti di storage.

Comprensione dei gruppi

È possibile creare gruppi in Unified Manager per gestire gli oggetti di storage. La comprensione dei concetti relativi ai gruppi e del modo in cui le regole di gruppo consentono di aggiungere oggetti di storage a un gruppo consente di gestire gli oggetti di storage nel proprio ambiente.

Che cos'è un gruppo

Un gruppo è una raccolta dinamica di oggetti storage eterogenei (cluster, SVM o volumi). È possibile creare gruppi in Unified Manager per gestire facilmente un set di oggetti di storage. I membri di un gruppo potrebbero cambiare, a seconda degli oggetti di storage monitorati da Unified Manager in un momento specifico.

- Ogni gruppo ha un nome univoco.
- È necessario configurare un minimo di una regola di gruppo per ciascun gruppo.
- È possibile associare un gruppo a più regole di gruppo.
- Ciascun gruppo può includere diversi tipi di oggetti storage, ad esempio cluster, SVM o volumi.
- Gli oggetti di storage vengono aggiunti dinamicamente a un gruppo in base al momento in cui viene creata una regola di gruppo o quando Unified Manager completa un ciclo di monitoraggio.
- È possibile applicare contemporaneamente azioni a tutti gli oggetti di storage di un gruppo, ad esempio l'impostazione di soglie per i volumi.

Funzionamento delle regole di gruppo per i gruppi

Una regola di gruppo è un criterio definito per consentire l'inclusione di oggetti storage (volumi, cluster o SVM) in un gruppo specifico. È possibile utilizzare i gruppi di condizioni o le condizioni per definire una regola di gruppo per un gruppo.

- È necessario associare una regola di gruppo a un gruppo.
- È necessario associare un tipo di oggetto per una regola di gruppo; per una regola di gruppo è associato un solo tipo di oggetto.
- Gli oggetti di storage vengono aggiunti o rimossi dal gruppo dopo ogni ciclo di monitoraggio o quando una regola viene creata, modificata o eliminata.
- Una regola di gruppo può avere uno o più gruppi di condizioni e ciascun gruppo di condizioni può avere una o più condizioni.
- Gli oggetti di storage possono appartenere a più gruppi in base alle regole di gruppo create dall'utente.

Condizioni

È possibile creare più gruppi di condizioni e ciascun gruppo di condizioni può avere una o più condizioni. È possibile applicare tutti i gruppi di condizioni definiti in una regola di gruppo per i gruppi al fine di specificare quali oggetti di storage sono inclusi nel gruppo.

Le condizioni all'interno di un gruppo di condizioni vengono eseguite utilizzando AND logico. Tutte le condizioni di un gruppo di condizioni devono essere soddisfatte. Quando si crea o si modifica una regola di gruppo, viene creata una condizione che applica, seleziona e raggruppa solo gli oggetti di storage che soddisfano tutte le condizioni del gruppo Condition. È possibile utilizzare più condizioni all'interno di un gruppo di condizioni quando si desidera limitare l'ambito degli oggetti di storage da includere in un gruppo.

È possibile creare condizioni con oggetti di storage utilizzando i seguenti operandi e operatore e specificando il valore richiesto.

Tipo di oggetto storage	Operandi applicabili
Volume	• Nome dell'oggetto • Nome del cluster proprietario • Nome SVM proprietario • Annotazioni
SVM	• Nome dell'oggetto • Nome del cluster proprietario • Annotazioni
Cluster	• Nome dell'oggetto • Annotazioni

Quando si seleziona un'annotazione come operando per qualsiasi oggetto di storage, è disponibile l'operatore "is". Per tutti gli altri operandi, è possibile selezionare "is" o "contains" come operatore.

- Operando

L’elenco degli operandi in Unified Manager cambia in base al tipo di oggetto selezionato. L’elenco include il nome dell’oggetto, il nome del cluster proprietario, il nome SVM proprietario e le annotazioni definite in Unified Manager.

- Operatore

  L’elenco degli operatori cambia in base all’operando selezionato per una condizione. Gli operatori supportati in Unified Manager sono “is” e “contains”.

  Quando si seleziona l’operatore “is”, la condizione viene valutata per la corrispondenza esatta del valore dell’operando con il valore fornito per l’operando selezionato.

  Quando si seleziona l’operatore “contains”, la condizione viene valutata per soddisfare uno dei seguenti criteri:

  - Il valore dell’operando corrisponde esattamente al valore fornito per l’operando selezionato
  - Il valore dell’operando contiene il valore fornito per l’operando selezionato

- Valore

  Il campo valore cambia in base all’operando selezionato.

Esempio di una regola di gruppo con condizioni

Considerare un gruppo di condizioni per un volume con le seguenti due condizioni:

- Il nome contiene “vol”
- Il nome SVM è “dATA_svm”

Questo gruppo di condizioni seleziona tutti i volumi che includono “vol” nei loro nomi e che sono ospitati su SVM con il nome “data_svm”.

Gruppi di condizioni

I gruppi di condizioni vengono eseguiti utilizzando OR logico e quindi applicati agli oggetti di storage. Gli oggetti di storage devono soddisfare uno dei gruppi di condizioni da includere in un gruppo. Gli oggetti di storage di tutti i gruppi di condizioni vengono combinati. È possibile utilizzare i gruppi di condizioni per aumentare l’ambito degli oggetti di storage da includere in un gruppo.

Esempio di una regola di gruppo con gruppi di condizioni

Prendere in considerazione due gruppi di condizioni per un volume, ciascuno dei quali contiene le seguenti due condizioni:

- Gruppo di condizioni 1
  - Il nome contiene “vol”
  - Il nome SVM è “dATA_svm”. Il gruppo di condizioni 1 seleziona tutti i volumi che includono “vol” nei loro nomi e che sono ospitati sulle SVM con il nome “dATA_svm”.
- Gruppo di condizioni 2
  - Il nome contiene “vol”
  - Il valore di annotazione della priorità dei dati è “critico”. Il gruppo di condizioni 2 seleziona tutti i volumi che includono “vol” nei loro nomi e che sono annotati con il valore di annotazione della priorità dei dati

come “critico”.

Quando una regola di gruppo contenente questi due gruppi di condizioni viene applicata agli oggetti di storage, i seguenti oggetti di storage vengono aggiunti a un gruppo selezionato:

- Tutti i volumi che includono “vol” nei loro nomi e che sono ospitati sulla SVM con il nome “data_svm”.
- Tutti i volumi che includono “vol” nei loro nomi e che sono annotati con il valore di annotazione della priorità dei dati “critical”.

Come funzionano le azioni di gruppo sugli oggetti storage

Un’azione di gruppo è un’operazione eseguita su tutti gli oggetti di storage di un gruppo. Ad esempio, è possibile configurare un’azione di gruppo di soglie del volume per modificare contemporaneamente i valori di soglia di tutti i volumi di un gruppo.

I gruppi supportano tipi di azione di gruppo univoci. È possibile disporre di un gruppo con un solo tipo di azione di gruppo per la soglia di integrità del volume. Tuttavia, è possibile configurare un diverso tipo di azione di gruppo, se disponibile, per lo stesso gruppo. Il rango di un’azione di gruppo determina l’ordine in cui l’azione viene applicata agli oggetti di storage. La pagina dei dettagli di un oggetto di storage fornisce informazioni sull’azione di gruppo applicata all’oggetto di storage.

Esempio di azioni di gruppo univoche

Si consideri un volume A che appartiene ai gruppi G1 e G2 e le seguenti azioni di gruppo relative alla soglia di integrità del volume sono configurate per questi gruppi:

- `Change_capacity_threshold` azione di gruppo con rango 1, per configurare la capacità del volume
- `Change_snapshot_copies` Azione di gruppo con rango 2, per la configurazione delle copie Snapshot del volume

Il `Change_capacity_threshold` l’azione di gruppo ha sempre la priorità su `Change_snapshot_copies` Azione di gruppo e viene applicata al volume A. Quando Unified Manager completa un ciclo di monitoraggio, gli eventi relativi alla soglia di integrità del volume A vengono rivalutati per `Change_capacity_threshold` azione di gruppo. Non è possibile configurare un altro tipo di azione di gruppo per la soglia del volume per il gruppo G1 o G2.

Aggiunta di gruppi

È possibile creare gruppi per combinare cluster, volumi e macchine virtuali di storage (SVM) per semplificare la gestione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell’applicazione o di amministratore dello storage.

È possibile definire regole di gruppo per aggiungere o rimuovere membri dal gruppo e per modificare le azioni di gruppo per il gruppo.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **gruppi**, fare clic su **Aggiungi**.

3. Nella finestra di dialogo **Aggiungi gruppo**, immettere un nome e una descrizione per il gruppo.
4. Fare clic su **Aggiungi**.

Modifica di gruppi

È possibile modificare il nome e la descrizione di un gruppo creato in Unified Manager.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Quando si modifica un gruppo per aggiornare il nome, è necessario specificare un nome univoco; non è possibile utilizzare un nome di gruppo esistente.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **gruppi**, selezionare il gruppo che si desidera modificare, quindi fare clic su **Modifica**.
3. Nella finestra di dialogo **Modifica gruppo**, modificare il nome, la descrizione o entrambi per il gruppo.
4. Fare clic su **Save** (Salva).

Eliminazione di gruppi

È possibile eliminare un gruppo da Unified Manager quando il gruppo non è più necessario.

Cosa ti serve

- Nessuno degli oggetti storage (cluster, SVM o volumi) deve essere associato a qualsiasi regola di gruppo associata al gruppo che si desidera eliminare.
- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **gruppi**, selezionare il gruppo che si desidera eliminare, quindi fare clic su **Elimina**.
3. Nella finestra di dialogo **Avviso**, confermare l'eliminazione facendo clic su **Sì**.

   L'eliminazione di un gruppo non elimina le azioni di gruppo associate al gruppo. Tuttavia, queste azioni di gruppo non verranno mappate dopo l'eliminazione del gruppo.

Aggiunta di regole di gruppo

È possibile creare regole di gruppo per un gruppo per aggiungere dinamicamente oggetti di storage come volumi, cluster o macchine virtuali di storage (SVM) al gruppo. Per creare una regola di gruppo, è necessario configurare almeno un gruppo di condizioni con almeno una condizione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Gli oggetti di storage attualmente monitorati vengono aggiunti non appena viene creata la regola di gruppo. I nuovi oggetti vengono aggiunti solo dopo il completamento del ciclo di monitoraggio.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **regole di gruppo**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi regola di gruppo**, specificare un nome per la regola di gruppo.
4. Nel campo **Target Object Type**, selezionare il tipo di oggetto di storage che si desidera raggruppare.
5. Nel campo **Gruppo**, selezionare il gruppo richiesto per il quale si desidera creare le regole di gruppo.
6. Nella sezione **Condizioni**, eseguire i seguenti passaggi per creare una condizione, un gruppo di condizioni o entrambi:

Per creare	Eseguire questa operazione…
Una condizione	a. Selezionare un operando dall'elenco. b. Selezionare **contains** o **is** come operatore. c. Inserire un valore o selezionarlo dall'elenco Available (disponibili).
Un gruppo di condizioni	a. Fare clic su **Aggiungi gruppo di condizioni** b. Selezionare un operando dall'elenco. c. Selezionare **contains** o **is** come operatore. d. Inserire un valore o selezionarlo dall'elenco Available (disponibili). e. Fare clic su **Add Condition** (Aggiungi condizione) per creare ulteriori condizioni, se necessario, e ripetere i passaggi da a a d per ciascuna condizione.

7. Fare clic su **Aggiungi**.

Esempio di creazione di una regola di gruppo

Per creare una regola di gruppo, inclusa la configurazione di una condizione e l'aggiunta di un gruppo di condizioni, eseguire le seguenti operazioni nella finestra di dialogo Aggiungi regola di gruppo:

Fasi

1. Specificare un nome per la regola di gruppo.
2. Selezionare il tipo di oggetto come SVM (Storage Virtual Machine).
3. Selezionare un gruppo dall'elenco dei gruppi.
4. Nella sezione Condizioni, selezionare **Nome oggetto** come operando.
5. Selezionare **contiene** come operatore.
6. Inserire il valore con nome `svm_data`.
7. Fare clic su **Aggiungi gruppo di condizioni**.

8. Selezionare **Nome oggetto** come operando.
9. Selezionare **contiene** come operatore.
10. Inserire il valore con nome `vol`.
11. Fare clic su **Aggiungi condizione**.
12. Ripetere i passi da 8 a 10 selezionando **data-priority** come operando nel passo 8, **is** come operatore nel passo 9 e **critical** come valore nel passo 10.
13. Fare clic su **Aggiungi** per creare la condizione per la regola di gruppo.

Modifica delle regole di gruppo

È possibile modificare le regole di gruppo per modificare i gruppi di condizioni e le condizioni all'interno di un gruppo di condizioni per aggiungere o rimuovere oggetti di storage da o verso un gruppo specifico.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **regole di gruppo**, selezionare la regola di gruppo che si desidera modificare, quindi fare clic su **Modifica**.
3. Nella finestra di dialogo **Edit Group Rule** (Modifica regola gruppo), modificare il nome della regola di gruppo, il nome del gruppo associato, i gruppi di condizioni e le condizioni in base alle esigenze.

   Non è possibile modificare il tipo di oggetto di destinazione per una regola di gruppo.

4. Fare clic su **Save** (Salva).

Eliminazione delle regole di gruppo

È possibile eliminare una regola di gruppo da Active IQ Unified Manager quando la regola di gruppo non è più richiesta.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Quando una regola di gruppo viene eliminata, gli oggetti di storage associati verranno rimossi dal gruppo.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **regole di gruppo**, selezionare la regola di gruppo che si desidera eliminare, quindi fare clic su **Elimina**.
3. Nella finestra di dialogo **Avviso**, confermare l'eliminazione facendo clic su **Sì**.

Aggiunta di azioni di gruppo

È possibile configurare le azioni di gruppo che si desidera applicare agli oggetti di storage di un gruppo. La configurazione delle azioni per un gruppo consente di risparmiare tempo, poiché non è necessario aggiungere queste azioni a ciascun oggetto singolarmente.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **azioni gruppo**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi azione gruppo**, immettere un nome e una descrizione per l'azione.
4. Dal menu **Gruppo**, selezionare un gruppo per il quale si desidera configurare l'azione.
5. Dal menu **Action Type**, selezionare un tipo di azione.

   La finestra di dialogo si espande, consentendo di configurare il tipo di azione selezionato con i parametri richiesti.

6. Immettere i valori appropriati per i parametri richiesti per configurare un'azione di gruppo.
7. Fare clic su **Aggiungi**.

Modifica delle azioni di gruppo

È possibile modificare i parametri delle azioni di gruppo configurati in Unified Manager, ad esempio il nome dell'azione di gruppo, la descrizione, il nome del gruppo associato e i parametri del tipo di azione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **azioni gruppo**, selezionare l'azione di gruppo che si desidera modificare, quindi fare clic su **Modifica**.
3. Nella finestra di dialogo **Modifica azione gruppo**, modificare il nome dell'azione di gruppo, la descrizione, il nome del gruppo associato e i parametri del tipo di azione, come richiesto.
4. Fare clic su **Save** (Salva).

Configurazione delle soglie di integrità dei volumi per i gruppi

È possibile configurare le soglie di integrità dei volumi a livello di gruppo per capacità, copie Snapshot, quote qtree, crescita e inode.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Il tipo di azione di gruppo relativa alla soglia di integrità del volume viene applicato solo ai volumi di un gruppo.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **azioni gruppo**, fare clic su **Aggiungi**.
3. Immettere un nome e una descrizione per l'azione di gruppo.
4. Dalla casella di riepilogo **Gruppo**, selezionare un gruppo per il quale si desidera configurare l'azione di gruppo.
5. Selezionare **Action Type** come soglia di integrità del volume.
6. Selezionare la categoria per la quale si desidera impostare la soglia.
7. Inserire i valori richiesti per la soglia di integrità.
8. Fare clic su **Aggiungi**.

Eliminazione delle azioni di gruppo

È possibile eliminare un'azione di gruppo da Unified Manager quando l'azione di gruppo non è più necessaria.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Quando si elimina l'azione di gruppo per la soglia di integrità del volume, le soglie globali vengono applicate agli oggetti di storage in quel gruppo. Le soglie di integrità a livello di oggetto impostate sull'oggetto di storage non subiscono alcun impatto.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **azioni gruppo**, selezionare l'azione di gruppo che si desidera eliminare, quindi fare clic su **Elimina**.
3. Nella finestra di dialogo **Avviso**, confermare l'eliminazione facendo clic su **Sì**.

Riordinamento delle azioni di gruppo

È possibile modificare l'ordine delle azioni di gruppo da applicare agli oggetti di storage di un gruppo. Le azioni di gruppo vengono applicate agli oggetti storage in sequenza in base al loro rango. Il livello più basso viene assegnato all'azione di gruppo configurata per ultima. È possibile modificare la classificazione dell'azione di gruppo in base alle proprie esigenze.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile selezionare una singola riga o più righe, quindi eseguire più operazioni di trascinamento per modificare il rango delle azioni di gruppo. Tuttavia, è necessario salvare le modifiche affinché la nuova priorità venga riflessa nella griglia delle azioni di gruppo.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Groups**.
2. Nella scheda **azioni gruppo**, fare clic su **Riordina**.
3. Nella finestra di dialogo **Riordina azioni gruppo**, trascinare le righe per riorganizzare la sequenza delle azioni gruppo secondo necessità.
4. Fare clic su **Save** (Salva).

Assegnazione di priorità agli eventi degli oggetti di storage utilizzando le annotazioni

È possibile creare e applicare regole di annotazione agli oggetti di storage in modo da identificare e filtrare tali oggetti in base al tipo di annotazione applicata e alla relativa priorità.

Ulteriori informazioni sulle annotazioni

La comprensione dei concetti relativi alle annotazioni consente di gestire gli eventi correlati agli oggetti di storage nel proprio ambiente.

Quali sono le annotazioni

Un'annotazione è una stringa di testo (il nome) assegnata a un'altra stringa di testo (il valore). Ogni coppia nome-valore dell'annotazione può essere associata dinamicamente agli oggetti di storage utilizzando regole di annotazione. Quando si associano oggetti di storage con annotazioni predefinite, è possibile filtrare e visualizzare gli eventi ad essi correlati. È possibile applicare annotazioni a cluster, volumi e macchine virtuali di storage (SVM).

Ogni nome di annotazione può avere più valori; ogni coppia nome-valore può essere associata a un oggetto di storage attraverso regole.

Ad esempio, è possibile creare un'annotazione denominata "dATA-center" con i valori "Boston" e "Canada". È quindi possibile applicare l'annotazione "data-center" con il valore "Boston" al volume v1. Quando viene generato un avviso per qualsiasi evento su un volume v1 annotato con "dATA-center", l'email generata indica la posizione del volume, "Boston", che consente di assegnare priorità e risolvere il problema.

Funzionamento delle regole di annotazione in Unified Manager

Una regola di annotazione è un criterio definito per annotare gli oggetti di storage (volumi, cluster o macchine virtuali di storage (SVM)). È possibile utilizzare gruppi di condizioni o condizioni per definire le regole di annotazione.

- È necessario associare una regola di annotazione a un'annotazione.
- È necessario associare un tipo di oggetto per una regola di annotazione; è possibile associare un solo tipo di oggetto per una regola di annotazione.
- Unified Manager aggiunge o rimuove le annotazioni dagli oggetti di storage dopo ogni ciclo di monitoraggio o quando una regola viene creata, modificata, eliminata o riordinata.
- Una regola di annotazione può avere uno o più gruppi di condizioni e ciascun gruppo di condizioni può

avere una o più condizioni.

- Gli oggetti di storage possono avere più annotazioni. Una regola di annotazione per una particolare annotazione può anche utilizzare annotazioni diverse nelle condizioni della regola per aggiungere un'altra annotazione agli oggetti già annotati.

Condizioni

È possibile creare più gruppi di condizioni e ciascun gruppo di condizioni può avere una o più condizioni. È possibile applicare tutti i gruppi di condizioni definiti in una regola di annotazione di un'annotazione per annotare gli oggetti di storage.

Le condizioni all'interno di un gruppo di condizioni vengono eseguite utilizzando AND logico. Tutte le condizioni di un gruppo di condizioni devono essere soddisfatte. Quando si crea o si modifica una regola di annotazione, viene creata una condizione che applica, seleziona e annota solo gli oggetti di storage che soddisfano tutte le condizioni del gruppo Condition. È possibile utilizzare più condizioni all'interno di un gruppo di condizioni per limitare l'ambito degli oggetti di storage da annotare.

È possibile creare condizioni con oggetti di storage utilizzando i seguenti operandi e operatore e specificando il valore richiesto.

Tipo di oggetto storage	Operandi applicabili
Volume	• Nome dell'oggetto • Nome del cluster proprietario • Nome SVM proprietario • Annotazioni
SVM	• Nome dell'oggetto • Nome del cluster proprietario • Annotazioni
Cluster	• Nome dell'oggetto • Annotazioni

Quando si seleziona un'annotazione come operando per qualsiasi oggetto di storage, è disponibile l'operatore "is". Per tutti gli altri operandi, è possibile selezionare "is" o "contains" come operatore. Quando si seleziona l'operatore "is", la condizione viene valutata per una corrispondenza esatta del valore dell'operando con il valore fornito per l'operando selezionato. Quando si seleziona l'operatore "contains", la condizione viene valutata per soddisfare uno dei seguenti criteri:

- Il valore dell'operando corrisponde esattamente al valore dell'operando selezionato.
- Il valore dell'operando contiene il valore fornito per l'operando selezionato.

Esempio di una regola di annotazione con condizioni

Prendere in considerazione una regola di annotazione con un gruppo di condizioni per un volume con le seguenti due condizioni:

- Il nome contiene "vol"

- Il nome SVM è “dATA_svm”

Questa regola di annotazione consente di annotare tutti i volumi che includono “vol” nei loro nomi e che sono ospitati sulle SVM con il nome “data_svm” con l’annotazione selezionata e il tipo di annotazione.

Gruppi di condizioni

I gruppi di condizioni vengono eseguiti utilizzando OR logico e quindi applicati agli oggetti di storage. Gli oggetti di storage devono soddisfare i requisiti di uno dei gruppi di condizioni da annotare. Gli oggetti di storage che soddisfano le condizioni di tutti i gruppi di condizioni vengono annotati. È possibile utilizzare i gruppi di condizioni per aumentare l’ambito degli oggetti di storage da annotare.

Esempio di una regola di annotazione con gruppi di condizioni

Prendere in considerazione una regola di annotazione con due gruppi di condizioni per un volume; ciascun gruppo contiene le seguenti due condizioni:

- Gruppo di condizioni 1
  - Il nome contiene “vol”
  - Il nome SVM è “dATA_svm”. Questo gruppo di condizioni annoterà tutti i volumi che includono “vol” nei loro nomi e che sono ospitati sulle SVM con il nome “dATA_svm”.
- Gruppo di condizioni 2
  - Il nome contiene “vol”
  - Il valore di annotazione della priorità dei dati è “critico”. Questo gruppo di condizioni annoterà tutti i volumi che includono “vol” nei loro nomi e che sono annotati con il valore di annotazione della priorità dei dati come “critico”.

Quando una regola di annotazione contenente questi due gruppi di condizioni viene applicata agli oggetti di storage, vengono annotati i seguenti oggetti di storage:

- Tutti i volumi che includono “vol” nei loro nomi e che sono ospitati su SVM con il nome “data_svm”.
- Tutti i volumi che includono “vol” nei loro nomi e che sono annotati con il valore di annotazione data-priority come “critical”.

Descrizione dei valori di annotazione predefiniti

Data-priority è un’annotazione predefinita con i valori Mission Critical, High e Low. Questi valori consentono di annotare gli oggetti di storage in base alla priorità dei dati in essi contenuti. Non è possibile modificare o eliminare i valori di annotazione predefiniti.

- **Priorità dei dati: Mission-critical**

  Questa annotazione viene applicata agli oggetti di storage che contengono dati mission-critical. Ad esempio, gli oggetti che contengono applicazioni di produzione possono essere considerati mission-critical.

- **Priorità dei dati: Alta**

  Questa annotazione viene applicata agli oggetti di storage che contengono dati ad alta priorità. Ad esempio, gli oggetti che ospitano applicazioni di business possono essere considerati ad alta priorità.

- **Priorità dei dati:bassa**

Questa annotazione viene applicata agli oggetti di storage che contengono dati a bassa priorità. Ad esempio, gli oggetti che si trovano sullo storage secondario, come le destinazioni di backup e mirror, potrebbero avere una priorità bassa.

Aggiunta dinamica di annotazioni

Quando si creano annotazioni personalizzate, Unified Manager associa dinamicamente cluster, macchine virtuali di storage (SVM) e volumi alle annotazioni utilizzando le regole. Queste regole assegnano automaticamente le annotazioni agli oggetti di storage.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Annotations**.
2. Nella pagina **Annotazioni**, fare clic su **Aggiungi annotazione**.
3. Nella finestra di dialogo **Aggiungi annotazione**, digitare un nome e una descrizione per l'annotazione.
4. Facoltativo: Nella sezione **Annotation Values** (valori annotazione), fare clic su **Add** (Aggiungi) per aggiungere valori all'annotazione.
5. Fare clic su **Save** (Salva).

Aggiunta di valori alle annotazioni

È possibile aggiungere valori alle annotazioni e associare gli oggetti di storage a una particolare coppia nome-valore dell'annotazione. L'aggiunta di valori alle annotazioni consente di gestire gli oggetti di storage in modo più efficace.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Non è possibile aggiungere valori alle annotazioni predefinite.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Annotations**.
2. Nella pagina **Annotazioni**, selezionare l'annotazione a cui si desidera aggiungere un valore, quindi fare clic su **Aggiungi** nella sezione **valori**.
3. Nella finestra di dialogo **Aggiungi valore annotazione**, specificare un valore per l'annotazione.

   Il valore specificato deve essere univoco per l'annotazione selezionata.

4. Fare clic su **Aggiungi**.

Eliminazione delle annotazioni

È possibile eliminare le annotazioni personalizzate e i relativi valori quando non sono più necessari.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- I valori delle annotazioni non devono essere utilizzati in altre annotazioni o regole di gruppo.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Annotations**.
2. Nella scheda **Annotazioni**, selezionare l'annotazione che si desidera eliminare.

   Vengono visualizzati i dettagli dell'annotazione selezionata.

3. Fare clic su **azioni** > **Elimina** per eliminare l'annotazione selezionata e il relativo valore.
4. Nella finestra di dialogo di avviso, fare clic su **Sì** per confermare l'eliminazione.

Visualizzazione dell'elenco delle annotazioni e dei dettagli

È possibile visualizzare l'elenco delle annotazioni associate dinamicamente a cluster, volumi e macchine virtuali di storage (SVM). È inoltre possibile visualizzare dettagli quali descrizione, creato da, data di creazione, valori, regole, e gli oggetti associati all'annotazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Annotations**.
2. Nella scheda **Annotazioni**, fare clic sul nome dell'annotazione per visualizzare i dettagli associati.

Eliminazione dei valori dalle annotazioni

È possibile eliminare i valori associati alle annotazioni personalizzate quando tale valore non si applica più all'annotazione.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- Il valore dell'annotazione non deve essere associato ad alcuna regola di annotazione o di gruppo.

Non è possibile eliminare i valori dalle annotazioni predefinite.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Annotations**.
2. Nell'elenco Annotazioni della scheda **Annotazioni**, selezionare l'annotazione da cui si desidera eliminare un valore.
3. Nell'area **valori** della scheda **Annotazioni**, selezionare il valore che si desidera eliminare, quindi fare clic su **Elimina**.
4. Nella finestra di dialogo **Avviso**, fare clic su **Sì**.

   Il valore viene cancellato e non viene più visualizzato nell'elenco dei valori per l'annotazione selezionata.

Creazione di regole di annotazione

È possibile creare regole di annotazione utilizzate da Unified Manager per annotare

dinamicamente oggetti di storage come volumi, cluster o macchine virtuali di storage (SVM).

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Gli oggetti di storage attualmente monitorati vengono annotati non appena viene creata la regola di annotazione. I nuovi oggetti vengono annotati solo dopo il completamento del ciclo di monitoraggio.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Annotations**.
2. Nella scheda **Annotation Rules** (regole annotazione), fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo **Add Annotation Rule** (Aggiungi regola annotazione), specificare un nome per la regola di annotazione.
4. Nel campo **Target Object Type**, selezionare il tipo di oggetto di storage che si desidera annotare.
5. Nei campi **Apply Annotation** (Applica annotazione), selezionare il valore di annotazione che si desidera utilizzare.
6. Nella sezione Condizioni, eseguire l'azione appropriata per creare una condizione, un gruppo di condizioni o entrambi:

Per creare…	Eseguire questa operazione…
Una condizione	a. Selezionare un operando dall'elenco. b. Selezionare **contains** o **is** come operatore. c. Inserire un valore o selezionarlo dall'elenco Available (disponibili).
Un gruppo di condizioni	a. Fare clic su **Aggiungi gruppo di condizioni**. b. Selezionare un operando dall'elenco. c. Selezionare **contains** o **is** come operatore. d. Inserire un valore o selezionarlo dall'elenco Available (disponibili). e. Fare clic su **Add Condition** (Aggiungi condizione) per creare ulteriori condizioni, se necessario, e ripetere i passaggi da a a d per ciascuna condizione.

7. Fare clic su **Aggiungi**.

Esempio di creazione di una regola di annotazione

Per creare una regola di annotazione, inclusa la configurazione di una condizione e l'aggiunta di un gruppo di condizioni, eseguire le seguenti operazioni nella finestra di dialogo Aggiungi regola annotazione:

Fasi

1. Specificare un nome per la regola di annotazione.

2. Selezionare il tipo di oggetto di destinazione come SVM (Storage Virtual Machine).
3. Selezionare un'annotazione dall'elenco e specificare un valore.
4. Nella sezione Condizioni, selezionare **Nome oggetto** come operando.
5. Selezionare **contiene** come operatore.
6. Inserire il valore con nome `svm_data`.
7. Fare clic su **Aggiungi gruppo di condizioni**.
8. Selezionare **Nome oggetto** come operando.
9. Selezionare **contiene** come operatore.
10. Inserire il valore con nome `vol`.
11. Fare clic su **Aggiungi condizione**.
12. Ripetere i passi da 8 a 10 selezionando **data-priority** come operando nel passo 8, **is** come operatore nel passo 9 e **mission-critical** come valore nel passo 10.
13. Fare clic su **Aggiungi**.

Aggiunta manuale di annotazioni a singoli oggetti di storage

È possibile annotare manualmente volumi, cluster e SVM selezionati senza utilizzare le regole di annotazione. È possibile annotare un singolo oggetto di storage o più oggetti di storage e specificare la combinazione di coppia nome-valore richiesta per l'annotazione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Individuare gli oggetti di storage che si desidera annotare:

Per aggiungere un'annotazione a…	Eseguire questa operazione…
Cluster	a. Fare clic su **Storage** > **Clusters**. b. Selezionare uno o più cluster.
Volumi	a. Fare clic su **Storage** > **Volumes**. b. Selezionare uno o più volumi.
SVM	a. Fare clic su **Storage** > **SVM**. b. Selezionare una o più SVM.

2. Fare clic su **Annotate** e selezionare una coppia nome-valore.
3. Fare clic su **Apply** (Applica).

Modifica delle regole di annotazione

È possibile modificare le regole di annotazione per modificare i gruppi di condizioni e le

condizioni all'interno del gruppo di condizioni per aggiungere annotazioni o rimuovere annotazioni dagli oggetti di storage.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Le annotazioni vengono dissociate dagli oggetti di storage quando si modificano le regole di annotazione associate.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Annotations**.
2. Nella scheda **Annotation Rules** (regole annotazione), selezionare la regola di annotazione che si desidera modificare, quindi fare clic su **Actions** > **Edit** (azioni*).
3. Nella finestra di dialogo **Edit Annotation Rule** (Modifica regola annotazione), modificare il nome della regola, il nome e il valore dell'annotazione, i gruppi di condizioni e le condizioni secondo necessità.

   Non è possibile modificare il tipo di oggetto di destinazione per una regola di annotazione.

4. Fare clic su **Save** (Salva).

Configurazione delle condizioni per le regole di annotazione

È possibile configurare una o più condizioni per creare regole di annotazione che Unified Manager applica agli oggetti di storage. Gli oggetti di storage che soddisfano la regola di annotazione vengono annotati con il valore specificato nella regola.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Annotations**.
2. Nella scheda **Annotation Rules** (regole annotazione), fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo **Add Annotation Rule** (Aggiungi regola annotazione), immettere un nome per la regola.
4. Selezionare un tipo di oggetto dall'elenco Target Object Type, quindi selezionare un nome e un valore di annotazione dall'elenco.
5. Nella sezione **Condizioni** della finestra di dialogo, selezionare un operando e un operatore dall'elenco e immettere un valore di condizione oppure fare clic su **Aggiungi condizione** per creare una nuova condizione.
6. Fare clic su **Save and Add** (Salva e Aggiungi).

Esempio di configurazione di una condizione per una regola di annotazione

Considerare una condizione per il tipo di oggetto SVM, in cui il nome dell'oggetto contiene "svm_data".

Per configurare la condizione, eseguire le seguenti operazioni nella finestra di dialogo Add Annotation Rule (Aggiungi regola annotazione):

Fasi

1. Inserire un nome per la regola di annotazione.
2. Selezionare il tipo di oggetto di destinazione come SVM.
3. Selezionare un'annotazione dall'elenco delle annotazioni e un valore.
4. Nel campo **Condizioni**, selezionare **Nome oggetto** come operando.
5. Selezionare **contiene** come operatore.
6. Inserire il valore con nome `svm_data`.
7. Fare clic su **Aggiungi**.

Eliminazione delle regole di annotazione

È possibile eliminare le regole di annotazione da Active IQ Unified Manager quando le regole non sono più necessarie.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Quando si elimina una regola di annotazione, l'annotazione viene disassociata e rimossa dagli oggetti di archiviazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Annotations**.
2. Nella scheda **Annotation Rules** (regole annotazione), selezionare la regola di annotazione che si desidera eliminare, quindi fare clic su **Delete** (Elimina).
3. Nella finestra di dialogo **Avviso**, fare clic su **Sì** per confermare l'eliminazione.

Riordinamento delle regole di annotazione

È possibile modificare l'ordine in cui Unified Manager applica le regole di annotazione agli oggetti di storage. Le regole di annotazione vengono applicate agli oggetti di storage in modo sequenziale in base al loro rango. Quando si configura una regola di annotazione, il grado è minimo. Tuttavia, è possibile modificare il rango della regola di annotazione in base alle proprie esigenze.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile selezionare una singola riga o più righe ed eseguire molte operazioni di trascinamento per modificare il rango delle regole di annotazione. Tuttavia, è necessario salvare le modifiche per visualizzare la nuova priorità nella scheda Annotation Rules (regole di annotazione).

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Annotations**.
2. Nella scheda **Annotation Rules** (regole annotazione), fare clic su **Reorder** (Riordina).
3. Nella finestra di dialogo **Riordina regola annotazione**, trascinare una o più righe per riordinare la sequenza delle regole di annotazione.

4. Fare clic su **Save** (Salva).

   È necessario salvare le modifiche per visualizzare il riordino.

Invio di un pacchetto di supporto tramite l'interfaccia utente Web e la console di manutenzione

È necessario inviare un pacchetto di supporto quando il problema richiede una diagnosi e una risoluzione dei problemi più dettagliate rispetto a un messaggio AutoSupport. È possibile inviare un pacchetto di supporto al supporto tecnico utilizzando l'interfaccia utente Web e la console di manutenzione di Unified Manager.

Unified Manager memorizza un massimo di due bundle di supporto completi e tre bundle di supporto leggeri alla volta.

Informazioni correlate

"Ruoli e funzionalità degli utenti di Unified Manager"

Invio di messaggi AutoSupport e pacchetti di supporto al supporto tecnico

La pagina AutoSupport consente di inviare messaggi AutoSupport predefiniti e on-demand al team di supporto tecnico per garantire il corretto funzionamento dell'ambiente e per aiutare l'utente a mantenere l'integrità dell'ambiente. AutoSupport è attivato per impostazione predefinita e non deve essere disattivato per ottenere i vantaggi di NetAppActive IQ.

È possibile inviare informazioni di sistema diagnostiche e dati dettagliati sul server Unified Manager in un messaggio come e quando richiesto, pianificare un messaggio da inviare periodicamente o persino generare e inviare pacchetti di supporto al team di supporto tecnico.

> Un utente con un ruolo di amministratore dello storage può generare e inviare messaggi AutoSupport on-demand e pacchetti di supporto al supporto tecnico. Tuttavia, solo un amministratore o un utente di manutenzione può attivare o disattivare il protocollo AutoSupport periodico e configurare le impostazioni HTTP come descritto nella sezione impostazione del server proxy HTTP. In un ambiente che deve utilizzare un server proxy HTTP, la configurazione deve essere completa prima che un amministratore dello storage possa inviare messaggi AutoSupport on-demand e pacchetti di supporto al supporto tecnico.

Invio di messaggi AutoSupport on-demand

È possibile generare e inviare un messaggio on-demand al supporto tecnico, a un destinatario e-mail specificato o a entrambi.

Fasi

1. Accedere a **Generale** > **AutoSupport** ed eseguire una o entrambe le operazioni descritte di seguito:
2. Se si desidera inviare il messaggio AutoSupport al supporto tecnico, selezionare la casella di controllo **Invia al supporto tecnico**.
3. Se si desidera inviare il messaggio AutoSupport a un destinatario di posta elettronica specifico, selezionare la casella di controllo **Invia a destinatario di posta elettronica** e immettere l'indirizzo di posta

elettronica del destinatario.

4. Fare clic su **Save** (Salva).
5. Fare clic su **generate and Send AutoSupport** (genera e invia dati).

Abilitazione di Periodic AutoSupport

È possibile inviare messaggi specifici e predefiniti al supporto tecnico per la diagnosi e la risoluzione dei problemi periodicamente. Questa funzionalità è attivata per impostazione predefinita. Se questa opzione è disattivata, un amministratore o un utente di manutenzione può attivare le impostazioni.

Fasi

1. Selezionare **Generale** > **AutoSupport**.
2. Nella sezione Periodic AutoSupport, selezionare la casella di controllo **Enable Sending AutoSupport Sending periodicamente to Active IQ** (Abilita invio periodico dati a).
3. Se necessario, definire il nome, la porta e le informazioni di autenticazione per il server proxy HTTP come descritto nella sezione impostazione del server proxy HTTP.
4. Fare clic su **Save** (Salva).

Caricamento del bundle di supporto on-demand

È possibile generare e inviare un pacchetto di supporto al supporto tecnico in base ai requisiti per la risoluzione dei problemi. Unified Manager memorizza solo i due pacchetti di supporto generati più di recente. I pacchetti di supporto meno recenti vengono eliminati dal sistema.

Poiché alcuni tipi di dati di supporto possono utilizzare una grande quantità di risorse del cluster o richiedere molto tempo per il completamento, quando si seleziona il bundle di supporto completo, è possibile includere o escludere tipi di dati specifici per ridurre le dimensioni del bundle di supporto. È inoltre possibile creare un bundle di supporto leggero che contiene solo 30 giorni di registri e record del database di configurazione, escludendo i dati sulle performance, i file di registrazione dell'acquisizione e il dump dell'heap del server.

Fasi

1. Selezionare **Generale** > **AutoSupport**.
2. Nella sezione on-Demand Support Bundle, fare clic su **generate and Send Support Bundle**.
3. Per inviare un pacchetto di supporto leggero al supporto tecnico, nella finestra a comparsa generate and Send Support Bundle (genera e invia bundle di supporto), selezionare la casella di controllo**generate light support bundle**.
4. In alternativa, per inviare un bundle di supporto completo, selezionare la casella di controllo **generate full support bundle** (genera bundle di supporto completo). Selezionare i tipi di dati specifici da includere o escludere nel bundle di supporto.

   Anche se non si seleziona alcun tipo di dati, il bundle di supporto viene comunque generato con altri dati di Unified Manager.

5. Selezionare la casella di controllo **Invia il bundle al supporto tecnico** per generare e inviare il bundle al supporto tecnico. Se non si seleziona questa casella di controllo, il bundle viene generato e memorizzato localmente nel server Unified Manager. Il bundle di supporto generato è disponibile per l'utilizzo successivo nella directory /support sui sistemi VMware, in `/opt/netapp/data/support/` Su sistemi Linux e in `ProgramData\NetApp\OnCommandAppData\ocum\support` Sui sistemi Windows.
6. Fare clic su **Invia**.

Configurazione del server proxy HTTP

È possibile designare un proxy per fornire l'accesso a Internet per inviare il contenuto AutoSupport al supporto se l'ambiente non fornisce l'accesso diretto dal server Unified Manager. Questa sezione è disponibile solo per gli amministratori e gli utenti di manutenzione.

- **Usa proxy HTTP**

  Selezionare questa casella per identificare il server utilizzato come proxy HTTP.

  Immettere il nome host o l'indirizzo IP del server proxy e il numero di porta utilizzato per connettersi al server.

- **Usa autenticazione**

  Selezionare questa casella se si desidera fornire informazioni di autenticazione per accedere al server utilizzato come proxy HTTP.

  Immettere il nome utente e la password richiesti per l'autenticazione con il proxy HTTP.

I proxy HTTP che forniscono solo l'autenticazione di base non sono supportati.

Accesso alla console di manutenzione

Se l'interfaccia utente di Unified Manager non è in funzione o se è necessario eseguire funzioni non disponibili nell'interfaccia utente, è possibile accedere alla console di manutenzione per gestire il sistema Unified Manager.

Cosa ti serve

Unified Manager deve essere installato e configurato.

Dopo 15 minuti di inattività, la console di manutenzione si disconnette.

Una volta installato su VMware, se si è già effettuato l'accesso come utente di manutenzione tramite la console VMware, non è possibile effettuare l'accesso simultaneo utilizzando Secure Shell.

Fase

1. Per accedere alla console di manutenzione, procedere come segue:

Su questo sistema operativo…	Attenersi alla procedura descritta di seguito…
VMware	a. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo dell'appliance virtuale Unified Manager. b. Accedere alla console di manutenzione utilizzando il nome utente e la password di manutenzione.

Su questo sistema operativo…	Attenersi alla procedura descritta di seguito…
Linux	a. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo del sistema Unified Manager. b. Accedere al sistema con il nome utente di manutenzione (umadmin) e la password. c. Immettere il comando `maintenance_console` E premere Invio.
Windows	a. Accedere al sistema Unified Manager con le credenziali di amministratore. b. Avviare PowerShell come amministratore di Windows. c. Immettere il comando `maintenance_console` E premere Invio.

Viene visualizzato il menu della console di manutenzione di Unified Manager.

Generazione e caricamento di un bundle di supporto

È possibile generare un pacchetto di supporto contenente informazioni diagnostiche, in modo da inviarlo al supporto tecnico per la risoluzione dei problemi.

A partire da Unified Manager 9.8, se il server Unified Manager è connesso a Internet, è anche possibile caricare il pacchetto di supporto a NetApp dalla console di manutenzione.

Cosa ti serve

È necessario avere accesso alla console di manutenzione come utente di manutenzione.

Poiché alcuni tipi di dati di supporto possono utilizzare una grande quantità di risorse del cluster o richiedere molto tempo per il completamento, quando si seleziona il bundle di supporto completo è possibile specificare i tipi di dati da includere o escludere per ridurre le dimensioni del bundle di supporto. È inoltre possibile creare un bundle di supporto leggero che contiene solo 30 giorni di registri e record del database di configurazione, escludendo i dati sulle performance, i file di registrazione dell'acquisizione e il dump dell'heap del server.

Unified Manager memorizza solo i due pacchetti di supporto generati più di recente. I pacchetti di supporto meno recenti vengono eliminati dal sistema.

Fasi

1. Nella console di manutenzione **Menu principale**, selezionare **supporto/Diagnostica**.
2. Selezionare **generate Light Support Bundle** o **generate Support Bundle** a seconda del livello di dettagli che si desidera includere nel pacchetto di supporto.
3. Se si sceglie il bundle di supporto completo, selezionare o deselezionare i seguenti tipi di dati da includere o escludere nel bundle di supporto:
    - **dump del database**

Un dump del database MySQL Server.

- **heap dump**

  Un'istantanea dello stato dei principali processi del server Unified Manager. Questa opzione è disattivata per impostazione predefinita e deve essere selezionata solo quando richiesto dall'assistenza clienti.

- **registrazioni di acquisizione**

  Registrazione di tutte le comunicazioni tra Unified Manager e i cluster monitorati.

> Se si deselezionano tutti i tipi di dati, il bundle di supporto viene ancora generato con altri dati di Unified Manager.

4. Tipo `g`, Quindi premere Invio per generare il bundle di supporto.

   Poiché la generazione di un bundle di supporto è un'operazione che richiede un uso intensivo della memoria, viene richiesto di verificare di voler generare il bundle di supporto in questo momento.

5. Tipo `y`, Quindi premere Invio per generare il bundle di supporto.

   Se non si desidera generare il bundle di supporto in questo momento, digitare `n`, Quindi premere Invio.

6. Se sono stati inclusi i file dump del database nel bundle di supporto completo, viene richiesto di specificare il periodo di tempo per il quale si desidera includere le statistiche delle performance. L'inclusione delle statistiche sulle performance può richiedere molto tempo e spazio, per cui è possibile eseguire il dump del database senza includere statistiche sulle performance:

   a. Inserire la data di inizio nel formato AAAAMMGG.

      Ad esempio, immettere `20210101` Per il 1° gennaio 2021. Invio `n` se non si desidera includere le statistiche delle performance.

   b. Inserire il numero di giorni di statistiche da includere, a partire dalle 12 alla data di inizio specificata.

      È possibile immettere un numero compreso tra 1 e 10.

   Se si includono le statistiche delle performance, il sistema visualizza il periodo di tempo per il quale verranno raccolte le statistiche delle performance.

7. Una volta creato il pacchetto di supporto, viene richiesto se si desidera caricarlo su NetApp. Tipo `y`, Quindi premere Invio.

   Viene richiesto di inserire il numero del caso di supporto.

8. Se si dispone già di un numero di caso, immetterlo e premere Invio. In caso contrario, premere Invio.

   Il bundle di supporto viene caricato in NetApp.

Se il server Unified Manager non è connesso a Internet o non è possibile caricare il bundle di supporto per qualsiasi altro motivo, è possibile recuperarlo e inviarlo manualmente. È possibile recuperarlo utilizzando un client SFTP o i comandi CLI UNIX o Linux. Nelle installazioni Windows è possibile utilizzare Desktop remoto (RDP) per recuperare il bundle di supporto.

Il bundle di supporto generato si trova nella directory /support sui sistemi VMware, in /opt/netapp/data/support/ sui sistemi Linux e in ProgramData/NetApp/OnCommandAppData/ocum/support sui sistemi Windows.

Informazioni correlate

"Ruoli e funzionalità degli utenti di Unified Manager"

Recupero del bundle di supporto utilizzando un client Windows

Gli utenti Windows possono scaricare e installare uno strumento per recuperare il pacchetto di supporto dal server Unified Manager. È possibile inviare il pacchetto di supporto al supporto tecnico per una diagnosi più dettagliata di un problema. FileZilla o WinSCP sono esempi di strumenti che è possibile utilizzare.

Cosa ti serve

Per eseguire questa attività, è necessario essere l'utente che esegue la manutenzione.

È necessario utilizzare uno strumento che supporti SCP o SFTP.

Fasi

1. Scaricare e installare uno strumento per recuperare il pacchetto di supporto.
2. Aprire lo strumento.
3. Connettersi al server di gestione di Unified Manager tramite SFTP.

   Lo strumento visualizza il contenuto della directory /support ed è possibile visualizzare tutti i pacchetti di supporto esistenti.
4. Selezionare la directory di destinazione del pacchetto di supporto che si desidera copiare.
5. Selezionare il pacchetto di supporto che si desidera copiare e utilizzare lo strumento per copiare il file dal server Unified Manager al sistema locale.

Recupero del bundle di supporto utilizzando un client UNIX o Linux

Se si utilizza UNIX o Linux, è possibile recuperare il pacchetto di supporto dalla vApp utilizzando l'interfaccia a riga di comando (CLI) sul server client Linux. È possibile utilizzare SCP o SFTP per recuperare il bundle di supporto.

Cosa ti serve

Per eseguire questa attività, è necessario essere l'utente che esegue la manutenzione.

È necessario aver generato un bundle di supporto utilizzando la console di manutenzione e avere a disposizione il nome del bundle di supporto.

Fasi

1. Accedere alla CLI tramite Telnet o la console, utilizzando il server client Linux.
2. Accedere a. `/support` directory.
3. Recuperare il pacchetto di supporto e copiarlo nella directory locale utilizzando il seguente comando:

Se si utilizza…	Quindi utilizzare il seguente comando…
SCP	`scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`
SFTP	`sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`

Il nome del bundle di supporto viene fornito quando viene generato utilizzando la console di manutenzione.

4. Inserire la password utente per la manutenzione.

Esempi

Nell'esempio seguente viene utilizzato SCP per recuperare il bundle di supporto:

```
        `$ 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
```

Nell'esempio seguente viene utilizzato SFTP per recuperare il bundle di supporto:

```
        `$ 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
```

Invio di un pacchetto di supporto al supporto tecnico

Quando un problema richiede informazioni di diagnosi e risoluzione dei problemi più dettagliate rispetto a quelle fornite da un messaggio AutoSupport, è possibile inviare un pacchetto di supporto al supporto tecnico.

Cosa ti serve

È necessario disporre dell'accesso al pacchetto di supporto per inviarlo al supporto tecnico.

È necessario disporre di un numero di caso generato tramite il sito Web del supporto tecnico.

Fasi

1. Accedere al sito di supporto NetApp.

2. Caricare il file.

   "Come caricare un file su NetApp"

Attività e informazioni relative a diversi flussi di lavoro

Alcune attività e testi di riferimento che possono aiutarti a comprendere e completare un workflow sono comuni a molti dei flussi di lavoro di Unified Manager, tra cui l'aggiunta e la revisione di note su un evento, l'assegnazione di un evento, il riconoscimento e la risoluzione di eventi e dettagli su volumi, storage virtual machine (SVM), aggregati, e così via.

Componenti del cluster e perché possono essere in conflitto

È possibile identificare i problemi di performance del cluster quando un componente del cluster entra in conflitto. Le performance dei carichi di lavoro che utilizzano il componente rallentano e il loro tempo di risposta (latenza) per le richieste dei client aumenta, il che attiva un evento in Unified Manager.

Un componente in conflitto non può funzionare a un livello ottimale. Le sue performance sono diminuite e le performance di altri componenti e carichi di lavoro del cluster, denominati *vittime*, potrebbero avere una maggiore latenza. Per eliminare un componente dai conflitti, è necessario ridurre il carico di lavoro o aumentare la capacità di gestire più lavoro, in modo che le performance possano tornare ai livelli normali. Poiché Unified Manager raccoglie e analizza le performance dei carichi di lavoro in intervalli di cinque minuti, rileva solo quando un componente del cluster viene costantemente utilizzato in eccesso. I picchi transitori di utilizzo eccessivo che durano solo per una breve durata nell'intervallo di cinque minuti non vengono rilevati.

Ad esempio, un aggregato di storage potrebbe essere in conflitto perché uno o più carichi di lavoro su di esso sono in competizione per soddisfare le richieste di i/O. Altri carichi di lavoro sull'aggregato possono risentirne, causando una diminuzione delle performance. Per ridurre la quantità di attività sull'aggregato, è possibile eseguire diverse operazioni, ad esempio lo spostamento di uno o più carichi di lavoro in un aggregato o nodo meno occupato, per ridurre la domanda complessiva del carico di lavoro sull'aggregato corrente. Per un gruppo di policy QoS, è possibile regolare il limite di throughput o spostare i carichi di lavoro in un gruppo di policy diverso, in modo che i carichi di lavoro non vengano più rallentati.

Unified Manager monitora i seguenti componenti del cluster per avvisare l'utente quando si trovano in conflitto:

- **Rete**

  Rappresenta il tempo di attesa delle richieste di i/o da parte dei protocolli di rete esterni sul cluster. Il tempo di attesa è il tempo impiegato in attesa del completamento delle transazioni "transfer ready" prima che il cluster possa rispondere a una richiesta di i/O. Se il componente di rete è in conflitto, significa che il tempo di attesa elevato a livello di protocollo influisce sulla latenza di uno o più carichi di lavoro.

- **Elaborazione di rete**

  Rappresenta il componente software del cluster coinvolto nell'elaborazione i/o tra il livello di protocollo e il cluster. Il nodo che gestisce l'elaborazione di rete potrebbe essere cambiato da quando è stato rilevato l'evento. Se il componente di elaborazione di rete è in conflitto, significa che un utilizzo elevato nel nodo di elaborazione di rete influisce sulla latenza di uno o più carichi di lavoro.

  Quando si utilizza un cluster All SAN Array in una configurazione Active-Active, il valore di latenza di

elaborazione della rete viene visualizzato per entrambi i nodi, in modo da poter verificare che i nodi condividano il carico in maniera uguale.

- **QoS Limit Max**

  Rappresenta l'impostazione di throughput massimo (picco) del gruppo di criteri QoS (Quality of Service) dello storage assegnato al carico di lavoro. Se il componente del gruppo di policy è in conflitto, significa che tutti i carichi di lavoro nel gruppo di policy vengono rallentati dal limite di throughput impostato, il che influisce sulla latenza di uno o più di tali carichi di lavoro.

- **Limite QoS min**

  Rappresenta la latenza per un carico di lavoro causata dall'impostazione QoS throughput Minimum (previsto) assegnata ad altri carichi di lavoro. Se il valore minimo di QoS impostato su alcuni carichi di lavoro utilizza la maggior parte della larghezza di banda per garantire il throughput promesso, altri carichi di lavoro verranno rallentati e otterranno una maggiore latenza.

- **Interconnessione cluster**

  Rappresenta i cavi e gli adattatori con cui i nodi in cluster sono fisicamente connessi. Se il componente di interconnessione del cluster è in conflitto, significa che l'elevato tempo di attesa per le richieste di i/o dell'interconnessione del cluster influisce sulla latenza di uno o più carichi di lavoro.

- **Elaborazione dei dati**

  Rappresenta il componente software del cluster coinvolto nell'elaborazione i/o tra il cluster e l'aggregato di storage che contiene il carico di lavoro. Il nodo che gestisce l'elaborazione dei dati potrebbe essere cambiato da quando è stato rilevato l'evento. Se il componente di elaborazione dei dati è in conflitto, significa che un utilizzo elevato nel nodo di elaborazione dei dati influisce sulla latenza di uno o più carichi di lavoro.

- **Attivazione del volume**

  Rappresenta il processo che tiene traccia dell'utilizzo di tutti i volumi attivi. In ambienti di grandi dimensioni in cui sono attivi più di 1000 volumi, questo processo tiene traccia del numero di volumi critici necessari per accedere alle risorse attraverso il nodo allo stesso tempo. Quando il numero di volumi attivi simultanei supera la soglia massima consigliata, alcuni volumi non critici sperimenteranno la latenza come indicato qui.

- **Risorse MetroCluster**

  Rappresenta le risorse MetroCluster, tra cui NVRAM e ISL (Interswitch link), utilizzate per eseguire il mirroring dei dati tra cluster in una configurazione MetroCluster. Se il componente MetroCluster è in conflitto, significa che un elevato throughput di scrittura dai carichi di lavoro sul cluster locale o un problema di integrità del collegamento sta influenzando la latenza di uno o più carichi di lavoro sul cluster locale. Se il cluster non si trova in una configurazione MetroCluster, questa icona non viene visualizzata.

- **Operazioni aggregate o aggregate SSD**

  Rappresenta l'aggregato di storage su cui vengono eseguiti i carichi di lavoro. Se il componente aggregato è in conflitto, significa che un utilizzo elevato dell'aggregato influisce sulla latenza di uno o più carichi di lavoro. Un aggregato è costituito da tutti i dischi rigidi o da una combinazione di dischi rigidi e SSD (un aggregato di pool flash) o da una combinazione di dischi rigidi e un Tier cloud (un aggregato FabricPool). Un "Saggregato SD" è costituito da tutti gli SSD (un aggregato all-flash) o da una combinazione di SSD e un Tier cloud (un aggregato FabricPool).

- **Latenza cloud**

  Rappresenta il componente software del cluster coinvolto nell'elaborazione i/o tra il cluster e il livello cloud in cui vengono memorizzati i dati dell'utente. Se il componente di latenza del cloud è in conflitto, significa che una grande quantità di letture da volumi ospitati sul Tier cloud influisce sulla latenza di uno o più carichi di lavoro.

- **Sync SnapMirror**

  Rappresenta il componente software del cluster coinvolto nella replica dei dati utente dal volume primario al volume secondario in una relazione sincrona di SnapMirror. Se il componente Sync SnapMirror è in conflitto, significa che l'attività delle operazioni di SnapMirror Synchronous influisce sulla latenza di uno o più carichi di lavoro.

Pagina dei dettagli relativi a volume/salute

È possibile utilizzare la pagina Volume / Health Details per visualizzare informazioni dettagliate su un volume selezionato, ad esempio capacità, efficienza dello storage, configurazione, protezione, annotazioni ed eventi generati. È inoltre possibile visualizzare informazioni sugli oggetti correlati e sugli avvisi correlati per il volume.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni per il volume selezionato:

- **Passa alla visualizzazione delle performance**

  Consente di accedere alla pagina dei dettagli relativi a volume/prestazioni.

- **Azioni**
  - Aggiungi avviso

    Consente di aggiungere un avviso al volume selezionato.

  - Modificare le soglie

    Consente di modificare le impostazioni di soglia per il volume selezionato.

  - Annotare

    Consente di annotare il volume selezionato.

  - Proteggere

    Consente di creare relazioni SnapMirror o SnapVault per il volume selezionato.

  - Relazione

    Consente di eseguire le seguenti operazioni di relazione di protezione:

    - Modifica

Apre la finestra di dialogo Edit Relationship (Modifica relazione) che consente di modificare policy, pianificazioni e velocità di trasferimento massime di SnapMirror esistenti per una relazione di protezione esistente.

- Interrompere

  Interrompe i trasferimenti in corso per una relazione selezionata. Facoltativamente, consente di rimuovere il checkpoint di riavvio per i trasferimenti diversi dal trasferimento di riferimento. Non è possibile rimuovere il punto di verifica per un trasferimento di riferimento.

- Quiesce

  Disattiva temporaneamente gli aggiornamenti pianificati per una relazione selezionata. I trasferimenti già in corso devono essere completati prima di interrompere la relazione.

- Rompere

  Interrompe la relazione tra i volumi di origine e di destinazione e modifica la destinazione in un volume di lettura/scrittura.

- Rimuovere

  Elimina in modo permanente la relazione tra l'origine e la destinazione selezionate. I volumi non vengono distrutti e le copie Snapshot sui volumi non vengono rimosse. Questa operazione non può essere annullata.

- Riprendi

  Consente i trasferimenti pianificati per una relazione a cui è stata data la disattivazione. Al successivo intervallo di trasferimento pianificato, viene utilizzato un checkpoint di riavvio, se presente.

- Risincronizzare

  Consente di risincronizzare una relazione interrotta in precedenza.

- Inizializzare/aggiornare

  Consente di eseguire un primo trasferimento baseline su una nuova relazione di protezione o di eseguire un aggiornamento manuale se la relazione è già inizializzata.

- Risincronizzazione inversa

  Consente di ristabilire una relazione di protezione precedentemente interrotta, invertendo la funzione dell'origine e della destinazione creando una copia dell'origine. I contenuti dell'origine vengono sovrascritti dai contenuti della destinazione e tutti i dati più recenti rispetto ai dati della copia Snapshot comune vengono cancellati.

◦ Ripristinare

Consente di ripristinare i dati da un volume a un altro. Per ulteriori informazioni, vedere "Ripristino dei dati mediante la pagina dei dettagli relativi a volume/salute".

Il pulsante Restore (Ripristina) e i pulsanti Relationship Operation (operazione relazione) non sono disponibili per i volumi che si trovano in relazioni di protezione sincrone.

- **Visualizza volumi**

  Consente di passare alla vista Health: All Volumes (Salute: Tutti i volumi).

Scheda capacità

La scheda Capacity (capacità) visualizza i dettagli relativi al volume selezionato, ad esempio la capacità fisica, la capacità logica, le impostazioni di soglia, la capacità di quota e le informazioni relative a qualsiasi operazione di spostamento del volume:

- **Capacità fisica**

  Dettagli sulla capacità fisica del volume:

  - Overflow dello snapshot

    Visualizza lo spazio dati utilizzato dalle copie Snapshot.

  - Utilizzato

    Visualizza lo spazio utilizzato dai dati nel volume.

  - Attenzione

    Indica che lo spazio nel volume è quasi pieno. Se questa soglia viene superata, viene generato l'evento spazio quasi pieno.

  - Errore

    Indica che lo spazio nel volume è pieno. Se questa soglia viene superata, viene generato l'evento spazio pieno.

  - Inutilizzabile

    Indica che viene generato l'evento Thin-Provisioning Volume Space at Risk e che lo spazio nel volume con thin provisioning è a rischio a causa di problemi di capacità aggregata. La capacità inutilizzabile viene visualizzata solo per i volumi con thin provisioning.

  - Grafico dei dati

    Visualizza la capacità totale dei dati e la capacità utilizzata del volume.

    Se la funzione di crescita automatica è attivata, il grafico dei dati visualizza anche lo spazio disponibile nell'aggregato. Il grafico dei dati mostra lo spazio di storage effettivo che può essere utilizzato dai dati nel volume, che può essere uno dei seguenti:

    - Capacità effettiva dei dati del volume per le seguenti condizioni:
      - Crescita automatica disattivata.
      - Il volume abilitato per la crescita automatica ha raggiunto la dimensione massima.
      - Il volume con provisioning di spessore abilitato per la crescita automatica non può crescere ulteriormente.
    - Capacità dei dati del volume dopo aver preso in considerazione le dimensioni massime del volume (per volumi con thin provisioning e per volumi con provisioning spesso quando l'aggregato dispone

di spazio per il volume per raggiungere le dimensioni massime)

- Capacità dei dati del volume dopo aver preso in considerazione la successiva dimensione di crescita automatica possibile (per volumi con provisioning spesso con una soglia percentuale di crescita automatica)

◦ Grafico delle copie Snapshot

Questo grafico viene visualizzato solo quando la capacità Snapshot utilizzata o la riserva Snapshot non è pari a zero.

Entrambi i grafici mostrano la capacità con cui la capacità Snapshot supera la riserva Snapshot se la capacità Snapshot utilizzata supera la riserva Snapshot.

- **Logica della capacità**

Visualizza le caratteristiche dello spazio logico del volume. Lo spazio logico indica la dimensione reale dei dati memorizzati su disco senza applicare i risparmi derivanti dall'utilizzo delle tecnologie di efficienza dello storage ONTAP.

◦ Reporting dello spazio logico

Visualizza se il volume ha configurato il reporting dello spazio logico. Il valore può essere Enabled (attivato), Disabled (Disattivato) o Not applicable (non applicabile). "non applicabile" viene visualizzato per i volumi su versioni precedenti di ONTAP o su volumi che non supportano il reporting dello spazio logico.

◦ Utilizzato

Visualizza la quantità di spazio logico utilizzata dai dati nel volume e la percentuale di spazio logico utilizzata in base alla capacità totale dei dati.

◦ Applicazione dello spazio logico

Visualizza se l'imposizione dello spazio logico è configurata per volumi con thin provisioning. Se impostato su Enabled (attivato), la dimensione logica utilizzata del volume non può essere superiore alla dimensione fisica del volume attualmente impostata.

- **Crescita automatica**

Visualizza se il volume cresce automaticamente quando è fuori spazio.

- **Garanzia di spazio**

Visualizza il controllo delle impostazioni del volume FlexVol quando un volume rimuove i blocchi liberi da un aggregato. Questi blocchi sono quindi garantiti per essere disponibili per le scritture nei file nel volume. La garanzia di spazio può essere impostata su una delle seguenti opzioni:

◦ Nessuno

Non è stata configurata alcuna garanzia di spazio per il volume.

◦ File

È garantita la dimensione completa dei file poco scritti (ad esempio LUN).

◦ Volume

La dimensione completa del volume è garantita.

- Parziale

  Il volume FlexCache riserva spazio in base alle sue dimensioni. Se le dimensioni del volume FlexCache sono pari o superiori a 100 MB, per impostazione predefinita viene impostato lo spazio minimo garantito su 100 MB. Se le dimensioni del volume FlexCache sono inferiori a 100 MB, lo spazio minimo garantito viene impostato sulle dimensioni del volume FlexCache. Se le dimensioni del volume FlexCache vengono aumentate in seguito, la garanzia di spazio minimo non viene incrementata.

La garanzia di spazio è parziale quando il volume è di tipo Data-cache.

- **Dettagli (fisici)**

  Visualizza le caratteristiche fisiche del volume.

- **Capacità totale**

  Visualizza la capacità fisica totale nel volume.

- **Capacità dei dati**

  Visualizza la quantità di spazio fisico utilizzato dal volume (capacità utilizzata) e la quantità di spazio fisico ancora disponibile (capacità libera) nel volume. Questi valori vengono visualizzati anche come percentuale della capacità fisica totale.

  Quando l'evento Thin-Provised Volume Space at Risk viene generato per volumi con thin provisioning, viene visualizzata la quantità di spazio utilizzata dal volume (capacità utilizzata) e la quantità di spazio disponibile nel volume ma non utilizzabile (capacità inutilizzabile) a causa di problemi di capacità aggregata.

- **Snapshot Reserve**

  Visualizza la quantità di spazio utilizzata dalle copie Snapshot (capacità utilizzata) e la quantità di spazio disponibile per le copie Snapshot (capacità libera) nel volume. Questi valori vengono visualizzati anche come percentuale della riserva snapshot totale.

  Quando viene generato l'evento Thin-Provisioning Volume Space at Risk per volumi con thin provisioning, la quantità di spazio utilizzata dalle copie Snapshot (capacità utilizzata) e la quantità di spazio disponibile nel volume ma non utilizzabile per la creazione di copie Snapshot (capacità inutilizzabile) a causa di problemi di capacità aggregata viene visualizzato.

- **Soglie del volume**

  Visualizza le seguenti soglie di capacità del volume:

  - Soglia quasi completa

    Specifica la percentuale in cui un volume è quasi pieno.

  - Soglia completa

    Specifica la percentuale di riempimento di un volume.

- **Altri dettagli**

- Dimensione massima crescita automatica

  Visualizza le dimensioni massime fino alle quali il volume può crescere automaticamente. Il valore predefinito è il 120% delle dimensioni del volume al momento della creazione. Questo campo viene visualizzato solo quando la funzione di crescita automatica è attivata per il volume.

- Capacità impegnata quota qtree

  Visualizza lo spazio riservato nelle quote.

- Capacità di overcommit quota qtree

  Visualizza la quantità di spazio che è possibile utilizzare prima che il sistema generi l'evento Volume Qtree quota Overcommit.

- Riserva frazionaria

  Controlla le dimensioni della riserva di sovrascrittura. Per impostazione predefinita, la riserva frazionale è impostata su 100, a indicare che il 100% dello spazio riservato richiesto è riservato in modo che gli oggetti siano completamente protetti per le sovrascritture. Se la riserva frazionale è inferiore al 100%, lo spazio riservato per tutti i file con spazio riservato in quel volume viene ridotto alla percentuale di riserva frazionale.

- Snapshot Daily Growth Rate

  Visualizza la modifica (in percentuale o in KB, MB, GB e così via) che si verifica ogni 24 ore nelle copie Snapshot del volume selezionato.

- Snapshot Days to Full (giorni snapshot completi)

  Visualizza il numero stimato di giorni rimanenti prima che lo spazio riservato per le copie Snapshot nel volume raggiunga la soglia specificata.

  Il campo Snapshot Days to Full (giorni snapshot a pieno) visualizza un valore non applicabile quando il tasso di crescita delle copie Snapshot nel volume è pari a zero o negativo o quando i dati non sono sufficienti per calcolare il tasso di crescita.

- Eliminazione automatica di Snapshot

  Specifica se le copie Snapshot vengono eliminate automaticamente in spazio libero quando una scrittura su un volume non riesce a causa della mancanza di spazio nell'aggregato.

- Copie Snapshot

  Visualizza le informazioni sulle copie Snapshot nel volume.

  Il numero di copie Snapshot nel volume viene visualizzato come collegamento. Facendo clic sul collegamento, viene visualizzata la finestra di dialogo Snapshot Copies on a Volume (copie Snapshot su un volume), che visualizza i dettagli delle copie Snapshot.

Il conteggio delle copie Snapshot viene aggiornato circa ogni ora; tuttavia, l'elenco delle copie Snapshot viene aggiornato quando si fa clic sull'icona. Ciò potrebbe determinare una differenza tra il numero di copie Snapshot visualizzate nella topologia e il numero di copie Snapshot elencate quando si fa clic sull'icona.

- **Spostamento del volume**

Visualizza lo stato dell'operazione corrente o dell'ultima operazione di spostamento del volume eseguita sul volume e altri dettagli, come la fase corrente dell'operazione di spostamento del volume in corso, l'aggregato di origine, l'aggregato di destinazione, l'ora di inizio, l'ora di fine, e ora di fine prevista.

Visualizza anche il numero di operazioni di spostamento del volume eseguite sul volume selezionato. Per ulteriori informazioni sulle operazioni di spostamento del volume, fare clic sul collegamento **Volume Move History** (Cronologia spostamento volume).

Scheda Configuration (Configurazione)

La scheda Configuration (Configurazione) visualizza i dettagli relativi al volume selezionato, ad esempio il criterio di esportazione, il tipo di RAID, la capacità e le funzionalità correlate all'efficienza dello storage del volume:

- **Panoramica**
  - Nome completo

    Visualizza il nome completo del volume.

  - Aggregati

    Visualizza il nome dell'aggregato su cui risiede il volume o il numero di aggregati su cui risiede il volume FlexGroup.

  - Policy di tiering

    Visualizza il set di criteri di tiering per il volume, se il volume viene distribuito su un aggregato abilitato a FabricPool. Il criterio può essere Nessuno, solo snapshot, Backup, Auto o tutto.

  - VM di storage

    Visualizza il nome della SVM che contiene il volume.

  - Percorso di giunzione

    Visualizza lo stato del percorso, che può essere attivo o inattivo. Viene visualizzato anche il percorso nella SVM su cui è montato il volume. Fare clic sul collegamento **History** per visualizzare le cinque modifiche più recenti al percorso di giunzione.

  - Policy di esportazione

    Visualizza il nome del criterio di esportazione creato per il volume. È possibile fare clic sul collegamento per visualizzare i dettagli relativi ai criteri di esportazione, ai protocolli di autenticazione e all'accesso attivato sui volumi che appartengono a SVM.

  - Stile

    Visualizza lo stile del volume. Lo stile del volume può essere FlexVol o FlexGroup.

  - Tipo

    Visualizza il tipo di volume selezionato. Il tipo di volume può essere Read-write, Load-sharing, Data-Protection, Data-cache o Temporary.

- Tipo RAID

  Visualizza il tipo di RAID del volume selezionato. Il tipo RAID può essere RAID0, RAID4, RAID-DP o RAID-TEC.

  > È possibile che vengano visualizzati diversi tipi di RAID per i volumi FlexGroup, poiché i volumi costituenti per FlexGroup possono trovarsi su aggregati di tipi diversi.

- Tipo di SnapLock

  Visualizza il tipo di SnapLock dell'aggregato che contiene il volume.

- Scadenza SnapLock

  Visualizza la data di scadenza del volume SnapLock.

- **Capacità**
  - Thin provisioning

    Visualizza se il thin provisioning è configurato per il volume.

  - Crescita automatica

    Visualizza se il volume flessibile cresce automaticamente all'interno di un aggregato.

  - Eliminazione automatica di Snapshot

    Specifica se le copie Snapshot vengono eliminate automaticamente in spazio libero quando una scrittura su un volume non riesce a causa della mancanza di spazio nell'aggregato.

  - Quote

    Specifica se le quote sono attivate per il volume.

- **Efficienza**
  - Compressione

    Specifica se la compressione è attivata o disattivata.

  - Deduplica

    Specifica se la deduplica è attivata o disattivata.

  - Modalità di deduplica

    Specifica se l'operazione di deduplica abilitata su un volume è un'operazione manuale, pianificata o basata su policy. Se la modalità è impostata su pianificato, viene visualizzata la pianificazione delle operazioni e, se la modalità è impostata su un criterio, viene visualizzato il nome del criterio.

  - Tipo di deduplica

    Specifica il tipo di operazione di deduplica in esecuzione sul volume. Se il volume si trova in una relazione SnapVault, il tipo visualizzato è SnapVault. Per qualsiasi altro volume, il tipo viene visualizzato come normale.

◦ Policy di efficienza dello storage

Specifica il nome del criterio di efficienza dello storage assegnato tramite Unified Manager a questo volume. Questo criterio può controllare le impostazioni di compressione e deduplica.

- **Protezione**
  ◦ Copie Snapshot

  Specifica se le copie Snapshot automatiche sono attivate o disattivate.

Scheda Protection (protezione)

La scheda protezione visualizza i dettagli di protezione relativi al volume selezionato, ad esempio informazioni sul ritardo, tipo di relazione e topologia della relazione.

- **Riepilogo**

  Visualizza le proprietà delle relazioni di protezione (SnapMirror, SnapVault o Storage VM DR) per un volume selezionato. Per qualsiasi altro tipo di relazione, viene visualizzata solo la proprietà tipo di relazione. Se si seleziona un volume primario, vengono visualizzati solo i criteri di copia Snapshot locale e gestito. Le proprietà visualizzate per le relazioni SnapMirror e SnapVault includono:

  ◦ Volume di origine

  Visualizza il nome dell'origine del volume selezionato se il volume selezionato è una destinazione.

  ◦ Stato di ritardo

  Visualizza lo stato di ritardo di aggiornamento o trasferimento per una relazione di protezione. Lo stato può essere Error (errore), Warning (Avviso) o Critical (critico).

  Lo stato di ritardo non è applicabile per le relazioni sincrone.

  ◦ Durata del ritardo

  Visualizza l'intervallo di tempo in cui i dati sul mirror si trovano indietro rispetto all'origine.

  ◦ Ultimo aggiornamento riuscito

  Visualizza la data e l'ora dell'aggiornamento della protezione più recente.

  L'ultimo aggiornamento riuscito non è applicabile per le relazioni sincrone.

  ◦ Membro del servizio di storage

  Visualizza Sì o No per indicare se il volume appartiene o meno a ed è gestito da un servizio di storage.

  ◦ Replica flessibile della versione

  Visualizza Sì, Sì con opzione di backup o Nessuno. Sì indica che la replica di SnapMirror è possibile anche se i volumi di origine e di destinazione eseguono versioni diverse del software ONTAP. Sì con opzione di backup indica l'implementazione della protezione SnapMirror con la possibilità di conservare più versioni delle copie di backup sulla destinazione. Nessuno indica che la replica flessibile della versione non è attivata.

- Funzionalità di relazione

  Indica le funzionalità di ONTAP disponibili per la relazione di protezione.

- Servizio di protezione

  Visualizza il nome del servizio di protezione se la relazione è gestita da un'applicazione del partner di protezione.

- Tipo di relazione

  Visualizza qualsiasi tipo di relazione, inclusi Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync, E Sync.

- Stato di relazione

  Visualizza lo stato della relazione SnapMirror o SnapVault. Lo stato può essere non inizializzato, SnapMirrored o interrotto. Se si seleziona un volume di origine, lo stato di relazione non è applicabile e non viene visualizzato.

- Transfer Status (Stato trasferimento)

  Visualizza lo stato di trasferimento per la relazione di protezione. Lo stato del trasferimento può essere uno dei seguenti:

  - Interruzione

    I trasferimenti SnapMirror sono attivati; tuttavia, è in corso un'operazione di interruzione del trasferimento che potrebbe includere la rimozione del checkpoint.

  - Verifica in corso

    Il volume di destinazione è sottoposto a un controllo diagnostico e non è in corso alcun trasferimento.

  - Finalizzazione

    I trasferimenti SnapMirror sono attivati. Il volume è attualmente in fase di post-trasferimento per i trasferimenti incrementali SnapVault.

  - Inattivo

    I trasferimenti sono attivati e non è in corso alcun trasferimento.

  - In-Sync

    I dati nei due volumi nella relazione sincrona vengono sincronizzati.

  - Out-of-Sync

    I dati nel volume di destinazione non vengono sincronizzati con il volume di origine.

  - Preparazione in corso

    I trasferimenti SnapMirror sono attivati. Il volume è attualmente in fase di pre-trasferimento per i trasferimenti incrementali SnapVault.

- In coda

  I trasferimenti SnapMirror sono attivati. Nessun trasferimento in corso.

- A Quiesced

  I trasferimenti SnapMirror sono disattivati. Nessun trasferimento in corso.

- Quiescing

  È in corso un trasferimento SnapMirror. I trasferimenti aggiuntivi sono disattivati.

- Trasferimento in corso

  I trasferimenti SnapMirror sono attivati e il trasferimento è in corso.

- In transizione

  Il trasferimento asincrono dei dati dal volume di origine al volume di destinazione è completo e la transizione all'operazione sincrona è iniziata.

- In attesa

  È stato avviato un trasferimento SnapMirror, ma alcune attività associate sono in attesa di essere accodate.

◦ Velocità di trasferimento massima

Visualizza la velocità di trasferimento massima per la relazione. La velocità di trasferimento massima può essere un valore numerico in kilobyte per secondo (Kbps), Megabyte per secondo (Mbps), Gigabyte per secondo (Gbps) o terabyte per secondo (Tbps). Se viene visualizzato No Limit (Nessun limite), il trasferimento della linea di base tra le relazioni è illimitato.

◦ Policy di SnapMirror

Visualizza il criterio di protezione per il volume. DPDefault indica il criterio di protezione predefinito di Asynchronous Mirror, XDPDefault indica il criterio predefinito di Asynchronous Vault e DPSyncDefault indica il criterio predefinito di Asynchronous MirrorVault. StrictSync indica il criterio di protezione Synchronous Strict predefinito, mentre Sync indica il criterio Synchronous predefinito. È possibile fare clic sul nome del criterio per visualizzare i dettagli associati a tale criterio, incluse le seguenti informazioni:

- Priorità di trasferimento
- Ignorare l'impostazione del tempo di accesso
- Limite di tentativi
- Commenti
- Etichette SnapMirror
- Impostazioni di conservazione
- Copie Snapshot effettive
- Conservare le copie Snapshot
- Soglia di avviso di conservazione

        - Copie Snapshot senza impostazioni di conservazione in una relazione SnapVault a cascata in cui l'origine è un volume di protezione dei dati (DP), si applica solo la regola "sm_created".
    - Aggiorna pianificazione

      Visualizza la pianificazione di SnapMirror assegnata alla relazione. Posizionando il cursore sull'icona delle informazioni vengono visualizzati i dettagli del programma.

    - Policy Snapshot locale

      Visualizza il criterio di copia Snapshot per il volume. Il criterio è predefinito, Nessuno o qualsiasi nome assegnato a un criterio personalizzato.

    - Protetto da

      Visualizza il tipo di protezione utilizzato per il volume selezionato. Ad esempio, se un volume è protetto dalle relazioni tra i volumi di Consistency Group e SnapMirror, in questo campo vengono visualizzati sia SnapMirror che Consistency Group. Questo campo fornisce anche un link che reindirizza l'utente alla pagina Relazioni per visualizzare lo stato di relazione unificata. Il link è applicabile solo alle relazioni costitutive.

    - Gruppo di coerenza

      Per i volumi protetti dalle relazioni di business continuity SnapMirror (SM-BC), in questa colonna viene visualizzato il gruppo di coerenza del volume.

- **Viste**

  Visualizza la topologia di protezione del volume selezionato. La topologia include rappresentazioni grafiche di tutti i volumi correlati al volume selezionato. Il volume selezionato è indicato da un bordo grigio scuro e le linee tra i volumi nella topologia indicano il tipo di relazione di protezione. La direzione delle relazioni nella topologia viene visualizzata da sinistra a destra, con l'origine di ciascuna relazione a sinistra e la destinazione a destra.

  Le linee doppie in grassetto specificano una relazione di mirror asincrono, una singola linea in grassetto specifica una relazione di vault asincrono, le doppie linee singole specificano una relazione di MirrorVault asincrono e una linea in grassetto e non in grassetto specifica una relazione sincrona. La tabella seguente indica se la relazione sincrona è StrictSync o Sync.

  Facendo clic con il pulsante destro del mouse su un volume viene visualizzato un menu dal quale è possibile scegliere se proteggere il volume o ripristinarne i dati. Facendo clic con il pulsante destro del mouse su una relazione viene visualizzato un menu dal quale è possibile scegliere di modificare, interrompere, interrompere, interrompere, rimuovere, o riprendere una relazione.

  I menu non vengono visualizzati nei seguenti casi:

    - Se le impostazioni RBAC non consentono questa azione, ad esempio, se si dispone solo di privilegi operatore
    - Se il volume si trova in una relazione di protezione sincrona
    - Quando l'ID del volume è sconosciuto, ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato, facendo clic su un altro volume nella topologia si selezionano e vengono visualizzate le informazioni relative a tale volume. Un punto interrogativo ( ) nell'angolo in alto a sinistra di un volume indica che il volume è mancante o che non è stato ancora rilevato. Potrebbe anche indicare che mancano le informazioni sulla capacità. Posizionando il cursore sul punto interrogativo vengono visualizzate ulteriori informazioni, tra cui suggerimenti per l'azione

correttiva.

La topologia visualizza le informazioni relative alla capacità del volume, al ritardo, alle copie Snapshot e all'ultimo trasferimento dei dati riuscito, se conforme a uno dei diversi modelli di topologia comuni. Se una topologia non è conforme a uno di questi modelli, le informazioni sul ritardo del volume e sull'ultimo trasferimento dei dati riuscito vengono visualizzate in una tabella di relazioni sotto la topologia. In tal caso, la riga evidenziata nella tabella indica il volume selezionato e, nella vista della topologia, le linee in grassetto con un punto blu indicano la relazione tra il volume selezionato e il volume di origine.

Le viste della topologia includono le seguenti informazioni:

- Capacità

  Visualizza la quantità totale di capacità utilizzata dal volume. Posizionando il cursore su un volume nella topologia, vengono visualizzate le impostazioni correnti di avviso e soglia critica per quel volume nella finestra di dialogo Current Threshold Settings (Impostazioni soglia correnti). È inoltre possibile modificare le impostazioni delle soglie facendo clic sul collegamento **Edit thresholds** (Modifica soglie) nella finestra di dialogo Current Threshold Settings (Impostazioni soglie correnti). Deselezionando la casella di controllo **capacità** vengono nascoste tutte le informazioni sulla capacità per tutti i volumi della topologia.

- Ritardo

  Visualizza la durata del ritardo e lo stato di ritardo delle relazioni di protezione in entrata. Deselezionando la casella di controllo **Lag** vengono nascoste tutte le informazioni di ritardo per tutti i volumi della topologia. Quando la casella di controllo **Lag** è disattivata, le informazioni sul ritardo per il volume selezionato vengono visualizzate nella tabella delle relazioni sotto la topologia, oltre alle informazioni sul ritardo per tutti i volumi correlati.

- Snapshot

  Visualizza il numero di copie Snapshot disponibili per un volume. Deselezionando la casella di controllo **Snapshot** vengono nascoste tutte le informazioni di copia Snapshot per tutti i volumi nella topologia. Fare clic sull'icona di una copia Snapshot ( ) Visualizza l'elenco di copie Snapshot di un volume. Il conteggio delle copie Snapshot visualizzato accanto all'icona viene aggiornato circa ogni ora; tuttavia, l'elenco delle copie Snapshot viene aggiornato al momento in cui si fa clic sull'icona. Ciò potrebbe determinare una differenza tra il numero di copie Snapshot visualizzate nella topologia e il numero di copie Snapshot elencate quando si fa clic sull'icona.

- Ultimo trasferimento riuscito

  Visualizza la quantità, la durata, l'ora e la data dell'ultimo trasferimento di dati riuscito. Quando la casella di controllo **Last Successful Transfer** (ultimo trasferimento riuscito) è disattivata, nella tabella delle relazioni sotto la topologia vengono visualizzate le informazioni sull'ultimo trasferimento riuscito per tutti i volumi correlati.

  - **Storia**

    Visualizza in un grafico la cronologia delle relazioni di protezione SnapMirror e SnapVault in entrata per il volume selezionato. Sono disponibili tre grafici cronologici: Durata del ritardo della relazione in entrata, durata del trasferimento della relazione in entrata e dimensione del trasferimento della relazione in entrata. Le informazioni sulla cronologia vengono visualizzate solo quando si seleziona un volume di destinazione. Se si seleziona un volume primario, i grafici sono vuoti e viene visualizzato il messaggio Nessun dato trovato. Se i volumi sono protetti dalle relazioni sincrone di Consistency Group e SnapMirror, le informazioni relative alla durata del trasferimento delle relazioni e alle dimensioni del trasferimento delle relazioni non vengono visualizzate.

È possibile selezionare un tipo di grafico dall'elenco a discesa nella parte superiore del riquadro Cronologia. È inoltre possibile visualizzare i dettagli di un periodo di tempo specifico selezionando 1 settimana, 1 mese o 1 anno. I grafici cronologici consentono di identificare le tendenze: Ad esempio, se si trasferiscono grandi quantità di dati alla stessa ora del giorno o della settimana, o se la soglia di errore di ritardo o di avviso viene costantemente violata, è possibile intraprendere l'azione appropriata. Inoltre, è possibile fare clic sul pulsante **Esporta** per creare un report in formato CSV per il grafico visualizzato.

I grafici della cronologia della protezione visualizzano le seguenti informazioni:

- **Durata ritardo relazione**

  Visualizza i secondi, i minuti o le ore sull'asse verticale (y) e i giorni, i mesi o gli anni sull'asse orizzontale (x), a seconda del periodo di tempo selezionato. Il valore superiore sull'asse y indica la durata massima del ritardo raggiunta nel periodo di durata mostrato sull'asse x. La linea arancione orizzontale sul grafico mostra la soglia di errore del ritardo, mentre la linea gialla orizzontale mostra la soglia di avviso del ritardo. Posizionando il cursore su queste righe viene visualizzata l'impostazione della soglia. La linea blu orizzontale indica la durata del ritardo. È possibile visualizzare i dettagli relativi a punti specifici del grafico posizionando il cursore su un'area di interesse.

- **Durata trasferimento relazione**

  Visualizza i secondi, i minuti o le ore sull'asse verticale (y) e i giorni, i mesi o gli anni sull'asse orizzontale (x), a seconda del periodo di tempo selezionato. Il valore superiore sull'asse y indica la durata massima del trasferimento raggiunta nel periodo di durata indicato sull'asse x. È possibile visualizzare i dettagli di punti specifici sul grafico posizionando il cursore sull'area di interesse.

  Questo grafico non è disponibile per i volumi che si trovano in relazioni di protezione sincrone.

- **Dimensione relazione trasferita**

  Visualizza byte, kilobyte, megabyte e così via sull'asse verticale (y) a seconda delle dimensioni del trasferimento e visualizza giorni, mesi o anni sull'asse orizzontale (x) a seconda del periodo di tempo selezionato. Il valore superiore sull'asse y indica la dimensione massima di trasferimento raggiunta nel periodo di durata indicato sull'asse x. È possibile visualizzare i dettagli relativi a punti specifici del grafico posizionando il cursore su un'area di interesse.

  Questo grafico non è disponibile per i volumi che si trovano in relazioni di protezione sincrone.

Area della storia

L'area History (Cronologia) visualizza i grafici che forniscono informazioni sulla capacità e sulle riserve di spazio del volume selezionato. Inoltre, è possibile fare clic sul pulsante **Esporta** per creare un report in formato CSV per il grafico visualizzato.

I grafici potrebbero essere vuoti e il messaggio Nessun dato trovato viene visualizzato quando i dati o lo stato del volume rimangono invariati per un certo periodo di tempo.

È possibile selezionare un tipo di grafico dall'elenco a discesa nella parte superiore del riquadro Cronologia. È inoltre possibile visualizzare i dettagli di un periodo di tempo specifico selezionando 1 settimana, 1 mese o 1 anno. I grafici cronologici consentono di identificare le tendenze, ad esempio, se l'utilizzo del volume supera costantemente la soglia quasi completa, è possibile intraprendere l'azione appropriata.

I grafici storici visualizzano le seguenti informazioni:

- **Capacità volume utilizzata**

  Visualizza la capacità utilizzata nel volume e l'andamento dell'utilizzo della capacità del volume in base alla cronologia di utilizzo, come grafici a linee in byte, kilobyte, megabyte e così via, sull'asse verticale (y). Il periodo di tempo viene visualizzato sull'asse orizzontale (x). È possibile selezionare un periodo di tempo di una settimana, un mese o un anno. È possibile visualizzare i dettagli di punti specifici del grafico posizionando il cursore su un'area specifica. È possibile nascondere o visualizzare un grafico a linee facendo clic sulla legenda appropriata. Ad esempio, quando si fa clic sulla legenda Volume used Capacity (capacità utilizzata volume), la riga del grafico Volume used Capacity (capacità utilizzata volume) viene nascosta.

- **Volume Capacity used vs Total** (capacità volume utilizzata vs totale)

  Visualizza l'andamento dell'utilizzo della capacità del volume in base alla cronologia di utilizzo, nonché la capacità utilizzata, la capacità totale e i dettagli dei risparmi di spazio derivanti dalla deduplica e dalla compressione, come grafici a linee, in byte, kilobyte, megabyte, e così via, sull'asse verticale (y). Il periodo di tempo viene visualizzato sull'asse orizzontale (x). È possibile selezionare un periodo di tempo di una settimana, un mese o un anno. È possibile visualizzare i dettagli di punti specifici del grafico posizionando il cursore su un'area specifica. È possibile nascondere o visualizzare un grafico a linee facendo clic sulla legenda appropriata. Ad esempio, quando si fa clic sulla legenda capacità di tendenza utilizzata, la linea del grafico capacità di tendenza utilizzata viene nascosta.

- **Capacità del volume utilizzata (%)**

  Visualizza la capacità utilizzata nel volume e l'andamento dell'utilizzo della capacità del volume in base alla cronologia di utilizzo, sotto forma di grafici a linee, in percentuale, sull'asse verticale (y). Il periodo di tempo viene visualizzato sull'asse orizzontale (x). È possibile selezionare un periodo di tempo di una settimana, un mese o un anno. È possibile visualizzare i dettagli di punti specifici del grafico posizionando il cursore su un'area specifica. È possibile nascondere o visualizzare un grafico a linee facendo clic sulla legenda appropriata. Ad esempio, quando si fa clic sulla legenda Volume used Capacity (capacità utilizzata volume), la riga del grafico Volume used Capacity (capacità utilizzata volume) viene nascosta.

- **Capacità Snapshot utilizzata (%)**

  Visualizza la soglia di avviso Snapshot Reserve e Snapshot come grafici a linee e la capacità utilizzata dalle copie Snapshot come grafico dell'area, in percentuale, sull'asse verticale (y). L'overflow dell'istantanea viene rappresentato con colori diversi. Il periodo di tempo viene visualizzato sull'asse orizzontale (x). È possibile selezionare un periodo di tempo di una settimana, un mese o un anno. È possibile visualizzare i dettagli di punti specifici del grafico posizionando il cursore su un'area specifica. È possibile nascondere o visualizzare un grafico a linee facendo clic sulla legenda appropriata. Ad esempio, quando si fa clic sulla legenda Snapshot Reserve, la linea del grafico Snapshot Reserve viene nascosta.

Elenco degli eventi

L'elenco Eventi visualizza i dettagli relativi agli eventi nuovi e riconosciuti:

- **Severità**

  Visualizza la severità dell'evento.

- **Evento**

  Visualizza il nome dell'evento.

- **Tempo di attivazione**

  Visualizza il tempo trascorso da quando è stato generato l'evento. Se il tempo trascorso supera una settimana, viene visualizzata l'indicazione dell'ora in cui è stato generato l'evento.

Riquadro delle annotazioni correlate

Il riquadro Annotazioni correlate consente di visualizzare i dettagli delle annotazioni associate al volume selezionato. I dettagli includono il nome dell'annotazione e i valori dell'annotazione applicati al volume. È inoltre possibile rimuovere le annotazioni manuali dal pannello Annotazioni correlate.

Pannello Related Devices (dispositivi correlati)

Il pannello Related Devices (dispositivi correlati) consente di visualizzare e accedere alle copie SVM, aggregati, qtree, LUN e Snapshot correlate al volume:

- **Storage Virtual Machine**

  Visualizza la capacità e lo stato di salute della SVM che contiene il volume selezionato.

- **Aggregato**

  Visualizza la capacità e lo stato di salute dell'aggregato che contiene il volume selezionato. Per i volumi FlexGroup, viene indicato il numero di aggregati che compongono il FlexGroup.

- **Volumi nell'aggregato**

  Visualizza il numero e la capacità di tutti i volumi che appartengono all'aggregato principale del volume selezionato. Viene inoltre visualizzato lo stato di salute dei volumi, in base al livello di gravità più elevato. Ad esempio, se un aggregato contiene dieci volumi, cinque dei quali visualizzano lo stato Avviso e gli altri cinque visualizzano lo stato critico, lo stato visualizzato è critico. Questo componente non viene visualizzato per i volumi FlexGroup.

- **Qtree**

  Visualizza il numero di qtree contenuti nel volume selezionato e la capacità dei qtree con quota contenuta nel volume selezionato. La capacità dei qtree con quota viene visualizzata in relazione alla capacità dei dati del volume. Viene visualizzato anche lo stato di salute dei qtree, in base al livello di severità più elevato. Ad esempio, se un volume ha dieci qtree, cinque con stato di avviso e i rimanenti cinque con stato critico, lo stato visualizzato è critico.

- **Condivisioni NFS**

  Visualizza il numero e lo stato delle condivisioni NFS associate al volume.

- **Condivisioni SMB**

  Visualizza il numero e lo stato delle condivisioni SMB/CIFS.

- **LUN**

  Visualizza il numero e le dimensioni totali di tutti i LUN nel volume selezionato. Viene inoltre visualizzato lo stato di salute delle LUN, in base al livello di gravità più elevato.

- **Quote utente e gruppo**

Visualizza il numero e lo stato delle quote utente e del gruppo di utenti associate al volume e ai relativi qtree.

- **Volumi FlexClone**

  Visualizza il numero e la capacità di tutti i volumi clonati del volume selezionato. Il numero e la capacità vengono visualizzati solo se il volume selezionato contiene volumi clonati.

- **Volume principale**

  Visualizza il nome e la capacità del volume principale di un volume FlexClone selezionato. Il volume padre viene visualizzato solo se il volume selezionato è un volume FlexClone.

Pannello gruppi correlati

Il riquadro Related Groups (gruppi correlati) consente di visualizzare l'elenco dei gruppi associati al volume selezionato.

Pannello Avvisi correlati

Il riquadro Related Alerts (Avvisi correlati) consente di visualizzare l'elenco degli avvisi creati per il volume selezionato. È inoltre possibile aggiungere un avviso facendo clic sul collegamento Add Alert (Aggiungi avviso) o modificarne uno esistente facendo clic sul nome dell'avviso.

Pagina Storage VM / Health Details

È possibile utilizzare la pagina Storage VM / Health Details per visualizzare informazioni dettagliate sulla VM di storage selezionata, come ad esempio lo stato, la capacità, la configurazione, le policy dei dati, le interfacce logiche (LIF), LUN, qtree, utente, quote gruppo utenti e dettagli di protezione . È inoltre possibile visualizzare informazioni sugli oggetti correlati e sugli avvisi correlati per la VM di storage.

È possibile monitorare solo le macchine virtuali per lo storage dei dati.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività per la VM di storage selezionata:

- **Passa alla visualizzazione delle performance**

  Consente di accedere alla pagina Storage VM / Performance Details.

- **Azioni**
  - Aggiungi avviso

    Consente di aggiungere un avviso alla VM di storage selezionata.

  - Annotare

    Consente di annotare la VM di storage selezionata.

- **Visualizza le VM di storage**

Consente di passare alla vista Health: All Storage VM (Salute: Tutte le macchine virtuali dello storage).

Scheda Health (Salute)

La scheda Health (Stato) visualizza informazioni dettagliate sulla disponibilità dei dati, la capacità dei dati e i problemi di protezione di vari oggetti, ad esempio volumi, aggregati, LIF NAS, LIF SAN, LUN, Protocolli, servizi, condivisioni NFS e condivisioni CIFS.

È possibile fare clic sul grafico di un oggetto per visualizzare l'elenco filtrato di oggetti. Ad esempio, è possibile fare clic sul grafico della capacità del volume che visualizza gli avvisi per visualizzare l'elenco dei volumi che presentano problemi di capacità con severità come avviso.

- **Problemi di disponibilità**

  Visualizza, sotto forma di grafico, il numero totale di oggetti, inclusi gli oggetti che presentano problemi di disponibilità e gli oggetti che non presentano problemi di disponibilità. I colori nel grafico rappresentano i diversi livelli di gravità dei problemi. Le informazioni sotto il grafico forniscono dettagli sui problemi di disponibilità che possono avere un impatto o hanno già influito sulla disponibilità dei dati nella VM di storage. Ad esempio, vengono visualizzate informazioni sui LIF NAS e SAN inattivi e sui volumi offline.

  È inoltre possibile visualizzare informazioni sui protocolli e sui servizi correlati attualmente in esecuzione, nonché sul numero e lo stato delle condivisioni NFS e CIFS.

- **Problemi di capacità**

  Visualizza, sotto forma di grafico, il numero totale di oggetti, inclusi quelli che presentano problemi di capacità e quelli che non presentano problemi di capacità. I colori nel grafico rappresentano i diversi livelli di gravità dei problemi. Le informazioni sotto il grafico forniscono dettagli sui problemi di capacità che possono avere un impatto o hanno già influito sulla capacità dei dati nella VM di storage. Ad esempio, vengono visualizzate informazioni sugli aggregati che potrebbero violare i valori di soglia impostati.

- **Problemi di protezione**

  Fornisce una rapida panoramica dello stato di salute relativo alla protezione delle macchine virtuali dello storage visualizzando, come finestra di dialogo sul campo, il numero totale di relazioni, incluse le relazioni che presentano problemi di protezione e le relazioni che non presentano problemi di protezione. È inoltre possibile visualizzare lo stato della relazione DR della VM di storage per la VM di storage selezionata. Gli eventi relativi alle relazioni DR delle macchine virtuali di storage vengono visualizzati qui e facendo clic sugli eventi si accede alla pagina dei dettagli dell'evento. Quando esistono volumi non protetti, facendo clic sul collegamento si passa alla vista Health: All Volumes (Salute: Tutti i volumi), in cui è possibile visualizzare un elenco filtrato dei volumi non protetti sulla VM di storage. I colori nel grafico rappresentano i diversi livelli di gravità dei problemi. Facendo clic su un grafico si passa alla vista relazione: Tutte le relazioni, in cui è possibile visualizzare un elenco filtrato di dettagli delle relazioni di protezione. Le informazioni sotto il grafico forniscono dettagli sui problemi di protezione che possono avere un impatto o hanno già influito sulla protezione dei dati nella VM di storage. Ad esempio, vengono visualizzate informazioni sui volumi con una riserva di copia Snapshot quasi piena o su problemi di ritardo della relazione SnapMirror.

Scheda capacità

La scheda Capacity (capacità) visualizza informazioni dettagliate sulla capacità dei dati della SVM selezionata.

Per una Storage VM con volume FlexVol o volume FlexGroup vengono visualizzate le seguenti informazioni:

- **Capacità**

  L'area Capacity (capacità) visualizza i dettagli relativi alla capacità utilizzata e disponibile allocata da tutti i volumi:

  - Capacità totale

    Visualizza la capacità totale della Storage VM.

  - Utilizzato

    Visualizza lo spazio utilizzato dai dati nei volumi che appartengono alla Storage VM.

  - Disponibilità garantita

    Visualizza lo spazio disponibile garantito per i dati disponibili per i volumi nella Storage VM.

  - Non garantito

    Visualizza lo spazio rimanente per i dati allocati per volumi con thin provisioning nella Storage VM.

- **Volumi con problemi di capacità**

  L'elenco Volumes with Capacity isumes (volumi con problemi di capacità) visualizza, in formato tabulare, i dettagli sui volumi che presentano problemi di capacità:

  - Stato

    Indica che il volume presenta un problema relativo alla capacità con un livello di gravità indicato.

    È possibile spostare il puntatore sullo stato per visualizzare ulteriori informazioni sull'evento o sugli eventi relativi alla capacità generati per il volume.

    Se lo stato del volume è determinato da un singolo evento, è possibile visualizzare informazioni quali il nome dell'evento, l'ora e la data in cui è stato attivato l'evento, il nome dell'amministratore a cui è assegnato l'evento e la causa dell'evento. È possibile utilizzare il pulsante **Visualizza dettagli** per visualizzare ulteriori informazioni sull'evento.

    Se lo stato del volume è determinato da più eventi della stessa severità, vengono visualizzati i primi tre eventi con informazioni quali il nome dell'evento, l'ora e la data di attivazione degli eventi e il nome dell'amministratore a cui è assegnato l'evento. È possibile visualizzare ulteriori dettagli su ciascuno di questi eventi facendo clic sul nome dell'evento. È inoltre possibile fare clic sul collegamento **View All Events** (Visualizza tutti gli eventi) per visualizzare l'elenco degli eventi generati.

    > Un volume può avere più eventi con la stessa severità o con diverse severità. Tuttavia, viene visualizzato solo il livello di severità più elevato. Ad esempio, se un volume presenta due eventi con severità di errore e avviso, viene visualizzato solo il livello di gravità dell'errore.

  - Volume

    Visualizza il nome del volume.

  - Capacità dei dati utilizzati

Visualizza, sotto forma di grafico, informazioni sull'utilizzo della capacità del volume (in percentuale).

- Giorni al massimo

  Visualizza il numero stimato di giorni rimanenti prima che il volume raggiunga la capacità massima.

- Con thin provisioning

  Visualizza se la garanzia di spazio è impostata per il volume selezionato. I valori validi sono Sì e No

- Aggregati

  Per FlexVol Volumes (volumi totali), visualizza il nome dell'aggregato che contiene il volume. Per i volumi FlexGroup, Visualizza il numero di aggregati utilizzati in FlexGroup.

Scheda Configuration (Configurazione)

La scheda Configurazione visualizza i dettagli di configurazione relativi alla VM di storage selezionata, ad esempio il cluster, il volume root, il tipo di volumi in essa contenuti (volumi FlexVol), i criteri e la protezione creati sulla VM di storage:

- **Panoramica**
  - Cluster

    Visualizza il nome del cluster a cui appartiene la VM di storage.

  - Tipo di volume consentito

    Visualizza il tipo di volumi che è possibile creare nella VM di storage. Il tipo può essere FlexVol o FlexVol/FlexGroup.

  - Volume root

    Visualizza il nome del volume root della VM di storage.

  - Protocolli consentiti

    Visualizza il tipo di protocolli che è possibile configurare sulla VM di storage. Inoltre, indica se un protocollo è attivo (), giù (), o non è configurato ().

- **Interfacce di rete dati**
  - NAS

    Visualizza il numero di interfacce NAS associate alla VM di storage. Inoltre, indica se le interfacce sono in funzione () o verso il basso ().

  - SAN

    Visualizza il numero di interfacce SAN associate alla VM di storage. Inoltre, indica se le interfacce sono in funzione () o verso il basso ().

  - FC-NVMe

    Visualizza il numero di interfacce FC-NVMe associate a Storage VM. Inoltre, indica se le interfacce sono in funzione () o verso il basso ().

- **Interfacce di rete di gestione**
  - Disponibilità

    Visualizza il numero di interfacce di gestione associate a Storage VM. Inoltre, indica se le interfacce di gestione sono in funzione ( ) o verso il basso ( ).
- **Politiche**
  - Snapshot

    Visualizza il nome del criterio Snapshot creato sulla Storage VM.
  - Policy di esportazione

    Visualizza il nome del criterio di esportazione se viene creato un singolo criterio o il numero di criteri di esportazione se vengono creati più criteri.
- **Protezione**
  - Dr. VM storage

    Visualizza se la VM di storage selezionata è protetta, di destinazione o non protetta e il nome della destinazione in cui è protetta la VM di storage. Se la VM di storage selezionata è la destinazione, vengono visualizzati i dettagli della VM di storage di origine. In caso di fan-out, questo campo visualizza il numero totale di VM storage di destinazione su cui è protetta la VM di storage. Il collegamento count consente di accedere alla griglia di relazioni delle VM di storage filtrata sulla VM di storage di origine.
  - Volumi protetti

    Visualizza il numero di volumi protetti sulla VM di storage selezionata su un totale di volumi. Se si sta visualizzando una VM di storage di destinazione, il collegamento numerico è relativo ai volumi di destinazione della VM di storage selezionata.
  - Volumi non protetti

    Visualizza il numero di volumi non protetti sulla VM di storage selezionata.
- **Servizi**
  - Tipo

    Visualizza il tipo di servizio configurato sulla VM di storage. Il tipo può essere DNS (Domain Name System) o NIS (Network Information Service).
  - Stato

    Visualizza lo stato del servizio, che può essere su ( ), giù ( ), o non configurato ( ).
  - Domain Name (Nome dominio)

    Visualizza i nomi di dominio completi (FQDN) del server DNS per i servizi DNS o il server NIS per i servizi NIS. Quando il server NIS è attivato, viene visualizzato l'FQDN attivo del server NIS. Quando il server NIS è disattivato, viene visualizzato l'elenco di tutti gli FQDN.
  - Indirizzo IP

Visualizza gli indirizzi IP del server DNS o NIS. Quando il server NIS è attivato, viene visualizzato l'indirizzo IP attivo del server NIS. Quando il server NIS è disattivato, viene visualizzato l'elenco di tutti gli indirizzi IP.

Scheda Network Interfaces (interfacce di rete)

La scheda Network Interfaces (interfacce di rete) visualizza i dettagli relativi alle interfacce di rete dati (LIF) create sulla VM di storage selezionata:

- **Interfaccia di rete**

  Visualizza il nome dell'interfaccia creata sulla VM di storage selezionata.

- **Stato operativo**

  Visualizza lo stato operativo dell'interfaccia, che può essere su (), giù () O Sconosciuto (). Lo stato operativo di un'interfaccia è determinato dallo stato delle porte fisiche.

- **Stato amministrativo**

  Visualizza lo stato amministrativo dell'interfaccia, che può essere Up (), giù () O Sconosciuto (). Lo stato amministrativo di un'interfaccia è controllato dall'amministratore dello storage per apportare modifiche alla configurazione o per scopi di manutenzione. Lo stato amministrativo può essere diverso dallo stato operativo. Tuttavia, se lo stato amministrativo di un'interfaccia non è attivo, lo stato operativo è inattivo per impostazione predefinita.

- **Indirizzo IP / WWPN**

  Visualizza l'indirizzo IP per le interfacce Ethernet e il nome della porta universale (WWPN) per le LIF FC.

- **Protocolli**

  Visualizza l'elenco dei protocolli dati specificati per l'interfaccia, ad esempio CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe e FlexCache.

- **Ruolo**

  Visualizza il ruolo dell'interfaccia. I ruoli possono essere dati o gestione.

- **Porta home**

  Visualizza la porta fisica a cui è stata originariamente associata l'interfaccia.

- **Porta corrente**

  Visualizza la porta fisica a cui è attualmente associata l'interfaccia. Se l'interfaccia viene migrata, la porta corrente potrebbe essere diversa dalla porta home.

- **Set di porte**

  Visualizza il set di porte a cui è mappata l'interfaccia.

- **Policy di failover**

  Visualizza il criterio di failover configurato per l'interfaccia. Per le interfacce NFS, CIFS e FlexCache, il criterio di failover predefinito è Next Available (Avanti disponibile). La policy di failover non è applicabile alle

interfacce FC e iSCSI.

- **Routing Groups**

  Visualizza il nome del gruppo di routing. È possibile visualizzare ulteriori informazioni sui percorsi e sul gateway di destinazione facendo clic sul nome del gruppo di routing.

  I gruppi di routing non sono supportati per ONTAP 8.3 o versioni successive e pertanto viene visualizzata una colonna vuota per questi cluster.

- **Gruppo di failover**

  Visualizza il nome del gruppo di failover.

Scheda qtree

La scheda Qtree visualizza i dettagli relativi ai qtree e alle relative quote. È possibile fare clic sul pulsante **Edit thresholds** (Modifica soglie) se si desidera modificare le impostazioni della soglia di integrità per la capacità di qtree per uno o più qtree.

Utilizzare il pulsante **Export** per creare un file con valori separati da virgola (.csv) contenente i dettagli di tutti i qtree monitorati. Quando si esporta in un file CSV, è possibile scegliere di creare un report qtree per la VM di storage corrente, per tutte le VM di storage nel cluster corrente o per tutte le VM di storage per tutti i cluster del data center. Alcuni campi qtree aggiuntivi vengono visualizzati nel file CSV esportato.

- **Stato**

  Visualizza lo stato corrente del qtree. Lo stato può essere critico ( ), errore ( ), Avviso ( ), o normale ().

  È possibile spostare il puntatore sull'icona di stato per visualizzare ulteriori informazioni sull'evento o sugli eventi generati per il qtree.

  Se lo stato del qtree è determinato da un singolo evento, è possibile visualizzare informazioni quali il nome dell'evento, l'ora e la data in cui è stato attivato l'evento, il nome dell'amministratore a cui è assegnato l'evento e la causa dell'evento. È possibile utilizzare **Visualizza dettagli** per visualizzare ulteriori informazioni sull'evento.

  Se lo stato del qtree è determinato da più eventi della stessa severità, vengono visualizzati i primi tre eventi con informazioni quali il nome dell'evento, l'ora e la data in cui sono stati attivati gli eventi e il nome dell'amministratore a cui è assegnato l'evento. È possibile visualizzare ulteriori dettagli su ciascuno di questi eventi facendo clic sul nome dell'evento. È inoltre possibile utilizzare **View All Events** (Visualizza tutti gli eventi) per visualizzare l'elenco degli eventi generati.

  > Un qtree può avere più eventi con la stessa severità o con diverse severità. Tuttavia, viene visualizzato solo il livello di severità più elevato. Ad esempio, se un qtree ha due eventi con severità di errore e di avviso, viene visualizzato solo il livello di gravità dell'errore.

- **Qtree**

  Visualizza il nome del qtree.

- **Cluster**

  Visualizza il nome del cluster che contiene il qtree. Viene visualizzato solo nel file CSV esportato.

- **Storage Virtual Machine**

  Visualizza il nome della macchina virtuale di storage (SVM) che contiene il qtree. Viene visualizzato solo nel file CSV esportato.

- **Volume**

  Visualizza il nome del volume che contiene il qtree.

  È possibile spostare il puntatore sul nome del volume per visualizzare ulteriori informazioni sul volume.

- **Insieme di quote**

  Indica se una quota è attivata o disattivata nel qtree.

- **Tipo di quota**

  Specifica se la quota è per un utente, un gruppo di utenti o un qtree. Viene visualizzato solo nel file CSV esportato.

- **Utente o gruppo**

  Visualizza il nome dell'utente o del gruppo di utenti. Sono disponibili più righe per ciascun utente e gruppo di utenti. Quando il tipo di quota è qtree o se la quota non è impostata, la colonna è vuota. Viene visualizzato solo nel file CSV esportato.

- **Disco utilizzato %**

  Visualizza la percentuale di spazio su disco utilizzato. Se viene impostato un limite massimo di dischi, questo valore si basa sul limite massimo di dischi. Se la quota viene impostata senza un limite massimo di dischi, il valore si basa sullo spazio dei dati del volume. Se la quota non è impostata o se le quote sono disattivate sul volume a cui appartiene il qtree, nella pagina della griglia viene visualizzato "non applicabile" e il campo è vuoto nei dati di esportazione CSV.

- **Disco rigido**

  Visualizza la quantità massima di spazio su disco allocato per il qtree. Unified Manager genera un evento critico quando viene raggiunto questo limite e non sono consentite ulteriori scritture su disco. Il valore viene visualizzato come "Unlimited" per le seguenti condizioni: Se la quota è impostata senza un limite fisso del disco, se la quota non è impostata o se le quote sono disattivate sul volume a cui appartiene il qtree.

- **Disk Soft Limit**

  Visualizza la quantità di spazio su disco allocato per il qtree prima che venga generato un evento di avviso. Il valore viene visualizzato come "Unlimited" per le seguenti condizioni: Se la quota è impostata senza un limite di tolleranza del disco, se la quota non è impostata o se le quote sono disattivate sul volume a cui appartiene il qtree. Per impostazione predefinita, questa colonna è nascosta.

- **Disk Threshold**

  Visualizza il valore di soglia impostato sullo spazio su disco. Il valore viene visualizzato come "Unlimited" per le seguenti condizioni: Se la quota è impostata senza un limite di soglia del disco, se la quota non è impostata o se le quote sono disattivate sul volume a cui appartiene il qtree. Per impostazione predefinita, questa colonna è nascosta.

- **File utilizzati %**

  Visualizza la percentuale di file utilizzati nel qtree. Se viene impostato il limite massimo del file, questo valore si basa sul limite massimo del file. Se la quota è impostata senza un limite massimo di file, non viene visualizzato alcun valore. Se la quota non è impostata o se le quote sono disattivate sul volume a cui appartiene il qtree, nella pagina della griglia viene visualizzato “non applicabile” e il campo è vuoto nei dati di esportazione CSV.

- **Limite massimo del file**

  Visualizza il limite massimo per il numero di file consentiti sui qtree. Il valore viene visualizzato come “Unlimited” per le seguenti condizioni: Se la quota è impostata senza un limite massimo di file, se la quota non è impostata o se le quote sono disattivate sul volume a cui appartiene il qtree.

- **Limite di software del file**

  Visualizza il soft limit per il numero di file consentiti sui qtree. Il valore viene visualizzato come “Unlimited” per le seguenti condizioni: Se la quota è impostata senza un limite software del file, se la quota non è impostata o se le quote sono disattivate sul volume a cui appartiene il qtree. Per impostazione predefinita, questa colonna è nascosta.

Scheda quote utente e gruppo

Visualizza i dettagli relativi alle quote utente e del gruppo di utenti per la VM di storage selezionata. È possibile visualizzare informazioni quali lo stato della quota, il nome dell’utente o del gruppo di utenti, i limiti di volume e di spazio su disco e i file impostati, la quantità di spazio su disco e il numero di file utilizzati e il valore di soglia del disco. È inoltre possibile modificare l’indirizzo e-mail associato a un utente o a un gruppo di utenti.

- **Pulsante di comando Modifica indirizzo email**

  Apre la finestra di dialogo Modifica indirizzo e-mail, che visualizza l’indirizzo e-mail corrente dell’utente o del gruppo di utenti selezionato. È possibile modificare l’indirizzo e-mail. Se il campo **Modifica indirizzo e-mail** è vuoto, viene utilizzata la regola predefinita per generare un indirizzo e-mail per l’utente o il gruppo di utenti selezionato.

  Se più utenti hanno la stessa quota, i nomi degli utenti vengono visualizzati come valori separati da virgole. Inoltre, la regola predefinita non viene utilizzata per generare l’indirizzo e-mail; pertanto, è necessario fornire l’indirizzo e-mail richiesto per l’invio delle notifiche.

- **Pulsante di comando Configura regole e-mail**

  Consente di creare o modificare le regole per generare un indirizzo e-mail per le quote dell’utente o del gruppo di utenti configurate sulla VM di storage. Quando si verifica una violazione delle quote, viene inviata una notifica all’indirizzo e-mail specificato.

- **Stato**

  Visualizza lo stato corrente della quota. Lo stato può essere critico (), Avviso (), o normale ().

  È possibile spostare il puntatore sull’icona di stato per visualizzare ulteriori informazioni sull’evento o sugli eventi generati per la quota.

  Se lo stato della quota è determinato da un singolo evento, è possibile visualizzare informazioni quali il nome dell’evento, l’ora e la data in cui è stato attivato l’evento, il nome dell’amministratore a cui è assegnato l’evento e la causa dell’evento. È possibile utilizzare **Visualizza dettagli** per visualizzare

ulteriori informazioni sull'evento.

Se lo stato della quota è determinato da più eventi della stessa severità, vengono visualizzati i primi tre eventi con informazioni quali il nome dell'evento, l'ora e la data di attivazione degli eventi e il nome dell'amministratore a cui è assegnato l'evento. È possibile visualizzare ulteriori dettagli su ciascuno di questi eventi facendo clic sul nome dell'evento. È inoltre possibile utilizzare **View All Events** (Visualizza tutti gli eventi) per visualizzare l'elenco degli eventi generati.

Una quota può avere più eventi con la stessa severità o con diverse severità. Tuttavia, viene visualizzato solo il livello di severità più elevato. Ad esempio, se una quota ha due eventi con severità di errore e avviso, viene visualizzato solo il livello di gravità dell'errore.

- **Utente o gruppo**

  Visualizza il nome dell'utente o del gruppo di utenti. Se più utenti hanno la stessa quota, i nomi degli utenti vengono visualizzati come valori separati da virgole.

  Il valore viene visualizzato come "Sconosciuto" quando ONTAP non fornisce un nome utente valido a causa di errori SecD.

- **Tipo**

  Specifica se la quota è per un utente o un gruppo di utenti.

- **Volume o Qtree**

  Visualizza il nome del volume o del qtree in cui è specificata la quota dell'utente o del gruppo di utenti.

  È possibile spostare il puntatore sul nome del volume o del qtree per visualizzare ulteriori informazioni sul volume o sul qtree.

- **Disco utilizzato %**

  Visualizza la percentuale di spazio su disco utilizzato. Il valore viene visualizzato come "non applicabile" se la quota è impostata senza un limite massimo di dischi.

- **Disco rigido**

  Visualizza la quantità massima di spazio su disco allocato per la quota. Unified Manager genera un evento critico quando viene raggiunto questo limite e non sono consentite ulteriori scritture su disco. Il valore viene visualizzato come "Unlimited" se la quota è impostata senza un limite di disco rigido.

- **Disk Soft Limit**

  Visualizza la quantità di spazio su disco allocato per la quota prima che venga generato un evento di avviso. Il valore viene visualizzato come "Unlimited" se la quota è impostata senza un limite di tolleranza del disco. Per impostazione predefinita, questa colonna è nascosta.

- **Disk Threshold**

  Visualizza il valore di soglia impostato sullo spazio su disco. Il valore viene visualizzato come "Unlimited" se la quota è impostata senza un limite di soglia del disco. Per impostazione predefinita, questa colonna è nascosta.

- **File utilizzati %**

Visualizza la percentuale di file utilizzati nel qtree. Il valore viene visualizzato come “non applicabile” se la quota è impostata senza un limite massimo di file.

- **Limite massimo del file**

  Visualizza il limite massimo per il numero di file consentiti nella quota. Il valore viene visualizzato come “Unlimited” se la quota è impostata senza un limite massimo di file.

- **Limite di software del file**

  Visualizza il soft limit per il numero di file consentiti nella quota. Il valore viene visualizzato come “Unlimited” se la quota è impostata senza un limite software del file. Per impostazione predefinita, questa colonna è nascosta.

- **Indirizzo e-mail**

  Visualizza l’indirizzo e-mail dell’utente o del gruppo di utenti a cui vengono inviate le notifiche in caso di violazione delle quote.

Scheda condivisioni NFS

La scheda condivisioni NFS visualizza informazioni relative alle condivisioni NFS, ad esempio il relativo stato, il percorso associato al volume (volumi FlexGroup o volumi FlexVol), i livelli di accesso dei client alle condivisioni NFS e i criteri di esportazione definiti per i volumi esportati. Le condivisioni NFS non vengono visualizzate nelle seguenti condizioni: Se il volume non è montato o se i protocolli associati alla policy di esportazione per il volume non contengono condivisioni NFS.

- **Stato**

  Visualizza lo stato corrente delle condivisioni NFS. Lo stato può essere Error ( ) O normale ( ).

- **Percorso di giunzione**

  Visualizza il percorso in cui è montato il volume. Se a un qtree viene applicato un criterio di esportazione NFS esplicito, la colonna visualizza il percorso del volume attraverso il quale è possibile accedere al qtree.

- **Percorso di giunzione attivo**

  Visualizza se il percorso per accedere al volume montato è attivo o inattivo.

- **Volume o Qtree**

  Visualizza il nome del volume o del qtree a cui viene applicato il criterio di esportazione NFS. Se un criterio di esportazione NFS viene applicato a un qtree nel volume, la colonna visualizza sia i nomi del volume che il qtree.

  È possibile fare clic sul collegamento per visualizzare i dettagli relativi all’oggetto nella relativa pagina dei dettagli. Se l’oggetto è un qtree, vengono visualizzati i collegamenti sia per il qtree che per il volume.

- **Stato del volume**

  Visualizza lo stato del volume che si sta esportando. Lo stato può essere Offline, Online, Restricted o Mixed.

  - Offline

Non è consentito l'accesso in lettura o scrittura al volume.

- Online

  È consentito l'accesso in lettura e scrittura al volume.

- Limitato

  Sono consentite operazioni limitate, come la ricostruzione della parità, ma non è consentito l'accesso ai dati.

- Misto

  I componenti di un volume FlexGroup non si trovano tutti nello stesso stato.

- **Stile di sicurezza**

  Visualizza l'autorizzazione di accesso per i volumi esportati. Lo stile di sicurezza può essere UNIX, Unified, NTFS o Mixed.

  - UNIX (client NFS)

    I file e le directory del volume dispongono delle autorizzazioni UNIX.

  - Unificato

    I file e le directory del volume hanno uno stile di sicurezza unificato.

  - NTFS (client CIFS)

    I file e le directory del volume dispongono delle autorizzazioni NTFS di Windows.

  - Misto

    I file e le directory del volume possono disporre di autorizzazioni UNIX o NTFS di Windows.

- **Autorizzazione UNIX**

  Visualizza i bit di autorizzazione UNIX in un formato di stringa ottale, impostato per i volumi esportati. È simile ai bit di permesso di stile UNIX.

- **Politica di esportazione**

  Visualizza le regole che definiscono l'autorizzazione di accesso per i volumi esportati. È possibile fare clic sul collegamento per visualizzare i dettagli sulle regole associate ai criteri di esportazione, ad esempio i protocolli di autenticazione e l'autorizzazione di accesso.

Scheda SMB Shares (condivisioni SMB

Visualizza le informazioni sulle condivisioni SMB sulla VM di storage selezionata. È possibile visualizzare informazioni quali lo stato della condivisione SMB, il nome della condivisione, il percorso associato alla VM di storage, lo stato del percorso di giunzione della condivisione, l'oggetto contenente, lo stato del volume contenente, i dati di sicurezza della condivisione e i criteri di esportazione definiti per la condivisione. È inoltre possibile determinare se esiste un percorso NFS equivalente per la condivisione SMB.

Le condivisioni nelle cartelle non vengono visualizzate nella scheda condivisioni SMB.

- **Pulsante di comando View User Mapping (Visualizza mappatura utente)**

  Apre la finestra di dialogo User Mapping (mappatura utente).

  È possibile visualizzare i dettagli della mappatura utente per la VM di storage.

- **Mostra pulsante di comando ACL**

  Apre la finestra di dialogo Access Control per la condivisione.

  È possibile visualizzare i dettagli dell'utente e delle autorizzazioni per la condivisione selezionata.

- **Stato**

  Visualizza lo stato corrente della condivisione. Lo stato può essere normale ( ) O Error ( ).

- **Nome condivisione**

  Visualizza il nome della condivisione SMB.

- **Percorso**

  Visualizza il percorso di giunzione in cui viene creata la condivisione.

- **Percorso di giunzione attivo**

  Visualizza se il percorso di accesso alla condivisione è attivo o inattivo.

- **Oggetto contenente**

  Visualizza il nome dell'oggetto contenente a cui appartiene la condivisione. L'oggetto contenente può essere un volume o un qtree.

  Facendo clic sul collegamento, è possibile visualizzare i dettagli sull'oggetto contenente nella relativa pagina Dettagli. Se l'oggetto contenente è un qtree, vengono visualizzati i collegamenti per qtree e volume.

- **Stato del volume**

  Visualizza lo stato del volume che si sta esportando. Lo stato può essere Offline, Online, Restricted o Mixed.

  - Offline

    Non è consentito l'accesso in lettura o scrittura al volume.

  - Online

    È consentito l'accesso in lettura e scrittura al volume.

  - Limitato

    Sono consentite operazioni limitate, come la ricostruzione della parità, ma non è consentito l'accesso ai dati.

◦ Misto

I componenti di un volume FlexGroup non si trovano tutti nello stesso stato.

- **Sicurezza**

  Visualizza l'autorizzazione di accesso per i volumi esportati. Lo stile di sicurezza può essere UNIX, Unified, NTFS o Mixed.

  ◦ UNIX (client NFS)

  I file e le directory del volume dispongono delle autorizzazioni UNIX.

  ◦ Unificato

  I file e le directory del volume hanno uno stile di sicurezza unificato.

  ◦ NTFS (client CIFS)

  I file e le directory del volume dispongono delle autorizzazioni NTFS di Windows.

  ◦ Misto

  I file e le directory del volume possono disporre di autorizzazioni UNIX o NTFS di Windows.

- **Politica di esportazione**

  Visualizza il nome della policy di esportazione applicabile alla condivisione. Se non viene specificato un criterio di esportazione per la VM di storage, il valore viene visualizzato come non abilitato.

  È possibile fare clic sul collegamento per visualizzare i dettagli sulle regole associate ai criteri di esportazione, ad esempio i protocolli di accesso e le autorizzazioni. Il collegamento è disattivato se il criterio di esportazione è disattivato per la VM di storage selezionata.

- **Equivalente NFS**

  Specifica se esiste un equivalente NFS per la condivisione.

Scheda SAN

Visualizza i dettagli relativi a LUN, gruppi di iniziatori e iniziatori per la VM di storage selezionata. Per impostazione predefinita, viene visualizzata la vista LUN. È possibile visualizzare i dettagli relativi ai gruppi iniziatori nella scheda Initiator Groups (gruppi iniziatori) e i dettagli sugli iniziatori nella scheda Initiator (iniziatori).

- Scheda **LUN**

  Visualizza i dettagli relativi ai LUN che appartengono alla VM di storage selezionata. È possibile visualizzare informazioni quali il nome del LUN, lo stato del LUN (online o offline), il nome del file system (volume o qtree) che contiene il LUN, il tipo di sistema operativo host, la capacità totale dei dati e il numero di serie del LUN. La colonna LUN Performance (prestazioni LUN) fornisce un collegamento alla pagina LUN/Performance Details (Dettagli LUN/prestazioni).

  È inoltre possibile visualizzare informazioni sull'attivazione del thin provisioning sul LUN e sul mapping del LUN a un gruppo iniziatore. Se è mappato a un iniziatore, è possibile visualizzare i gruppi e gli iniziatori

iniziatori che sono mappati al LUN selezionato.

- Scheda **Initiator Groups**

  Visualizza i dettagli sui gruppi di iniziatori. È possibile visualizzare dettagli quali il nome del gruppo iniziatore, lo stato di accesso, il tipo di sistema operativo host utilizzato da tutti gli iniziatori del gruppo e il protocollo supportato. Facendo clic sul collegamento nella colonna Access state (Stato di accesso), è possibile visualizzare lo stato di accesso corrente del gruppo Initiator.

  - **Normale**

    Il gruppo iniziatore è connesso a più percorsi di accesso.

  - **Percorso singolo**

    Il gruppo iniziatore è connesso a un singolo percorso di accesso.

  - **Nessun percorso**

    Nessun percorso di accesso connesso al gruppo iniziatore.

    È possibile visualizzare se i gruppi di iniziatori sono mappati a tutte le interfacce o a interfacce specifiche attraverso un set di porte. Quando si fa clic sul collegamento count nella colonna mapped interfaces (interfacce mappate), vengono visualizzate tutte le interfacce o interfacce specifiche per un set di porte. Le interfacce mappate attraverso il portale di destinazione non vengono visualizzate. Viene visualizzato il numero totale di iniziatori e LUN mappati a un gruppo di iniziatori.

  È inoltre possibile visualizzare i LUN e gli iniziatori mappati al gruppo iniziatore selezionato.

- Scheda **Initiator**

  Visualizza il nome e il tipo dell'iniziatore e il numero totale di gruppi di iniziatori mappati a questo iniziatore per la VM di storage selezionata.

```
initiator groups that are mapped to the selected initiator group.
```

Riquadro delle annotazioni correlate

Il riquadro Annotazioni correlate consente di visualizzare i dettagli delle annotazioni associati alla VM di storage selezionata. I dettagli includono il nome dell'annotazione e i valori dell'annotazione applicati alla VM di storage. È inoltre possibile rimuovere le annotazioni manuali dal pannello Annotazioni correlate.

Pannello Related Devices (dispositivi correlati)

Il pannello Related Devices (dispositivi correlati) consente di visualizzare il cluster, gli aggregati e i volumi correlati alla VM di storage:

- **Cluster**

  Visualizza lo stato di integrità del cluster a cui appartiene la VM di storage.

- **Aggregati**

  Visualizza il numero di aggregati che appartengono alla VM di storage selezionata. Viene inoltre

visualizzato lo stato di salute degli aggregati, in base al livello di severità più elevato. Ad esempio, se una VM di storage contiene dieci aggregati, cinque dei quali visualizzano lo stato di avviso e gli altri cinque visualizzano lo stato critico, lo stato visualizzato è critico.

- **Aggregati assegnati**

  Visualizza il numero di aggregati assegnati a una VM di storage. Viene inoltre visualizzato lo stato di salute degli aggregati, in base al livello di severità più elevato.

- **Volumi**

  Visualizza il numero e la capacità dei volumi che appartengono alla VM di storage selezionata. Viene inoltre visualizzato lo stato di salute dei volumi, in base al livello di gravità più elevato. Quando sono presenti volumi FlexGroup nella VM di storage, il conteggio include anche FlexGroup e non i componenti FlexGroup.

Pannello gruppi correlati

Il riquadro Related Groups (gruppi correlati) consente di visualizzare l'elenco dei gruppi associati alla VM di storage selezionata.

Pannello Avvisi correlati

Il riquadro Related Alerts (Avvisi correlati) consente di visualizzare l'elenco degli avvisi creati per la VM di storage selezionata. È inoltre possibile aggiungere un avviso facendo clic sul collegamento **Aggiungi avviso** oppure modificare un avviso esistente facendo clic sul nome dell'avviso.

Pagina dei dettagli del cluster/stato di salute

La pagina Cluster / Health Details fornisce informazioni dettagliate su un cluster selezionato, ad esempio informazioni su stato, capacità e configurazione. È inoltre possibile visualizzare informazioni sulle interfacce di rete (LIF), i nodi, i dischi, le periferiche correlate e gli avvisi correlati per il cluster.

Lo stato accanto al nome del cluster, ad esempio (buona), rappresenta lo stato della comunicazione; indica se Unified Manager può comunicare con il cluster. Non rappresenta lo stato di failover o lo stato generale del cluster.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti attività per il cluster selezionato:

- **Passa alla visualizzazione delle performance**

  Consente di accedere alla pagina Cluster / Performance Details (Dettagli cluster/prestazioni).

- **Azioni**

  - Add Alert (Aggiungi avviso): Apre la finestra di dialogo Add Alert (Aggiungi avviso), che consente di aggiungere un avviso al cluster selezionato.
  - Riscopri: Avvia un aggiornamento manuale del cluster, che consente a Unified Manager di rilevare le recenti modifiche apportate al cluster.

    Se Unified Manager è associato a OnCommand Workflow Automation, l'operazione di risDiscovery

riacquisisce anche i dati memorizzati nella cache da WFA, se presenti.

Una volta avviata l'operazione di riscoperta, viene visualizzato un collegamento ai dettagli del lavoro associato per consentire la registrazione dello stato del lavoro.

- Annotate (Annotazione): Consente di annotare il cluster selezionato.

- **Visualizza cluster**

  Consente di accedere alla vista Health: Tutti i cluster.

Scheda Health (Salute)

Visualizza informazioni dettagliate sui problemi di disponibilità dei dati e capacità dei dati di vari oggetti cluster, ad esempio nodi, SVM e aggregati. I problemi di disponibilità sono correlati alla funzionalità di erogazione dei dati degli oggetti del cluster. I problemi di capacità sono legati alla capacità di memorizzazione dei dati degli oggetti del cluster.

È possibile fare clic sul grafico di un oggetto per visualizzare un elenco filtrato degli oggetti. Ad esempio, è possibile fare clic sul grafico della capacità SVM che visualizza gli avvisi per visualizzare un elenco filtrato di SVM. Questo elenco contiene SVM con volumi o qtree che presentano problemi di capacità con un livello di gravità di Warning. È inoltre possibile fare clic sul grafico della disponibilità delle SVM che visualizza gli avvisi per visualizzare l'elenco delle SVM che presentano problemi di disponibilità con un livello di gravità di avviso.

Problemi di disponibilità

Visualizza graficamente il numero totale di oggetti, inclusi gli oggetti che presentano problemi di disponibilità e gli oggetti che non presentano problemi di disponibilità. I colori nel grafico rappresentano i diversi livelli di gravità dei problemi. Le informazioni riportate di seguito nel grafico forniscono dettagli sui problemi di disponibilità che possono avere un impatto o hanno già influito sulla disponibilità dei dati nel cluster. Ad esempio, vengono visualizzate informazioni sugli shelf di dischi inattivi e sugli aggregati offline.

I dati visualizzati per il grafico a barre SFO si basano sullo stato ha dei nodi. I dati visualizzati per tutti gli altri grafici a barre vengono calcolati in base agli eventi generati.

Problemi di capacità

Visualizza graficamente il numero totale di oggetti, inclusi gli oggetti che presentano problemi di capacità e gli oggetti che non presentano problemi di capacità. I colori nel grafico rappresentano i diversi livelli di gravità dei problemi. Le informazioni sotto il grafico forniscono dettagli sui problemi di capacità che possono avere un impatto o hanno già influito sulla capacità dei dati nel cluster. Ad esempio, vengono visualizzate informazioni sugli aggregati che potrebbero violare i valori di soglia impostati.

Scheda capacità

Visualizza informazioni dettagliate sulla capacità del cluster selezionato.

Capacità

Visualizza il grafico della capacità dei dati sulla capacità utilizzata e la capacità disponibile di tutti gli aggregati allocati:

- Spazio logico utilizzato

  La dimensione reale dei dati memorizzati in tutti gli aggregati di questo cluster senza applicare i risparmi

derivanti dall'utilizzo delle tecnologie di efficienza dello storage ONTAP.

- Utilizzato

  La capacità fisica utilizzata dai dati su tutti gli aggregati. Ciò non include la capacità utilizzata per parità, dimensionamento corretto e prenotazione.

- Disponibile

  Visualizza la capacità disponibile per i dati.

- Parti di ricambio

  Visualizza la capacità storage disponibile per lo storage in tutti i dischi spare.

- Con provisioning

  Visualizza la capacità fornita per tutti i volumi sottostanti.

Dettagli

Visualizza informazioni dettagliate sulla capacità utilizzata e disponibile. Il calcolo esclude i dati dell'aggregato root.

- Capacità totale

  Visualizza la capacità totale del cluster. Non include la capacità assegnata per la parità.

- Utilizzato

  Visualizza la capacità utilizzata dai dati. Ciò non include la capacità utilizzata per parità, dimensionamento corretto e prenotazione.

- Disponibile

  Visualizza la capacità disponibile per i dati.

- Con provisioning

  Visualizza la capacità fornita per tutti i volumi sottostanti.

- Parti di ricambio

  Visualizza la capacità storage disponibile per lo storage in tutti i dischi spare.

Tier cloud

Visualizza la capacità del livello cloud totale utilizzata e la capacità utilizzata per ciascun livello cloud connesso per gli aggregati abilitati FabricPool nel cluster. Un FabricPool può essere concesso in licenza o senza licenza.

Breakout della capacità fisica per tipo di disco

L'area Physical Capacity Breakout by Disk Type (suddivisione capacità fisica per tipo di disco) visualizza informazioni dettagliate sulla capacità dei dischi dei vari tipi di disco nel cluster. Facendo clic sul tipo di disco, è possibile visualizzare ulteriori informazioni sul tipo di disco dalla scheda Disks (dischi).

- Capacità totale utilizzabile

  Visualizza la capacità disponibile e la capacità di riserva dei dischi dati.

- DISCO RIGIDO

  Visualizza graficamente la capacità utilizzata e la capacità disponibile di tutti i dischi dati HDD nel cluster. La linea tratteggiata rappresenta la capacità di riserva dei dischi dati nell'HDD.

- Flash
  - Dati SSD

    Visualizza graficamente la capacità utilizzata e la capacità disponibile dei dischi dati SSD nel cluster.

  - Cache SSD

    Visualizza graficamente la capacità memorizzabile dei dischi della cache SSD nel cluster.

  - SSD Spare

    Visualizza graficamente la capacità di riserva dei dischi SSD, dei dati e della cache nel cluster.

- Dischi non assegnati

  Visualizza il numero di dischi non assegnati nel cluster.

Aggregazioni con elenco problemi di capacità

Visualizza in formato tabulare i dettagli sulla capacità utilizzata e la capacità disponibile degli aggregati che presentano problemi di capacità.

- Stato

  Indica che l'aggregato presenta un problema relativo alla capacità di una certa gravità.

  È possibile spostare il puntatore sullo stato per visualizzare ulteriori informazioni sull'evento o sugli eventi generati per l'aggregato.

  Se lo stato dell'aggregato è determinato da un singolo evento, è possibile visualizzare informazioni quali il nome dell'evento, l'ora e la data in cui è stato attivato l'evento, il nome dell'amministratore a cui è assegnato l'evento e la causa dell'evento. Fare clic sul pulsante **View Details** (Visualizza dettagli) per visualizzare ulteriori informazioni sull'evento.

  Se lo stato dell'aggregato è determinato da più eventi della stessa severità, vengono visualizzati i primi tre eventi con informazioni quali il nome dell'evento, l'ora e la data di attivazione degli eventi e il nome dell'amministratore a cui è assegnato l'evento. È possibile visualizzare ulteriori dettagli su ciascuno di questi eventi facendo clic sul nome dell'evento. È inoltre possibile fare clic sul collegamento **View All Events** (Visualizza tutti gli eventi) per visualizzare l'elenco degli eventi generati.

  > Un aggregato può avere più eventi correlati alla capacità con la stessa severità o con diverse severità. Tuttavia, viene visualizzato solo il livello di severità più elevato. Ad esempio, se un aggregato ha due eventi con livelli di gravità di errore e critico, viene visualizzata solo la severità critica.

- Aggregato

  Visualizza il nome dell'aggregato.

- Capacità dei dati utilizzati

  Visualizza graficamente le informazioni sull'utilizzo della capacità aggregata (in percentuale).

- Giorni al massimo

  Visualizza il numero stimato di giorni rimanenti prima che l'aggregato raggiunga la capacità completa.

Scheda Configuration (Configurazione)

Visualizza i dettagli sul cluster selezionato, ad esempio indirizzo IP, contatto e posizione:

Panoramica del cluster

- Interfaccia di gestione

  Visualizza la LIF di gestione del cluster utilizzata da Unified Manager per connettersi al cluster. Viene visualizzato anche lo stato operativo dell'interfaccia.

- Host Name (Nome host) o IP Address (Indirizzo IP

  Visualizza l'FQDN, il nome breve o l'indirizzo IP della LIF di gestione del cluster utilizzata da Unified Manager per connettersi al cluster.

- FQDN

  Visualizza il nome di dominio completo (FQDN) del cluster.

- Versione del sistema operativo

  Visualizza la versione di ONTAP in esecuzione nel cluster. Se i nodi del cluster eseguono versioni diverse di ONTAP, viene visualizzata la versione ONTAP più recente.

- Contatto

  Visualizza i dettagli dell'amministratore da contattare in caso di problemi con il cluster.

- Posizione

  Visualizza la posizione del cluster.

- Personalità

  Identifica se si tratta di un cluster configurato con All SAN Array.

Panoramica del cluster remoto

Fornisce dettagli sul cluster remoto in una configurazione MetroCluster. Queste informazioni vengono visualizzate solo per le configurazioni MetroCluster.

- Cluster

Visualizza il nome del cluster remoto. È possibile fare clic sul nome del cluster per accedere alla pagina dei dettagli del cluster.

- Nome host o indirizzo IP

  Visualizza l'FQDN, il nome breve o l'indirizzo IP del cluster remoto.

- Posizione

  Visualizza la posizione del cluster remoto.

Panoramica di MetroCluster

Fornisce dettagli sul cluster locale in una configurazione MetroCluster over FC o MetroCluster over IP. Queste informazioni vengono visualizzate solo per le configurazioni MetroCluster su FC o IP.

- Tipo

  Visualizza se il tipo di MetroCluster è a due o quattro nodi. Per MetroCluster over IP, sono supportati solo quattro nodi.

- Configurazione

  Visualizza la configurazione MetroCluster su FC e IP, che può avere i seguenti valori:

Per FC

- Configurazione stretch con cavi SAS
- Configurazione stretch con bridge FC-SAS
- Configurazione fabric con switch FC

> Per un MetroCluster a quattro nodi, è supportata solo la configurazione fabric con switch FC.

Per IP

- Configurazione IP con switch Ethernet (L2 o L3, a seconda della configurazione del cluster)
  - Switch over automatizzato non pianificato (AUSO)

    Visualizza se lo switchover automatizzato non pianificato è attivato per il cluster locale. Per impostazione predefinita, AUSO è abilitato per tutti i cluster in una configurazione MetroCluster a due nodi in Unified Manager. È possibile utilizzare l'interfaccia della riga di comando per modificare l'impostazione DI AUSO. Questo è supportato solo per MetroCluster su FC.

  - Modalità di commutazione

    Visualizza la modalità di switchover per la configurazione MetroCluster over IP. I valori disponibili sono: `Active`, `Negotiated Switchover`, e. `Automatic Unplanned Switchover`.

Nodi

- Disponibilità

  Visualizza il numero di nodi attivi ( ) o verso il basso ( ) nel cluster.

- Versioni del sistema operativo

  Visualizza le versioni di ONTAP in esecuzione sui nodi e il numero di nodi in cui è in esecuzione una determinata versione di ONTAP. Ad esempio, 9.6 (2), 9.3 (1) specifica che due nodi eseguono ONTAP 9.6 e un nodo esegue ONTAP 9.3.

Macchine virtuali di storage

- Disponibilità

  Visualizza il numero di SVM attive ( ) o verso il basso ( ) nel cluster.

Interfacce di rete

- Disponibilità

  Visualizza il numero di LIF non di dati in servizio ( ) o verso il basso ( ) nel cluster.

- Interfacce di gestione dei cluster

  Visualizza il numero di LIF di gestione del cluster.

- Interfacce di gestione dei nodi

  Visualizza il numero di LIF di gestione dei nodi.

- Interfacce cluster

  Visualizza il numero di LIF del cluster.

- Interfacce di intercluster

  Visualizza il numero di LIF intercluster.

Protocolli

- Protocolli dati

  Visualizza l'elenco dei protocolli dati concessi in licenza abilitati per il cluster. I protocolli dati includono iSCSI, CIFS, NFS, NVMe e FC/FCoE.

Protezione

- Mediatori

  Visualizza se il cluster supporta i mediatori e lo stato di connettività del mediatore. Indica se il mediatore è configurato e, se configurato, visualizza lo stato dei mediatori.

- Non applicabile

  Viene visualizzato quando il cluster non supporta i mediatori.

- Non configurato

  Viene visualizzato quando il cluster supporta i mediatori, ma il mediatore non è configurato.

- Indirizzo IP

  Viene visualizzato quando il cluster supporta i mediatori e il mediatore è configurato. Lo stato del mediatore è indicato dal colore. Il colore verde indica che lo stato del mediatore è raggiungibile. Il colore rosso indica che lo stato del mediatore non è raggiungibile.

Livelli di cloud

Elenca i nomi dei Tier cloud a cui è connesso il cluster. Elenca inoltre il tipo (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage o StorageGRID) e gli stati dei Tier cloud (disponibili o non disponibili).

Scheda connettività MetroCluster

Visualizza i problemi e lo stato di connettività dei componenti del cluster nella configurazione MetroCluster over FC. Un cluster viene visualizzato in una casella rossa quando il partner per il disaster recovery del cluster presenta problemi.

La scheda connettività MetroCluster viene visualizzata solo per i cluster che si trovano in una configurazione MetroCluster over FC.

È possibile accedere alla pagina dei dettagli di un cluster remoto facendo clic sul nome del cluster remoto. È inoltre possibile visualizzare i dettagli dei componenti facendo clic sul collegamento count di un componente. Ad esempio, facendo clic sul collegamento count del nodo nel cluster viene visualizzata la scheda Node (nodo) nella pagina Details (dettagli) del cluster. Facendo clic sul collegamento Count dei dischi nel cluster remoto, viene visualizzata la scheda Disk (disco) nella pagina Details (dettagli) del cluster remoto.

Quando si gestisce una configurazione MetroCluster a otto nodi, facendo clic sul collegamento Count del componente Disk Shelf vengono visualizzati solo gli shelf locali della coppia ha predefinita. Inoltre, non è possibile visualizzare gli shelf locali sull'altra coppia ha.

È possibile spostare il puntatore sui componenti per visualizzare i dettagli e lo stato di connettività dei cluster in caso di problemi e per visualizzare ulteriori informazioni sull'evento o sugli eventi generati per il problema.

Se lo stato del problema di connettività tra i componenti è determinato da un singolo evento, è possibile visualizzare informazioni come il nome dell'evento, l'ora e la data in cui è stato attivato l'evento, il nome dell'amministratore a cui è assegnato l'evento e la causa dell'evento. Il pulsante View Details (Visualizza dettagli) fornisce ulteriori informazioni sull'evento.

Se lo stato del problema di connettività tra i componenti è determinato da più eventi della stessa severità, vengono visualizzati i primi tre eventi con informazioni quali il nome dell'evento, l'ora e la data di attivazione degli eventi e il nome dell'amministratore a cui è assegnato l'evento. È possibile visualizzare ulteriori dettagli su ciascuno di questi eventi facendo clic sul nome dell'evento. È inoltre possibile fare clic sul collegamento **View All Events** (Visualizza tutti gli eventi) per visualizzare l'elenco degli eventi generati.

Scheda Replica MetroCluster

Visualizza lo stato dei dati replicati in una configurazione MetroCluster su FC. È possibile utilizzare la scheda Replica MetroCluster per garantire la protezione dei dati eseguendo il mirroring sincrono dei dati con i cluster già in peering. Un cluster viene visualizzato in una casella rossa quando il partner per il disaster recovery del cluster presenta problemi.

La scheda Replica MetroCluster viene visualizzata solo per i cluster in una configurazione MetroCluster over FC.

In un ambiente MetroCluster, è possibile utilizzare questa scheda per verificare le connessioni logiche e il peering del cluster locale con il cluster remoto. È possibile visualizzare la rappresentazione obiettiva dei componenti del cluster con le relative connessioni logiche. In questo modo è possibile identificare i problemi che potrebbero verificarsi durante il mirroring di metadati e dati.

Nella scheda Replica MetroCluster, il cluster locale fornisce la rappresentazione grafica dettagliata del cluster selezionato e il partner MetroCluster fa riferimento al cluster remoto.

Scheda Network Interfaces (interfacce di rete)

Visualizza i dettagli di tutte le LIF non di dati create sul cluster selezionato.

Interfaccia di rete

Visualizza il nome della LIF creata sul cluster selezionato.

Stato operativo

Visualizza lo stato operativo dell'interfaccia, che può essere su (), giù () O Sconosciuto (). Lo stato operativo di un'interfaccia di rete è determinato dallo stato delle porte fisiche.

Stato amministrativo

Visualizza lo stato amministrativo dell'interfaccia, che può essere Up (), giù () O Sconosciuto (). È possibile controllare lo stato amministrativo di un'interfaccia quando si apportano modifiche alla configurazione o durante la manutenzione. Lo stato amministrativo può essere diverso dallo stato operativo. Tuttavia, se lo stato amministrativo di una LIF è inattivo, lo stato operativo è inattivo per impostazione predefinita.

Indirizzo IP

Visualizza l'indirizzo IP dell'interfaccia.

Ruolo

Visualizza il ruolo dell'interfaccia. I ruoli possibili sono LIF di gestione cluster, LIF di gestione nodi, LIF cluster e LIF intercluster.

Porta home

Visualizza la porta fisica a cui è stata originariamente associata l'interfaccia.

Porta corrente

Visualizza la porta fisica a cui è attualmente associata l'interfaccia. Dopo la migrazione LIF, la porta corrente

potrebbe essere diversa dalla porta home.

Policy di failover

Visualizza il criterio di failover configurato per l'interfaccia.

Gruppi di routing

Visualizza il nome del gruppo di routing. È possibile visualizzare ulteriori informazioni sui percorsi e sul gateway di destinazione facendo clic sul nome del gruppo di routing.

I gruppi di routing non sono supportati per ONTAP 8.3 o versioni successive e pertanto viene visualizzata una colonna vuota per questi cluster.

Gruppo di failover

Visualizza il nome del gruppo di failover.

Scheda nodi

Visualizza le informazioni sui nodi nel cluster selezionato. È possibile visualizzare informazioni dettagliate sulle coppie ha, sugli shelf di dischi e sulle porte:

Dettagli HA

Fornisce una rappresentazione grafica dello stato ha e dello stato di salute dei nodi nella coppia ha. Lo stato di salute del nodo è indicato dai seguenti colori:

- **Verde**

  Il nodo è in una condizione di funzionamento.

- **Giallo**

  Il nodo ha assunto il controllo del nodo partner o il nodo deve affrontare alcuni problemi ambientali.

- **Rosso**

  Il nodo non è attivo.

È possibile visualizzare informazioni sulla disponibilità della coppia ha e intraprendere le azioni necessarie per prevenire eventuali rischi. Ad esempio, nel caso di una possibile operazione di takeover, viene visualizzato il seguente messaggio: Failover dello storage possibile.

È possibile visualizzare un elenco degli eventi relativi alla coppia ha e al relativo ambiente, ad esempio ventole, alimentatori, batteria NVRAM, schede flash, service processor e connettività degli shelf di dischi. È inoltre possibile visualizzare l'ora in cui sono stati attivati gli eventi.

È possibile visualizzare altre informazioni relative al nodo, ad esempio il numero di modello.

Se sono presenti cluster a nodo singolo, è possibile visualizzare anche i dettagli relativi ai nodi.

Shelf di dischi

Visualizza le informazioni sugli shelf di dischi nella coppia ha.

È inoltre possibile visualizzare gli eventi generati per gli shelf di dischi e i componenti ambientali e l'ora in cui sono stati attivati gli eventi.

- **ID shelf**

  Visualizza l'ID dello shelf in cui si trova il disco.

- **Stato del componente**

  Visualizza i dettagli ambientali degli shelf di dischi, come alimentatori, ventole, sensori di temperatura, sensori di corrente, connettività del disco, e sensori di tensione. I dettagli ambientali vengono visualizzati sotto forma di icone nei seguenti colori:

  - **Verde**

    I componenti ambientali funzionano correttamente.

  - **Grigio**

    Non sono disponibili dati per i componenti ambientali.

  - **Rosso**

    Alcuni dei componenti ambientali sono inutilizzati.

- **Stato**

  Visualizza lo stato dello shelf di dischi. Gli stati possibili sono Offline, Online, No status, Initialization Required, Missing, E Sconosciuto.

- **Modello**

  Visualizza il numero di modello dello shelf di dischi.

- **Local Disk Shelf**

  Indica se lo shelf di dischi si trova nel cluster locale o nel cluster remoto. Questa colonna viene visualizzata solo per i cluster in una configurazione MetroCluster.

- **ID univoco**

  Visualizza l'identificatore univoco dello shelf di dischi.

- **Versione firmware**

  Visualizza la versione del firmware dello shelf di dischi.

Porte

Visualizza le informazioni relative alle porte FC, FCoE ed Ethernet associate. È possibile visualizzare i dettagli relativi alle porte e ai LIF associati facendo clic sulle icone delle porte.

È inoltre possibile visualizzare gli eventi generati per le porte.

È possibile visualizzare i seguenti dettagli della porta:

- ID porta

  Visualizza il nome della porta. Ad esempio, i nomi delle porte possono essere e0M, e0a e e0b.

- Ruolo

  Visualizza il ruolo della porta. I ruoli possibili sono Cluster, Data, Intercluster, Node-Management e Undefined.

- Tipo

  Visualizza il protocollo di layer fisico utilizzato per la porta. I tipi possibili sono Ethernet, Fibre Channel e FCoE.

- PN. WWN

  Visualizza il nome della porta universale (WWPN) della porta.

- Rev. Firmware

  Visualizza la revisione del firmware della porta FC/FCoE.

- Stato

  Visualizza lo stato corrente della porta. Gli stati possibili sono Up (su), Down (non attivo), link Not Connected (collegamento non connesso) o Sconosciuto ( ).

  È possibile visualizzare gli eventi relativi alle porte dall'elenco Eventi. È inoltre possibile visualizzare i dettagli LIF associati, ad esempio nome LIF, stato operativo, indirizzo IP o WWPN, protocolli, nome della SVM associata alla LIF, porta corrente, policy di failover e gruppo di failover.

Scheda Disks (dischi)

Visualizza i dettagli relativi ai dischi nel cluster selezionato. È possibile visualizzare informazioni relative al disco, ad esempio il numero di dischi utilizzati, dischi di riserva, dischi rotti e dischi non assegnati. È inoltre possibile visualizzare altri dettagli, ad esempio il nome del disco, il tipo di disco e il nodo proprietario del disco.

Riepilogo del pool di dischi

Visualizza il numero di dischi classificati in base ai tipi effettivi (FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN e VMDISK) e lo stato dei dischi. È inoltre possibile visualizzare altri dettagli, ad esempio il numero di aggregati, dischi condivisi, dischi di riserva, dischi rotti, dischi non assegnati, e dischi non supportati. Se si fa clic sul collegamento numero effettivo dei tipi di disco, vengono visualizzati i dischi dello stato selezionato e del tipo effettivo. Ad esempio, se si fa clic sul collegamento Count (Conteggio) per lo stato del disco rotto e il tipo effettivo SAS, vengono visualizzati tutti i dischi con lo stato del disco rotto e il tipo effettivo SAS.

Disco

Visualizza il nome del disco.

Gruppi RAID

Visualizza il nome del gruppo RAID.

Nodo proprietario

Visualizza il nome del nodo a cui appartiene il disco. Se il disco non è assegnato, in questa colonna non viene visualizzato alcun valore.

Stato

Visualizza lo stato del disco: Aggregato, condiviso, spare, interrotto, non assegnato, Non supportato o sconosciuto. Per impostazione predefinita, questa colonna viene ordinata per visualizzare gli stati nel seguente ordine: Interrotto, non assegnato, non supportato, Spare, aggregato, E condiviso.

Disco locale

Visualizza Sì o No per indicare se il disco si trova nel cluster locale o nel cluster remoto. Questa colonna viene visualizzata solo per i cluster in una configurazione MetroCluster.

Posizione

Visualizza la posizione del disco in base al tipo di contenitore, ad esempio Copia, dati o parità. Per impostazione predefinita, questa colonna è nascosta.

Aggregati interessati

Visualizza il numero di aggregati interessati dal problema a causa del disco guasto. È possibile spostare il puntatore sul collegamento del conteggio per visualizzare gli aggregati interessati, quindi fare clic sul nome dell'aggregato per visualizzare i dettagli dell'aggregato. È inoltre possibile fare clic sul conteggio aggregato per visualizzare l'elenco degli aggregati interessati nella vista Health: All aggregates (Salute: Tutti gli aggregati).

In questa colonna non viene visualizzato alcun valore per i seguenti casi:

- Per i dischi rotti quando un cluster contenente tali dischi viene aggiunto a Unified Manager
- Quando non ci sono dischi guasti

Pool di storage

Visualizza il nome del pool di storage a cui appartiene l'SSD. È possibile spostare il puntatore sul nome del pool di storage per visualizzare i dettagli del pool di storage.

Capacità memorizzabile

Visualizza la capacità del disco disponibile per l'utilizzo.

Capacità raw

Visualizza la capacità del disco raw non formattato prima del dimensionamento corretto e della configurazione RAID. Per impostazione predefinita, questa colonna è nascosta.

Tipo

Visualizza i tipi di dischi, ad esempio ATA, SATA, FCAL o VMDISK.

Tipo effettivo

Visualizza il tipo di disco assegnato da ONTAP.

Alcuni tipi di dischi ONTAP sono considerati equivalenti ai fini della creazione e dell'aggiunta di aggregati e della gestione delle spare. ONTAP assegna un tipo di disco effettivo per ciascun tipo di disco.

Blocchi di riserva consumati in %

Visualizza in percentuale i blocchi di riserva consumati nel disco SSD. Questa colonna è vuota per i dischi diversi dai dischi SSD.

Durata nominale utilizzata %

Visualizza in percentuale una stima della durata degli SSD utilizzati, in base all'utilizzo effettivo degli SSD e alla previsione del produttore della durata degli SSD. Un valore superiore a 99 indica che la durata stimata è stata consumata, ma potrebbe non indicare un guasto dell'unità SSD. Se il valore non è noto, il disco viene omesso.

Firmware

Visualizza la versione del firmware del disco.

GIRI/MIN

Visualizza i giri al minuto (RPM) del disco. Per impostazione predefinita, questa colonna è nascosta.

Modello

Visualizza il numero di modello del disco. Per impostazione predefinita, questa colonna è nascosta.

Vendor

Visualizza il nome del produttore del disco. Per impostazione predefinita, questa colonna è nascosta.

ID shelf

Visualizza l'ID dello shelf in cui si trova il disco.

Baia

Visualizza l'ID dell'alloggiamento in cui si trova il disco.

Riquadro delle annotazioni correlate

Consente di visualizzare i dettagli delle annotazioni associati al cluster selezionato. I dettagli includono il nome dell'annotazione e i valori dell'annotazione applicati al cluster. È inoltre possibile rimuovere le annotazioni manuali dal pannello Annotazioni correlate.

Pannello Related Devices (dispositivi correlati)

Consente di visualizzare i dettagli dei dispositivi associati al cluster selezionato.

I dettagli includono le proprietà del dispositivo connesso al cluster, ad esempio il tipo di dispositivo, le dimensioni, il numero e lo stato di salute. È possibile fare clic sul collegamento del conteggio per ulteriori

analisi su quel particolare dispositivo.

È possibile utilizzare il pannello dei partner MetroCluster per ottenere il conteggio e i dettagli sul partner MetroCluster remoto insieme ai componenti del cluster associati, ad esempio nodi, aggregati e SVM. Il pannello dei partner MetroCluster viene visualizzato solo per i cluster in una configurazione MetroCluster.

Il pannello Related Devices (dispositivi correlati) consente di visualizzare e accedere ai nodi, alle SVM e agli aggregati correlati al cluster:

Partner MetroCluster

Visualizza lo stato di salute del partner MetroCluster. Utilizzando il collegamento count, è possibile spostarsi ulteriormente e ottenere informazioni sullo stato e la capacità dei componenti del cluster.

Nodi

Visualizza il numero, la capacità e lo stato di salute dei nodi che appartengono al cluster selezionato. Capacità indica la capacità totale utilizzabile rispetto alla capacità disponibile.

Macchine virtuali di storage

Visualizza il numero di SVM appartenenti al cluster selezionato.

Aggregati

Visualizza il numero, la capacità e lo stato di salute degli aggregati che appartengono al cluster selezionato.

Pannello gruppi correlati

Consente di visualizzare l'elenco dei gruppi che include il cluster selezionato.

Pannello Avvisi correlati

Il riquadro Related Alerts (Avvisi correlati) consente di visualizzare l'elenco degli avvisi per il cluster selezionato. È inoltre possibile aggiungere un avviso facendo clic sul collegamento Add Alert (Aggiungi avviso) o modificarne uno esistente facendo clic sul nome dell'avviso.

Informazioni correlate

"Pagina volumi"
"Visualizzazione dell'elenco e dei dettagli del cluster"

Pagina aggregata/Dettagli salute

È possibile utilizzare la pagina aggregato/Dettagli salute per visualizzare informazioni dettagliate sull'aggregato selezionato, ad esempio la capacità, le informazioni sul disco, i dettagli di configurazione e gli eventi generati. È inoltre possibile visualizzare informazioni sugli oggetti correlati e sugli avvisi correlati per l'aggregato.

Pulsanti di comando

Durante il monitoraggio di un aggregato abilitato a FabricPool, i valori di commit e overcommit in questa pagina sono rilevanti solo per la capacità locale o del Tier di performance. La quantità di spazio disponibile nel Tier cloud non viene riflessa nei valori di overcommit. Analogamente, i valori di soglia aggregati sono rilevanti solo per il Tier di performance locale.

I pulsanti di comando consentono di eseguire le seguenti attività per l'aggregato selezionato:

- **Passa alla visualizzazione delle performance**

  Consente di accedere alla pagina aggregata/Dettagli sulle prestazioni.

- **Azioni**
  - Aggiungi avviso

    Consente di aggiungere un avviso all'aggregato selezionato.

  - Modificare le soglie

    Consente di modificare le impostazioni di soglia per l'aggregato selezionato.

- **Visualizza aggregati**

  Consente di passare alla vista Health: All aggregates (Salute: Tutti gli aggregati).

Scheda capacità

La scheda Capacity (capacità) visualizza informazioni dettagliate sull'aggregato selezionato, ad esempio capacità, soglie e tasso di crescita giornaliero.

Per impostazione predefinita, gli eventi di capacità non vengono generati per gli aggregati root. Inoltre, i valori di soglia utilizzati da Unified Manager non sono applicabili agli aggregati root dei nodi. Solo un rappresentante del supporto tecnico può modificare le impostazioni per questi eventi da generare. Quando le impostazioni vengono modificate da un rappresentante del supporto tecnico, i valori di soglia vengono applicati all'aggregato root del nodo.

- **Capacità**

  Visualizza il grafico della capacità dei dati e il grafico delle copie Snapshot, che visualizzano i dettagli della capacità dell'aggregato:

  - Spazio logico utilizzato

    La dimensione reale dei dati memorizzati nell'aggregato senza applicare i risparmi derivanti dall'utilizzo delle tecnologie di efficienza dello storage ONTAP.

  - Utilizzato

    La capacità fisica utilizzata dai dati nell'aggregato.

  - Assegnazione in eccesso

    Quando lo spazio nell'aggregato viene sottoposto a overcommit, il grafico visualizza un flag con la quantità di overcommit.

- Attenzione

  Visualizza una linea punteggiata nella posizione in cui è impostata la soglia di avviso; ciò significa che lo spazio nell'aggregato è quasi pieno. Se questa soglia viene superata, viene generato l'evento spazio quasi pieno.

- Errore

  Visualizza una linea continua nella posizione in cui è impostata la soglia di errore; ciò significa che lo spazio nell'aggregato è pieno. Se questa soglia viene superata, viene generato l'evento spazio pieno.

- Grafico delle copie Snapshot

  Questo grafico viene visualizzato solo quando la capacità Snapshot utilizzata o la riserva Snapshot non è pari a zero.

Entrambi i grafici mostrano la capacità con cui la capacità Snapshot supera la riserva Snapshot se la capacità Snapshot utilizzata supera la riserva Snapshot.

- **Tier cloud**

  Visualizza lo spazio utilizzato dai dati nel livello cloud per gli aggregati abilitati a FabricPool. Un FabricPool può essere concesso in licenza o senza licenza.

  Quando il cloud Tier viene mirrorato su un altro cloud provider (il "mirror Tier"), vengono visualizzati entrambi i livelli di cloud.

- **Dettagli**

  Visualizza informazioni dettagliate sulla capacità.

  - Capacità totale

    Visualizza la capacità totale nell'aggregato.

  - Capacità dei dati

    Visualizza la quantità di spazio utilizzata dall'aggregato (capacità utilizzata) e la quantità di spazio disponibile nell'aggregato (capacità libera).

  - Riserva di Snapshot

    Visualizza la capacità Snapshot utilizzata e libera dell'aggregato.

  - Capacità con overcommit

    Visualizza l'overcommitment aggregato. L'overcommitment aggregato consente di fornire più storage di quello effettivamente disponibile da un dato aggregato, purché non tutto lo storage sia attualmente in uso. Quando viene utilizzato il thin provisioning, la dimensione totale dei volumi nell'aggregato può superare la capacità totale dell'aggregato.

    > Se l'aggregato è stato sottoposto a overcommit, è necessario monitorarne attentamente lo spazio disponibile e aggiungere storage secondo necessità per evitare errori di scrittura dovuti a spazio insufficiente.

◦ Tier cloud

Visualizza lo spazio utilizzato dai dati nel livello cloud per gli aggregati abilitati a FabricPool. Un FabricPool può essere concesso in licenza o senza licenza. Quando il cloud Tier viene mirrorato su un altro cloud provider (il Tier mirror), vengono visualizzati entrambi i Tier cloud

◦ Spazio cache totale

Visualizza lo spazio totale dei dischi a stato solido (SSD) o delle unità di allocazione aggiunti a un aggregato di Flash Pool. Se Flash Pool è stato abilitato per un aggregato ma non sono stati aggiunti SSD, lo spazio cache viene visualizzato come 0 KB.

Questo campo è nascosto se Flash Pool è disattivato per un aggregato.

◦ Soglie aggregate

Visualizza le seguenti soglie di capacità aggregate:

▪ Soglia quasi completa

Specifica la percentuale in cui un aggregato è quasi pieno.

▪ Soglia completa

Specifica la percentuale in cui un aggregato è pieno.

▪ Soglia quasi sovrascrittura

Specifica la percentuale in cui un aggregato viene quasi sottoposto a overcommit.

▪ Soglia di overcommit

Specifica la percentuale di overcommit di un aggregato.

◦ Altri dettagli: Tasso di crescita giornaliero

Visualizza lo spazio su disco utilizzato nell'aggregato se il tasso di variazione tra gli ultimi due campioni continua per 24 ore.

Ad esempio, se un aggregato utilizza 10 GB di spazio su disco alle 14:00 e 12 GB alle 18:00, il tasso di crescita giornaliero (GB) per questo aggregato è di 2 GB.

◦ Spostamento del volume

Visualizza il numero di operazioni di spostamento del volume attualmente in corso:

▪ Volumi in uscita

Visualizza il numero e la capacità dei volumi spostati fuori dall'aggregato.

È possibile fare clic sul collegamento per visualizzare ulteriori dettagli, ad esempio il nome del volume, l'aggregato in cui il volume viene spostato, lo stato dell'operazione di spostamento del volume e l'ora di fine stimata.

▪ Volumi in

Visualizza il numero e la capacità rimanente dei volumi spostati nell'aggregato.

È possibile fare clic sul collegamento per visualizzare ulteriori dettagli, ad esempio il nome del volume, l'aggregato da cui il volume viene spostato, lo stato dell'operazione di spostamento del volume e l'ora di fine stimata.

- Capacità utilizzata stimata dopo lo spostamento del volume

  Visualizza la quantità stimata di spazio utilizzato (in percentuale e in KB, MB, GB e così via) nell'aggregato al termine delle operazioni di spostamento del volume.

- **Panoramica della capacità - volumi**

  Visualizza i grafici che forniscono informazioni sulla capacità dei volumi contenuti nell'aggregato. Viene visualizzata la quantità di spazio utilizzata dal volume (capacità utilizzata) e la quantità di spazio disponibile (capacità libera) nel volume. Quando l'evento Thin-Provised Volume Space at Risk viene generato per volumi con thin provisioning, viene visualizzata la quantità di spazio utilizzata dal volume (capacità utilizzata) e la quantità di spazio disponibile nel volume ma non utilizzabile (capacità inutilizzabile) a causa di problemi di capacità aggregata.

  È possibile selezionare il grafico che si desidera visualizzare dagli elenchi a discesa. È possibile ordinare i dati visualizzati nel grafico per visualizzare dettagli quali le dimensioni utilizzate, le dimensioni fornite, la capacità disponibile, il tasso di crescita giornaliero più rapido e il tasso di crescita più lento. È possibile filtrare i dati in base alle macchine virtuali di storage (SVM) che contengono i volumi nell'aggregato. È inoltre possibile visualizzare i dettagli dei volumi con thin provisioning. È possibile visualizzare i dettagli di punti specifici sul grafico posizionando il cursore sull'area di interesse. Per impostazione predefinita, il grafico visualizza i primi 30 volumi filtrati nell'aggregato.

Scheda Disk Information (informazioni disco)

Visualizza informazioni dettagliate sui dischi nell'aggregato selezionato, inclusi il tipo e le dimensioni RAID e il tipo di dischi utilizzati nell'aggregato. La scheda visualizza inoltre graficamente i gruppi RAID e i tipi di dischi utilizzati (ad esempio SAS, ATA, FCAL, SSD o VMDISK). È possibile visualizzare ulteriori informazioni, ad esempio l'alloggiamento del disco, lo shelf e la velocità di rotazione, posizionando il cursore sui dischi di parità e sui dischi dati.

- **Dati**

  Visualizza graficamente i dettagli relativi a dischi dati dedicati, dischi dati condivisi o entrambi. Quando i dischi dati contengono dischi condivisi, vengono visualizzati i dettagli grafici dei dischi condivisi. Quando i dischi dati contengono dischi dedicati e dischi condivisi, vengono visualizzati i dettagli grafici dei dischi dati dedicati e dei dischi dati condivisi.

  - **Dettagli RAID**

    I dettagli RAID vengono visualizzati solo per i dischi dedicati.

    - Tipo

      Visualizza il tipo di RAID (RAID0, RAID4, RAID-DP o RAID-TEC).

    - Dimensione gruppo

      Visualizza il numero massimo di dischi consentiti nel gruppo RAID.

        - Gruppi

          Visualizza il numero di gruppi RAID nell'aggregato.

    - **Dischi utilizzati**
        - Tipo effettivo

          Visualizza i tipi di dischi dati (ad esempio ATA, SATA, FCAL, SSD, O VMDISK) nell'aggregato.

        - Dischi di dati

          Visualizza il numero e la capacità dei dischi dati assegnati a un aggregato. I dettagli del disco dati non vengono visualizzati quando l'aggregato contiene solo dischi condivisi.

        - Dischi di parità

          Visualizza il numero e la capacità dei dischi di parità assegnati a un aggregato. I dettagli del disco di parità non vengono visualizzati quando l'aggregato contiene solo dischi condivisi.

        - Dischi condivisi

          Visualizza il numero e la capacità dei dischi dati condivisi assegnati a un aggregato. I dettagli dei dischi condivisi vengono visualizzati solo quando l'aggregato contiene dischi condivisi.

    - **Dischi di riserva**

      Visualizza il tipo, il numero e la capacità effettivi dei dischi dati di riserva disponibili per il nodo nell'aggregato selezionato.

      Quando un aggregato viene eseguito il failover nel nodo partner, Unified Manager non visualizza tutti i dischi di riserva compatibili con l'aggregato.

- **Cache SSD**

  Fornisce dettagli sui dischi SSD con cache dedicata e sui dischi SSD con cache condivisa.

  Vengono visualizzati i seguenti dettagli per i dischi SSD della cache dedicata:

    - **Dettagli RAID**
        - Tipo

          Visualizza il tipo di RAID (RAID0, RAID4, RAID-DP o RAID-TEC).

        - Dimensione gruppo

          Visualizza il numero massimo di dischi consentiti nel gruppo RAID.

        - Gruppi

          Visualizza il numero di gruppi RAID nell'aggregato.

    - **Dischi utilizzati**
        - Tipo effettivo

Indica che i dischi utilizzati per la cache nell'aggregato sono di tipo SSD.

- Dischi di dati

  Visualizza il numero e la capacità dei dischi dati assegnati a un aggregato per la cache.

- Dischi di parità

  Visualizza il numero e la capacità dei dischi di parità assegnati a un aggregato per la cache.

◦ **Dischi di riserva**

Visualizza il tipo, il numero e la capacità effettivi dei dischi spare disponibili per il nodo nell'aggregato selezionato per la cache.

> Quando un aggregato viene eseguito il failover nel nodo partner, Unified Manager non visualizza tutti i dischi di riserva compatibili con l'aggregato.

Fornisce i seguenti dettagli per la cache condivisa:

◦ **Pool di storage**

Visualizza il nome del pool di storage. È possibile spostare il puntatore sul nome del pool di storage per visualizzare i seguenti dettagli:

- Stato

  Visualizza lo stato del pool di storage, che può essere integro o non funzionante.

- Allocazioni totali

  Visualizza le unità di allocazione totali e le dimensioni del pool di storage.

- Dimensione unità di allocazione

  Visualizza la quantità minima di spazio nel pool di storage che è possibile allocare a un aggregato.

- Dischi

  Visualizza il numero di dischi utilizzati per creare il pool di storage. Se il numero di dischi nella colonna del pool di storage e il numero di dischi visualizzati nella scheda Disk Information (informazioni disco) per il pool di storage non corrispondono, significa che uno o più dischi sono rotti e che il pool di storage non è integro.

- Allocazione utilizzata

  Visualizza il numero e la dimensione delle unità di allocazione utilizzate dagli aggregati. È possibile fare clic sul nome dell'aggregato per visualizzare i dettagli dell'aggregato.

- Allocazione disponibile

  Visualizza il numero e le dimensioni delle unità di allocazione disponibili per i nodi. È possibile fare clic sul nome del nodo per visualizzare i dettagli dell'aggregato.

◦ **Cache allocata**

Visualizza le dimensioni delle unità di allocazione utilizzate dall'aggregato.

- **Unità di allocazione**

  Visualizza il numero di unità di allocazione utilizzate dall'aggregato.

- **Dischi**

  Visualizza il numero di dischi contenuti nel pool di storage.

- **Dettagli**
  - Pool di storage

    Visualizza il numero di pool di storage.

  - Dimensione totale

    Visualizza le dimensioni totali dei pool di storage.

- **Tier cloud**

  Visualizza il nome del livello cloud, se è stato configurato un aggregato abilitato a FabricPool, e mostra lo spazio totale utilizzato. Quando il cloud Tier viene mirrorato su un altro cloud provider (il Tier mirror), vengono visualizzati i dettagli di entrambi i Tier cloud

Scheda Configuration (Configurazione)

La scheda Configuration (Configurazione) visualizza i dettagli relativi all'aggregato selezionato, ad esempio il nodo del cluster, il tipo di blocco, il tipo di RAID, la dimensione RAID e il numero di gruppi RAID:

- **Panoramica**
  - Nodo

    Visualizza il nome del nodo che contiene l'aggregato selezionato.

  - Tipo di blocco

    Visualizza il formato a blocchi dell'aggregato: A 32 bit o a 64 bit.

  - Tipo RAID

    Visualizza il tipo di RAID (RAID0, RAID4, RAID-DP, RAID-TEC o RAID misto).

  - Dimensione RAID

    Visualizza le dimensioni del gruppo RAID.

  - Gruppi RAID

    Visualizza il numero di gruppi RAID nell'aggregato.

  - Tipo di SnapLock

    Visualizza il tipo di SnapLock dell'aggregato.

- **Tier cloud**

  Se si tratta di un aggregato abilitato a FabricPool, vengono visualizzati i dettagli del livello cloud. Alcuni campi sono diversi a seconda del provider di storage. Quando il cloud Tier viene mirrorato su un altro cloud provider (il “mirror Tier”), vengono visualizzati entrambi i livelli di cloud.

  - Provider

    Visualizza il nome del provider di storage, ad esempio StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud, Google Cloud Storage o Alibaba Cloud Object Storage.

  - Nome

    Visualizza il nome del livello cloud quando è stato creato da ONTAP.

  - Server

    Visualizza l’FQDN del livello cloud.

  - Porta

    La porta utilizzata per comunicare con il provider cloud.

  - Access Key o account

    Visualizza la chiave di accesso o l’account per il livello cloud.

  - Nome container

    Visualizza il nome del bucket o del container del livello cloud.

  - SSL

    Visualizza se la crittografia SSL è attivata per il livello cloud.

Area della storia

L’area History (Cronologia) visualizza i grafici che forniscono informazioni sulla capacità dell’aggregato selezionato. Inoltre, è possibile fare clic sul pulsante **Esporta** per creare un report in formato CSV per il grafico visualizzato.

È possibile selezionare un tipo di grafico dall’elenco a discesa nella parte superiore del riquadro Cronologia. È inoltre possibile visualizzare i dettagli di un periodo di tempo specifico selezionando 1 settimana, 1 mese o 1 anno. I grafici cronologici consentono di identificare le tendenze: Ad esempio, se l’utilizzo dell’aggregato supera costantemente la soglia quasi completa, è possibile intraprendere l’azione appropriata.

I grafici storici visualizzano le seguenti informazioni:

- **Capacità aggregata utilizzata (%)**

  Visualizza la capacità utilizzata nell’aggregato e l’andamento dell’utilizzo della capacità aggregata in base alla cronologia di utilizzo come grafici a linee, in percentuale, sull’asse verticale (y). Il periodo di tempo viene visualizzato sull’asse orizzontale (x). È possibile selezionare un periodo di tempo di una settimana, un mese o un anno. È possibile visualizzare i dettagli di punti specifici del grafico posizionando il cursore su un’area specifica. È possibile nascondere o visualizzare un grafico a linee facendo clic sulla legenda

appropriata. Ad esempio, quando si fa clic sulla legenda capacità utilizzata, la linea del grafico capacità utilizzata viene nascosta.

- **Capacità aggregata utilizzata rispetto alla capacità totale**

  Visualizza l'andamento dell'utilizzo della capacità aggregata in base alla cronologia di utilizzo, alla capacità utilizzata e alla capacità totale, come grafici a linee, in byte, kilobyte, megabyte, e così via, sull'asse verticale (y). Il periodo di tempo viene visualizzato sull'asse orizzontale (x). È possibile selezionare un periodo di tempo di una settimana, un mese o un anno. È possibile visualizzare i dettagli di punti specifici del grafico posizionando il cursore su un'area specifica. È possibile nascondere o visualizzare un grafico a linee facendo clic sulla legenda appropriata. Ad esempio, quando si fa clic sulla legenda capacità di tendenza utilizzata, la linea del grafico capacità di tendenza utilizzata viene nascosta.

- **Capacità aggregata utilizzata (%) rispetto a impegnata (%)**

  Visualizza l'andamento dell'utilizzo della capacità aggregata in base alla cronologia di utilizzo, nonché lo spazio impegnato come grafici a linee, in percentuale, sull'asse verticale (y). Il periodo di tempo viene visualizzato sull'asse orizzontale (x). È possibile selezionare un periodo di tempo di una settimana, un mese o un anno. È possibile visualizzare i dettagli di punti specifici del grafico posizionando il cursore su un'area specifica. È possibile nascondere o visualizzare un grafico a linee facendo clic sulla legenda appropriata. Ad esempio, quando si fa clic sulla legenda spazio impegnato, la riga del grafico spazio impegnato viene nascosta.

Elenco degli eventi

L'elenco Eventi visualizza i dettagli relativi agli eventi nuovi e riconosciuti:

- **Severità**

  Visualizza la severità dell'evento.

- **Evento**

  Visualizza il nome dell'evento.

- **Tempo di attivazione**

  Visualizza il tempo trascorso da quando è stato generato l'evento. Se il tempo trascorso supera una settimana, viene visualizzata l'indicazione dell'ora in cui è stato generato l'evento.

Pannello Related Devices (dispositivi correlati)

Il pannello Related Devices (dispositivi correlati) consente di visualizzare il nodo del cluster, i volumi e i dischi correlati all'aggregato:

- Nodo *

  Visualizza la capacità e lo stato di integrità del nodo che contiene l'aggregato. Capacità indica la capacità totale utilizzabile rispetto alla capacità disponibile.

- **Aggregati nel nodo**

  Visualizza il numero e la capacità di tutti gli aggregati nel nodo del cluster che contiene l'aggregato selezionato. Viene inoltre visualizzato lo stato di salute degli aggregati, in base al livello di severità più elevato. Ad esempio, se un nodo del cluster contiene dieci aggregati, cinque dei quali visualizzano lo stato

Warning e gli altri cinque dei quali visualizzano lo stato critico, lo stato visualizzato è critico.

- **Volumi**

  Visualizza il numero e la capacità dei volumi FlexVol e FlexGroup nell'aggregato; il numero non include i componenti FlexGroup. Viene inoltre visualizzato lo stato di salute dei volumi, in base al livello di gravità più elevato.

- **Pool di risorse**

  Visualizza i pool di risorse correlati all'aggregato.

- **Dischi**

  Visualizza il numero di dischi nell'aggregato selezionato.

Pannello Avvisi correlati

Il riquadro Related Alerts (Avvisi correlati) consente di visualizzare l'elenco degli avvisi creati per l'aggregato selezionato. È inoltre possibile aggiungere un avviso facendo clic sul collegamento Add Alert (Aggiungi avviso) o modificarne uno esistente facendo clic sul nome dell'avviso.

Informazioni correlate

"Visualizzazione dei dettagli del pool di storage"

Proteggere e ripristinare i dati

Creazione, monitoraggio e risoluzione dei problemi delle relazioni di protezione

Unified Manager consente di creare relazioni di protezione, monitorare e risolvere i problemi relativi alla protezione mirror e alla protezione del vault di backup dei dati memorizzati nei cluster gestiti e ripristinare i dati quando vengono sovrascritti o persi.

Tipi di protezione SnapMirror

In base all'implementazione della topologia dello storage dei dati, Unified Manager consente di configurare diversi tipi di relazioni di protezione di SnapMirror. Tutte le varianti della protezione di SnapMirror offrono una protezione di disaster recovery con failover, ma offrono diverse funzionalità in termini di performance, flessibilità della versione e protezione di più copie di backup.

Relazioni di protezione asincrona SnapMirror tradizionali

La protezione asincrona SnapMirror tradizionale offre la protezione del mirror di replica a blocchi tra i volumi di origine e di destinazione.

Nelle relazioni tradizionali di SnapMirror, le operazioni di mirroring vengono eseguite più velocemente rispetto alle relazioni alternative di SnapMirror, in quanto l'operazione di mirroring si basa sulla replica a blocchi. Tuttavia, la protezione SnapMirror tradizionale richiede che il volume di destinazione venga eseguito con la stessa versione minore o successiva del software ONTAP del volume di origine all'interno della stessa release principale (ad esempio, dalla versione 8.x alla 8.x o dalla 9.x alla 9.x). La replica da un'origine 9.1 a una destinazione 9.0 non è supportata perché la destinazione esegue una versione principale precedente.

Protezione asincrona di SnapMirror con replica flessibile della versione

La protezione asincrona di SnapMirror con replica flessibile della versione offre la protezione del mirror della replica logica tra i volumi di origine e di destinazione, anche se tali volumi vengono eseguiti con versioni diverse di ONTAP 8.3 o software successivo (ad esempio, dalla versione 8.3 alla 8.3.1, dalla 8.3 alla 9.1 o dalla 9.2.2 alla 9.2).

Nelle relazioni di SnapMirror con la replica flessibile della versione, le operazioni di mirroring non vengono eseguite con la stessa velocità delle relazioni di SnapMirror tradizionali.

A causa di un'esecuzione più lenta, SnapMirror con protezione della replica flessibile dalla versione non è adatto per l'implementazione in una delle seguenti circostanze:

- L'oggetto di origine contiene più di 10 milioni di file da proteggere.
- L'obiettivo del punto di ripristino per i dati protetti è di due ore o meno. (Ovvero, la destinazione deve sempre contenere dati ripristinabili mirrorati che non siano più di due ore precedenti rispetto ai dati di origine).

In entrambe le circostanze elencate, è richiesta l'esecuzione più rapida basata sulla replica di blocchi della protezione SnapMirror predefinita.

Protezione asincrona di SnapMirror con replica flessibile della versione e opzione di backup

La protezione asincrona di SnapMirror con replica e opzione di backup flessibili in base alla versione offre una protezione mirror tra i volumi di origine e di destinazione e la capacità di memorizzare più copie dei dati mirrorati nella destinazione.

L'amministratore dello storage può specificare quali copie Snapshot vengono duplicate dall'origine alla destinazione e può anche specificare per quanto tempo conservare tali copie nella destinazione, anche se vengono eliminate dall'origine.

Nelle relazioni di SnapMirror con l'opzione di replica e backup flessibile della versione, le operazioni di mirroring non vengono eseguite con la stessa velocità delle relazioni di SnapMirror tradizionali.

Replica unificata di SnapMirror (mirror e vault)

La replica unificata di SnapMirror consente di configurare il disaster recovery e l'archiviazione sullo stesso volume di destinazione. Come con SnapMirror, la protezione unificata dei dati esegue un trasferimento di riferimento la prima volta che lo si richiama. Un trasferimento di riferimento con la policy di protezione dei dati unificata predefinita "MirrorAndVault" crea una copia Snapshot del volume di origine, quindi trasferisce tale copia e i blocchi di dati a cui fa riferimento al volume di destinazione. Come SnapVault, la protezione unificata dei dati non include copie Snapshot precedenti nella linea di base.

SnapMirror protezione sincrona con sincronizzazione rigorosa

La protezione sincrona di SnapMirror con sincronizzazione "strit" garantisce che i volumi primario e secondario siano sempre una copia reale l'uno dell'altro. Se si verifica un errore di replica quando si tenta di scrivere dati nel volume secondario, l'i/o del client nel volume primario viene interrotto.

SnapMirror protezione sincrona con sincronizzazione regolare

La protezione sincrona di SnapMirror con sincronizzazione "regular" non richiede che il volume primario e secondario siano sempre una copia reale l'uno dell'altro, garantendo così la disponibilità del volume primario. Se si verifica un errore di replica quando si tenta di scrivere i dati nel volume secondario, i volumi primario e secondario non sono sincronizzati e l'i/o del client continua sul volume primario.

Il pulsante Restore (Ripristina) e i pulsanti Relationship Operation (operazione relazione) non sono disponibili durante il monitoraggio delle relazioni di protezione sincrone dalla vista Health: All Volumes (Salute: Tutti i volumi) o dalla pagina Volume / Health Details (Dettagli volume/salute).

Continuità di business sincrona di SnapMirror

La funzionalità di continuità aziendale di SnapMirror (SM-BC) è disponibile con ONTAP 9.8 e versioni successive e può essere utilizzata per proteggere le applicazioni con LUN, consentendo il failover delle applicazioni in modo trasparente, garantendo la business continuity in caso di disastro.

Consente di rilevare e monitorare le relazioni sincrone SnapMirror per i gruppi di coerenza (CGS) disponibili su cluster e macchine virtuali di storage di Unified Manager. SM-BC è supportato sui cluster AFF o su tutti i cluster ARRAY SAN (ASA), in cui i cluster primario e secondario possono essere AFF o ASA. SM-BC protegge le applicazioni con LUN iSCSI o FCP.

Quando si visualizzano i volumi e le LUN protetti dalla relazione SM-BC, è possibile ottenere una vista unificata per le relazioni di protezione, i gruppi di coerenza nell'inventario dei volumi, la topologia di protezione per le relazioni dei gruppi di coerenza, la visualizzazione dei dati storici per le relazioni dei gruppi di coerenza

fino a un anno. È inoltre possibile scaricare il report. È inoltre possibile visualizzare il riepilogo delle relazioni del gruppo di coerenza, cercare il supporto per le relazioni del gruppo di coerenza e ottenere informazioni sui volumi protetti dal gruppo di coerenza.

Nella pagina Relazioni è inoltre possibile ordinare, filtrare ed estendere la protezione degli oggetti di storage di origine e di destinazione e delle relative relazioni protette dal Consistency Group.

Per ulteriori informazioni su SnapMirror Synchronous Business Continuity, fare riferimento a. "ONTAP 9, documentazione per SM-BC".

Impostazione delle relazioni di protezione in Unified Manager

Per utilizzare Unified Manager e OnCommand Workflow Automation per impostare le relazioni SnapMirror e SnapVault per proteggere i dati, è necessario eseguire diversi passaggi.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario stabilire relazioni peer tra due cluster o due macchine virtuali di storage (SVM).
- OnCommand Workflow Automation deve essere integrato con Unified Manager:
  - "Configurare OnCommand Workflow Automation".
  - "Verifica del caching dell'origine dati di Unified Manager in Workflow Automation".

Fasi

1. A seconda del tipo di relazione di protezione che si desidera creare, eseguire una delle seguenti operazioni:
   - "Creare una relazione di protezione SnapMirror".
   - "Creare una relazione di protezione SnapVault".
2. Se si desidera creare un criterio per la relazione, a seconda del tipo di relazione che si sta creando, eseguire una delle seguenti operazioni:
   - "Creare un criterio SnapVault".
   - "Creare un criterio SnapMirror".
3. "Creare una pianificazione SnapMirror o SnapVault".

Configurazione di una connessione tra Workflow Automation e Unified Manager

È possibile configurare una connessione sicura tra OnCommand Workflow Automation (Wfa) e Unified Manager. La connessione all'automazione del flusso di lavoro consente di utilizzare funzionalità di protezione come i flussi di lavoro di configurazione di SnapMirror e SnapVault, oltre a comandi per la gestione delle relazioni di SnapMirror.

Cosa ti serve

- La versione installata di Workflow Automation deve essere 5.1 o superiore.

Il “pacchetto WFA per la gestione di Clustered Data ONTAP” è incluso in WFA 5.1, pertanto non è necessario scaricare questo pacchetto dal NetAppStorage Automation Store e installarlo separatamente sul server WFA come richiesto in passato. "PACCHETTO WFA per la gestione di ONTAP"

- Per supportare le connessioni WFA e Unified Manager, è necessario disporre del nome dell’utente del database creato in Unified Manager.

  A questo utente del database deve essere stato assegnato il ruolo utente Integration Schema.

- È necessario assegnare il ruolo di amministratore o di architetto nell’automazione del flusso di lavoro.
- Per la configurazione di Workflow Automation, è necessario disporre dell’indirizzo host, del numero di porta 443, del nome utente e della password.
- È necessario disporre del ruolo di amministratore dell’applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **automazione del flusso di lavoro**.
2. Nell’area **Database User** della pagina **Workflow Automation**, selezionare il nome e inserire la password dell’utente del database creato per supportare le connessioni di Unified Manager e Workflow Automation.
3. Nell’area **Workflow Automation Credentials** della pagina, immettere il nome host o l’indirizzo IP (IPv4 o IPv6), il nome utente e la password per la configurazione di Workflow Automation.

   È necessario utilizzare la porta del server Unified Manager (porta 443).

4. Fare clic su **Save** (Salva).
5. Se si utilizza un certificato autofirmato, fare clic su **Sì** per autorizzare il certificato di protezione.

   Viene visualizzata la pagina Workflow Automation.

6. Fare clic su **Sì** per ricaricare l’interfaccia utente Web e aggiungere le funzioni di automazione del flusso di lavoro.

Informazioni correlate

"Documentazione NetApp: OnCommand Workflow Automation (release correnti)"

Verifica del caching dell’origine dati di Unified Manager in Workflow Automation

È possibile determinare se il caching dell’origine dati di Unified Manager funziona correttamente controllando se l’acquisizione dell’origine dati ha esito positivo in Workflow Automation. È possibile farlo quando si integra l’automazione del flusso di lavoro con Unified Manager per garantire che la funzionalità di automazione del flusso di lavoro sia disponibile dopo l’integrazione.

Cosa ti serve

Per eseguire questa attività, è necessario assegnare il ruolo di amministratore o di architetto nell’automazione del flusso di lavoro.

Fasi

1. Dall'interfaccia utente di Workflow Automation, selezionare **esecuzione** > **origini dati**.
2. Fare clic con il pulsante destro del mouse sul nome dell'origine dati di Unified Manager, quindi selezionare **Acquire Now** (Acquisisci ora).
3. Verificare che l'acquisizione abbia esito positivo senza errori.

   Gli errori di acquisizione devono essere risolti affinché l'integrazione di Workflow Automation con Unified Manager abbia successo.

Cosa succede quando OnCommand Workflow Automation viene reinstallato o aggiornato

Prima di reinstallare o aggiornare OnCommand Workflow Automation, è necessario rimuovere la connessione tra OnCommand Workflow Automation e Unified Manager e assicurarsi che tutti i processi pianificati o in esecuzione in OnCommand Workflow Automation vengano interrotti.

È inoltre necessario eliminare manualmente Unified Manager da OnCommand Workflow Automation.

Dopo aver reinstallato o aggiornato OnCommand Workflow Automation, è necessario configurare nuovamente la connessione con Unified Manager.

Rimozione dell'installazione di OnCommand Workflow Automation da Unified Manager

È possibile rimuovere la configurazione di OnCommand Workflow Automation da Unified Manager quando non si desidera più utilizzare l'automazione del flusso di lavoro.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **General** > **Workflow Automation** nel menu Setup di sinistra.
2. Nella pagina **Workflow Automation**, fare clic su **Remove Setup** (Rimuovi installazione).

Esecuzione di failover e failback delle relazioni di protezione

Quando un volume di origine nella relazione di protezione viene disattivato a causa di un guasto hardware o di un disastro, è possibile utilizzare le funzionalità delle relazioni di protezione di Unified Manager per rendere la destinazione di protezione accessibile in lettura/scrittura e eseguire il failover su tale volume fino a quando l'origine non è nuovamente online; quindi, è possibile tornare all'origine originale quando è disponibile per la distribuzione dei dati.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- Per eseguire questa operazione, è necessario aver configurato OnCommand Workflow Automation.

Fasi

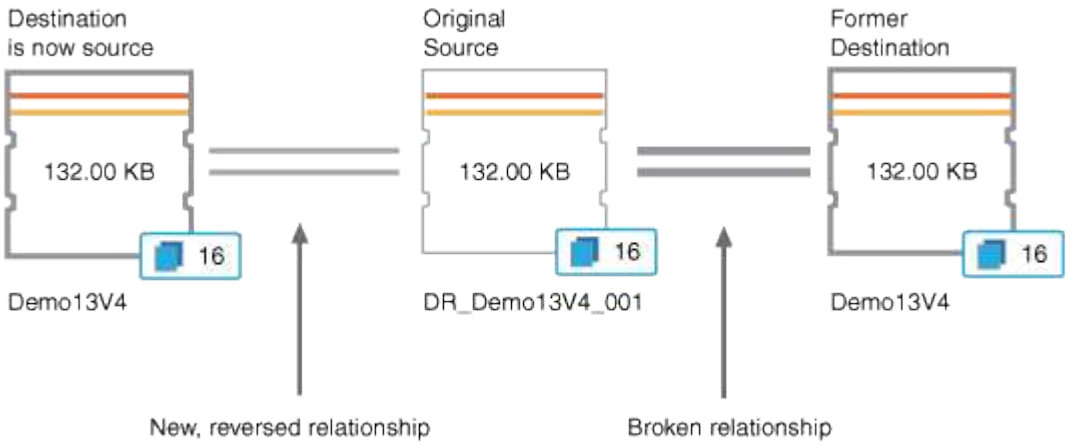
1. "Interrompere la relazione di SnapMirror".

   È necessario interrompere la relazione prima di poter convertire la destinazione da un volume di protezione dati a un volume di lettura/scrittura e prima di invertire la relazione.

2. "Invertire la relazione di protezione".

   Quando il volume di origine originale è nuovamente disponibile, è possibile decidere di ristabilire la relazione di protezione originale ripristinando il volume di origine. Prima di poter ripristinare l'origine, è necessario sincronizzarla con i dati scritti nella destinazione precedente. L'operazione di risincronizzazione inversa consente di creare una nuova relazione di protezione invertendo i ruoli della relazione originale e sincronizzando il volume di origine con la destinazione precedente. Viene creata una nuova copia Snapshot di riferimento per la nuova relazione.

   La relazione invertita appare simile a una relazione a cascata:



3. "Interrompere la relazione SnapMirror inversa".

   Quando il volume di origine originale viene risincronizzato e può nuovamente servire i dati, utilizzare l'operazione di interruzione per interrompere la relazione inversa.

4. "Rimuovere la relazione".

   Quando la relazione invertita non è più necessaria, è necessario rimuovere tale relazione prima di ristabilire la relazione originale.

5. "Risincronizzare la relazione".

   Utilizzare l'operazione di risincronizzazione per sincronizzare i dati dall'origine alla destinazione e ristabilire la relazione originale.

Interruzione di una relazione SnapMirror dalla pagina dei dettagli relativi a volume e salute

È possibile interrompere una relazione di protezione dalla pagina dei dettagli relativi a volume/salute e interrompere i trasferimenti di dati tra un volume di origine e un volume di destinazione in una relazione SnapMirror. È possibile interrompere una relazione quando si desidera migrare i dati, per il disaster recovery o per il test delle applicazioni. Il volume di destinazione viene modificato in un volume di lettura/scrittura. Non è possibile

interrompere una relazione SnapVault.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Nella scheda **Protection** della pagina dei dettagli **Volume / Health**, selezionare dalla topologia la relazione SnapMirror che si desidera interrompere.
2. Fare clic con il pulsante destro del mouse sulla destinazione e selezionare **Interrompi** dal menu.

   Viene visualizzata la finestra di dialogo Interrompi relazione.

3. Fare clic su **continua** per interrompere la relazione.
4. Nella topologia, verificare che la relazione sia interrotta.

Invertire le relazioni di protezione dalla pagina dei dettagli relativi a volume/salute

Quando un disastro disattiva il volume di origine nella relazione di protezione, è possibile utilizzare il volume di destinazione per fornire i dati convertendolo in lettura/scrittura durante la riparazione o la sostituzione dell'origine. Quando l'origine è nuovamente disponibile per ricevere i dati, è possibile utilizzare l'operazione di risincronizzazione inversa per stabilire la relazione nella direzione inversa, sincronizzando i dati sull'origine con i dati sulla destinazione di lettura/scrittura.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.
- La relazione non deve essere una relazione SnapVault.
- Una relazione di protezione deve già esistere.
- Il rapporto di protezione deve essere interrotto.
- Sia l'origine che la destinazione devono essere in linea.
- L'origine non deve essere la destinazione di un altro volume di protezione dei dati.
- Quando si esegue questa attività, i dati sull'origine più recenti dei dati sulla copia Snapshot comune vengono cancellati.
- Le policy e le pianificazioni create sulla relazione di risincronizzazione inversa sono le stesse della relazione di protezione originale.

  Se le policy e le pianificazioni non esistono, vengono create.

Fasi

1. Dalla scheda **Protection** della pagina dei dettagli **Volume / Health**, individuare nella topologia la relazione SnapMirror su cui si desidera invertire l'origine e la destinazione, quindi fare clic con il pulsante destro del mouse.
2. Selezionare **Reverse Resync** (risincronizzazione inversa) dal menu.

Viene visualizzata la finestra di dialogo Reverse Resync (risincronizzazione inversa).

3. Verificare che la relazione visualizzata nella finestra di dialogo **Reverse Resync** sia quella per cui si desidera eseguire l'operazione di risincronizzazione inversa, quindi fare clic su **Submit** (Invia).

   La finestra di dialogo Reverse Resync (risincronizzazione inversa) viene chiusa e viene visualizzato un collegamento al processo nella parte superiore della pagina dei dettagli relativi a volume/salute.

4. **Opzionale:** fare clic su **Visualizza processi** nella pagina dei dettagli **Volume / Health** per tenere traccia dello stato di ciascun processo di risincronizzazione inversa.

   Viene visualizzato un elenco filtrato di lavori.

5. **Opzionale:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina dei dettagli **Volume / Health**.

   L'operazione di risincronizzazione inversa è terminata quando tutte le attività del lavoro sono state completate correttamente.

Rimozione di una relazione di protezione dalla pagina Dettagli volume/salute

È possibile rimuovere una relazione di protezione per eliminare in modo permanente una relazione esistente tra l'origine e la destinazione selezionate, ad esempio quando si desidera creare una relazione utilizzando una destinazione diversa. Questa operazione rimuove tutti i metadati e non può essere annullata.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Nella scheda **Protection** della pagina dei dettagli **Volume / Health**, selezionare dalla topologia la relazione SnapMirror che si desidera rimuovere.
2. Fare clic con il pulsante destro del mouse sul nome della destinazione e selezionare **Remove** (Rimuovi) dal menu.

   Viene visualizzata la finestra di dialogo Rimuovi relazione.

3. Fare clic su **continua** per rimuovere la relazione.

   La relazione viene rimossa dalla pagina Volume / Health Details (Dettagli volume/salute).

Risincronizzazione delle relazioni di protezione dalla pagina dei dettagli relativi a volume/salute

È possibile risincronizzare i dati su una relazione SnapMirror o SnapVault che è stata interrotta e quindi la destinazione è stata fatta in lettura/scrittura in modo che i dati sull'origine corrispondano ai dati sulla destinazione. È inoltre possibile risincronizzare quando viene eliminata una copia Snapshot comune richiesta sul volume di origine, causando il mancato aggiornamento di SnapMirror o SnapVault.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver configurato OnCommand Workflow Automation.

Fasi

1. Dalla scheda **Protection** della pagina dei dettagli **Volume / Health**, individuare nella topologia la relazione di protezione che si desidera risincronizzare e fare clic con il pulsante destro del mouse su di essa.
2. Selezionare **Risincronizza** dal menu.

   In alternativa, dal menu **azioni**, selezionare **relazione** > **risincronizza** per risincronizzare la relazione per la quale si stanno visualizzando i dettagli.

   Viene visualizzata la finestra di dialogo risincronizza.

3. Nella scheda **Opzioni di risincronizzazione**, selezionare una priorità di trasferimento e la velocità di trasferimento massima.
4. Fare clic su **Source Snapshot Copies**, quindi nella colonna **Snapshot Copy**, fare clic su **Default**.

   Viene visualizzata la finestra di dialogo Select Source Snapshot Copy (Seleziona copia snapshot di origine).

5. Se si desidera specificare una copia Snapshot esistente invece di trasferire la copia Snapshot predefinita, fare clic su **Existing Snapshot Copy** (Copia istantanea esistente) e selezionare una copia Snapshot dall'elenco.
6. Fare clic su **Invia**.

   Viene visualizzata nuovamente la finestra di dialogo risincronizza.

7. Se sono state selezionate più origini da risincronizzare, fare clic su **Default** per l'origine successiva per la quale si desidera specificare una copia Snapshot esistente.
8. Fare clic su **Submit** (Invia) per avviare il processo di risincronizzazione.

   Viene avviato il processo di risincronizzazione, viene visualizzata la pagina dei dettagli relativi al volume/salute e viene visualizzato un collegamento ai processi nella parte superiore della pagina.

9. **Opzionale:** fare clic su **Visualizza processi** nella pagina **Dettagli volume/salute** per tenere traccia dello stato di ciascun processo di risincronizzazione.

   Viene visualizzato un elenco filtrato di lavori.

10. **Opzionale:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina dei dettagli **Volume / Health**.

    Il processo di risincronizzazione è terminato al termine di tutte le attività del processo.

Risoluzione di un errore di un lavoro di protezione

Questo flusso di lavoro fornisce un esempio di come è possibile identificare e risolvere un errore di un processo di protezione dalla dashboard di Unified Manager.

Cosa ti serve

Poiché alcune attività di questo flusso di lavoro richiedono l'accesso mediante il ruolo di amministratore, è necessario conoscere i ruoli richiesti per utilizzare le varie funzionalità.

In questo scenario, puoi accedere alla pagina Dashboard per verificare se ci sono problemi con i tuoi processi di protezione. Nell'area incidente di protezione, si noterà la presenza di un incidente con interruzione del processo, che mostra un errore di errore relativo al processo di protezione non riuscito su un volume. Esaminare questo errore per determinare la possibile causa e la potenziale risoluzione.

Fasi

1. Nel pannello incidenti di protezione dell'area incidenti e rischi non risolti della dashboard, fare clic sull'evento **errore del processo di protezione**.

   Il testo associato all'evento viene scritto nel modulo `object_name:/object_name - Error Name`, ad esempio `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

   Viene visualizzata la pagina Dettagli evento relativa al processo di protezione non riuscito.

2. Esaminare il messaggio di errore nel campo cause dell'area **Summary** per determinare il problema e valutare le potenziali azioni correttive.

   Vedere "Identificazione del problema ed esecuzione di azioni correttive per un lavoro di protezione non riuscito".

Identificazione del problema ed esecuzione di azioni correttive per un lavoro di protezione non riuscito

Esaminare il messaggio di errore del lavoro nel campo cause della pagina Dettagli evento e determinare che il lavoro non è riuscito a causa di un errore di copia Snapshot. Quindi, accedere alla pagina dei dettagli relativi a volume/salute per ottenere ulteriori informazioni.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Il messaggio di errore fornito nel campo causa della pagina Dettagli evento contiene il seguente testo relativo al processo non riuscito:

```
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
```

Questo messaggio fornisce le seguenti informazioni:

- Un processo di backup o mirroring non è stato completato correttamente.

  Il lavoro ha comportato una relazione di protezione tra il volume di origine `cluster2_src_vol2` sul server virtuale `cluster2_src_svm` e il volume di destinazione `managed_svc2_vol3` sul server virtuale

denominato `cluster3_dst_svm`.

- Un lavoro di copia Snapshot non è riuscito per `0426cluster2_src_vol2snap` sul volume di origine `cluster2_src_svm:/cluster2_src_vol2`.

In questo scenario, è possibile identificare la causa e le potenziali azioni correttive dell'errore del processo. Tuttavia, la risoluzione del problema richiede l'accesso all'interfaccia utente Web di Gestione sistema o ai comandi dell'interfaccia utente di ONTAP.

Fasi

1. Il messaggio di errore viene esaminato e si determina che un lavoro di copia Snapshot non è riuscito sul volume di origine, indicando che probabilmente si è verificato un problema con il volume di origine.

   In alternativa, è possibile fare clic sul collegamento **Dettagli lavoro** alla fine del messaggio di errore, ma per gli scopi di questo scenario si sceglie di non farlo.

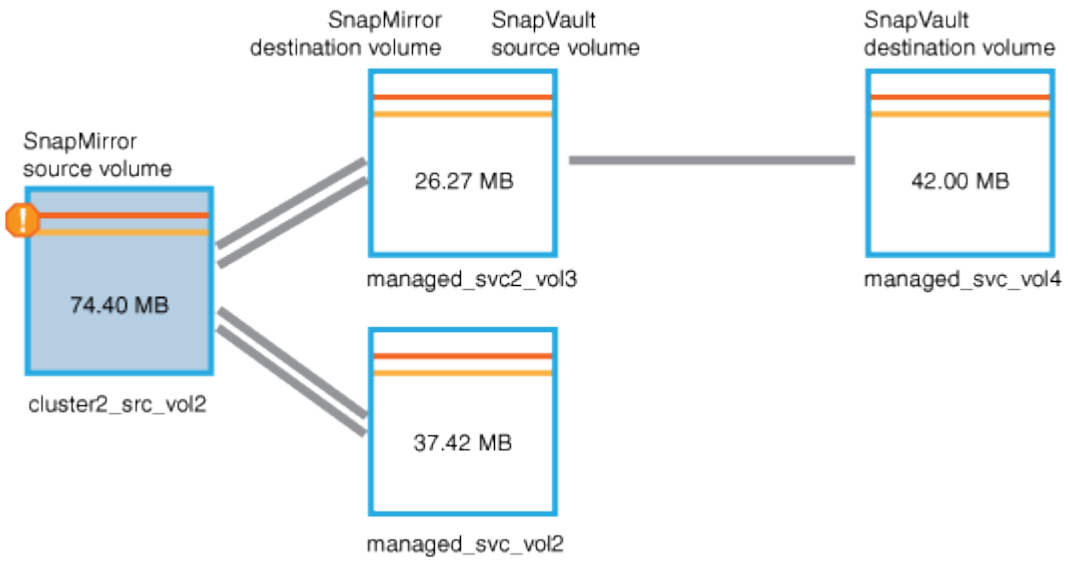
2. Si decide di tentare di risolvere l'evento, quindi eseguire le seguenti operazioni:
   a. Fare clic sul pulsante **Assegna a** e selezionare **Me** dal menu.
   b. Fare clic sul pulsante **Acknowledge** (Conferma) per non continuare a ricevere notifiche di avviso ripetute, se sono stati impostati avvisi per l'evento.
   c. In alternativa, è possibile aggiungere note sull'evento.
3. Fare clic sul campo **Source** (origine) nel riquadro **Summary** (Riepilogo) per visualizzare i dettagli sul volume di origine.

   Il campo **origine** contiene il nome dell'oggetto di origine: In questo caso, il volume su cui è stato pianificato il lavoro di copia Snapshot.

   Viene visualizzata la pagina Volume / Health Details (Dettagli volume/salute) per `cluster2_src_vol2`, Che mostra il contenuto della scheda protezione.

4. Osservando il grafico della topologia di protezione, viene visualizzata un'icona di errore associata al primo volume della topologia, ovvero il volume di origine per la relazione SnapMirror.

   Vengono inoltre visualizzate le barre orizzontali nell'icona del volume di origine, che indicano le soglie di avviso e di errore impostate per tale volume.



5. Posizionare il cursore sull'icona di errore per visualizzare la finestra di dialogo a comparsa che visualizza le impostazioni di soglia e verificare che il volume abbia superato la soglia di errore, indicando un problema di capacità.
6. Fare clic sulla scheda **Capacity**.

   Informazioni sulla capacità del volume `cluster2_src_vol2` viene visualizzato.

7. Nel pannello **Capacity**, viene visualizzata un'icona di errore nel grafico a barre, che indica ancora una volta che la capacità del volume ha superato il livello di soglia impostato per il volume.
8. Sotto il grafico della capacità, si vede che la crescita automatica del volume è stata disattivata e che è stata impostata una garanzia di spazio del volume.

   Si potrebbe decidere di attivare la crescita automatica, ma ai fini di questo scenario, si decide di approfondire la ricerca prima di prendere una decisione su come risolvere il problema di capacità.

9. Scorrere verso il basso fino all'elenco **Eventi** e verificare che siano stati generati gli eventi Protection Job Failed (processo di protezione non riuscito), Volume Days until Full (giorni volume fino al pieno) e Volume Space Full (spazio volume pieno).
10. Nell'elenco **Eventi**, fare clic sull'evento **Volume Space Full** per ottenere ulteriori informazioni, avendo deciso che questo evento sembra più rilevante per il problema di capacità.

    La pagina Dettagli evento visualizza l'evento Volume Space Full per il volume di origine.

11. Nell'area **Riepilogo**, leggi il campo causa dell'evento: `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Sotto l'area Summary (Riepilogo), vengono visualizzate le azioni correttive suggerite.

    Le azioni correttive suggerite vengono visualizzate solo per alcuni eventi, pertanto questa area non viene visualizzata per tutti i tipi di eventi.

    Fare clic nell'elenco delle azioni consigliate che è possibile eseguire per risolvere l'evento Volume Space Full (spazio volume pieno):

    - Abilitare la crescita automatica su questo volume.
    - Ridimensionare il volume.
    - Abilitare ed eseguire la deduplica su questo volume.
    - Attivare ed eseguire la compressione su questo volume.

13. Si decide di attivare la crescita automatica sul volume, ma per farlo, è necessario determinare lo spazio libero disponibile sull'aggregato di origine e il tasso di crescita del volume corrente:
    a. Esaminare l'aggregato di origine, `cluster2_src_aggr1`Nel riquadro **Related Devices** (periferiche correlate).

       È possibile fare clic sul nome dell'aggregato per ottenere ulteriori dettagli sull'aggregato.

       Si determina che l'aggregato dispone di spazio sufficiente per abilitare la crescita automatica del volume.

    b. Nella parte superiore della pagina, osservare l'icona che indica un incidente critico e consultare il testo sotto l'icona.

Si determina che "giorni a pieno: Meno di un giorno | tasso di crescita giornaliero: 5.4%".

14. Accedere a Gestore di sistema o alla CLI ONTAP per attivare `volume autogrow` opzione.

Prendere nota dei nomi del volume e dell'aggregato in modo che siano disponibili quando si attiva la crescita automatica.

15. Dopo aver risolto il problema di capacità, tornare alla pagina dei dettagli di Unified Manager **Event** e contrassegnare l'evento come risolto.

Risoluzione dei problemi di ritardo

Questo flusso di lavoro fornisce un esempio di come è possibile risolvere un problema di ritardo. In questo scenario, sei un amministratore o un operatore che accede alla pagina Unified ManagerDashboard per vedere se ci sono problemi con le tue relazioni di protezione e, se esistono, per trovare soluzioni.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Nella pagina Dashboard, viene visualizzata l'area Incidents and Risks non risolti e viene visualizzato un errore di SnapMirror Lag nel pannello Protection (protezione) sotto Protection Risks (rischi di protezione).

Fasi

1. Nel riquadro **Protection** della pagina **Dashboard**, individuare l'errore di ritardo della relazione SnapMirror e fare clic su di esso.

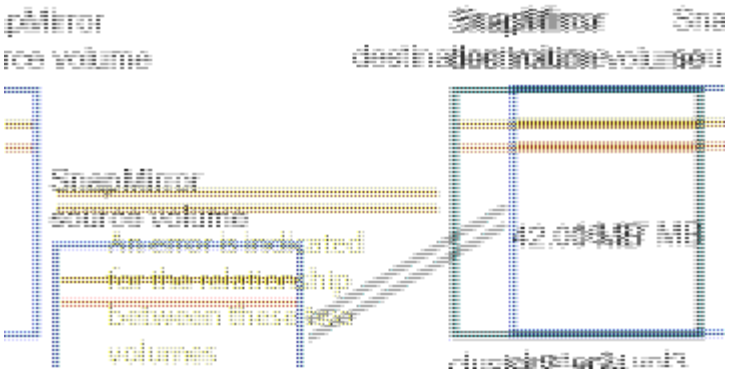
   Viene visualizzata la pagina dei dettagli dell'evento relativo all'errore di ritardo.

2. Dalla pagina dei dettagli **evento** è possibile eseguire una o più delle seguenti attività:
   - Esaminare il messaggio di errore nel campo cause dell'area Summary (Riepilogo) per determinare se sono presenti azioni correttive suggerite.
   - Fare clic sul nome dell'oggetto, in questo caso un volume, nel campo Source (origine) dell'area Summary (Riepilogo) per visualizzare i dettagli sul volume.
   - Cercare le note che potrebbero essere state aggiunte a questo evento.
   - Aggiungere una nota all'evento.
   - Assegnare l'evento a un utente specifico.
   - Riconoscere o risolvere l'evento.
3. In questo scenario, fare clic sul nome dell'oggetto (in questo caso, un volume) nel campo Source (origine) dell'area **Summary** (Riepilogo) per ottenere i dettagli sul volume.

   Viene visualizzata la scheda Protection (protezione) della pagina Volume / Health details (Dettagli volume/salute).

4. Nella scheda **protezione**, viene illustrato il diagramma della topologia.

   Si noti che il volume con l'errore di ritardo è l'ultimo volume in una cascata SnapMirror a tre volumi. Il volume selezionato viene evidenziato in grigio scuro e una doppia linea arancione dal volume di origine indica un errore di relazione di SnapMirror.



5. Fare clic su ciascuno dei volumi nella cascata di SnapMirror.

   Quando si seleziona ciascun volume, le informazioni di protezione in Riepilogo, topologia, Cronologia, Eventi, dispositivi correlati, E le aree degli avvisi correlati vengono modificate per visualizzare i dettagli relativi al volume selezionato.

6. Esaminare l'area **Summary** e posizionare il cursore sull'icona delle informazioni nel campo **Update Schedule** per ciascun volume.

   In questo scenario, si nota che il criterio SnapMirror è DPDefault e la pianificazione di SnapMirror viene aggiornata ogni ora cinque minuti dopo l'ora. Ti renderai conto che tutti i volumi della relazione stanno tentando di completare un trasferimento SnapMirror contemporaneamente.

7. Per risolvere il problema del ritardo, modificare le pianificazioni per due dei volumi a cascata in modo che ciascuna destinazione inizi un trasferimento SnapMirror dopo che l'origine ha completato un trasferimento.

Gestione e monitoraggio delle relazioni di protezione

Active IQ Unified Manager consente di creare relazioni di protezione, monitorare e risolvere i problemi delle relazioni SnapMirror e SnapVault sui cluster gestiti e ripristinare i dati quando vengono sovrascritti o persi.

Per le operazioni di SnapMirror sono disponibili due tipi di replica:

- Asincrono

  La replica dal volume primario al volume secondario è determinata da una pianificazione.

- Sincrono

  La replica viene eseguita simultaneamente sul volume primario e secondario.

È possibile eseguire fino a 10 lavori di protezione contemporaneamente senza alcun impatto sulle performance. Si potrebbe riscontrare un certo impatto sulle performance quando si eseguono contemporaneamente da 11 a 30 job. Si sconsiglia di eseguire più di 30 lavori contemporaneamente.

Visualizzazione dello stato di protezione del volume

La pagina Data Protection (protezione dati) presenta una vista olistica dei dettagli di protezione dei dati per tutti i volumi protetti in un singolo cluster o per tutti i cluster in un

data center.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Dashboard**.
2. A seconda che si desideri visualizzare lo stato di protezione dei dati per tutti i cluster monitorati o per un singolo cluster, selezionare **tutti i cluster** o selezionare un singolo cluster dal menu a discesa.
3. Fare clic sulla freccia destra nella parte superiore del pannello Data Protection (protezione dati). Viene visualizzata la pagina **Data Protection**.

A seconda che sia stato selezionato un singolo cluster o tutti i cluster nel data center, questa pagina visualizza lo stato di protezione dei dati dei volumi protetti dalle copie Snapshot o dalle policy di SnapMirror, oltre al conteggio dei volumi non protetti.

Selezionando un cluster dall'elenco **Individual Cluster** (singolo cluster), viene visualizzato lo stato di relazione di Snapshot Protection e SnapMirror dei volumi protetti in quel cluster.

Facendo clic sugli eventi in questa pagina si accede alla pagina Dettagli evento. È possibile fare clic sul collegamento **View All** (Visualizza tutto) per visualizzare tutti gli eventi di protezione attivi nella pagina Event Management Inventory (inventario gestione eventi). Puoi passare il mouse per visualizzare i rispettivi conteggi e legende. È possibile fare clic su:

- I grafici a barre dei volumi non protetti e dei volumi protetti dalle copie Snapshot consentono di accedere alla pagina volumi e visualizzare i dettagli.
- I grafici a barre per tutte le relazioni vanno alla pagina Relazioni, dove i dettagli vengono filtrati dal cluster di origine.

Visualizzare lo stato di protezione dei volumi protetti dalle copie Snapshot

Snapshot Copies Overview: Panoramica dei volumi protetti dalle copie Snapshot, ad esempio:

- Il numero totale di volumi protetti e non protetti dalle copie Snapshot.
- Il numero totale di volumi che utilizzano o superano lo spazio riservato per le copie Snapshot.

Snapshot Copies Analysis illustra in dettaglio le seguenti informazioni:

- Singoli eventi per le copie Snapshot, inclusi gli eventi generati nelle ultime 24 ore.
- Grafico dettagliato dei volumi protetti e non protetti dalle copie Snapshot.
- Volumi che utilizzano, non utilizzano e violano la capacità di copia Snapshot riservata.
- Disgresso dei conteggi dei volumi in termini di numero di copie Snapshot.

Punti da notare per le copie Snapshot

- Per il conteggio dei volumi protetti dalle copie Snapshot, vengono presi in considerazione sia i volumi di origine che quelli di destinazione.
- Il numero di copie Snapshot restituite riguarda solo i volumi online e disponibili.
- L'intervallo del grafico per il numero di copie Snapshot è dinamico. Viene generato in base al numero di snapshot presenti nel cluster selezionato.
- Per considerare un volume come protetto, è necessario attivare la pianificazione della copia Snapshot del volume.

- Il valore dello spazio riservato per le copie Snapshot è importante per visualizzare la quantità di spazio su disco utilizzata o per calcolare lo spazio che può essere recuperato se una o più copie Snapshot vengono eliminate.

Visualizzare lo stato di protezione per le relazioni SnapMirror

Panoramica di SnapMirror: Panoramica dei volumi protetti dalle policy di SnapMirror, ad esempio:

- Il numero di volumi protetti dalle rispettive policy di SnapMirror, ad esempio le relazioni di SnapMirror dei volumi, il disaster recovery delle macchine virtuali di storage (SVM-DR) e le relative combinazioni.
- Il numero totale di relazioni SnapMirror che hanno riscontrato un ritardo nell'obiettivo del punto di ripristino (RPO) in base allo stato di ritardo.

SnapMirror Analysis illustra in dettaglio le seguenti informazioni:

- Singoli eventi generati per le relazioni SnapMirror, inclusi gli eventi generati nelle ultime 24 ore
- Il numero di volumi protetti da ciascun tipo di policy SnapMirror.
- Il numero di relazioni protette dai tipi di relazione SnapMirror, come Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StricxtSync, SnapMirror Business Continuity (SMBC) e Sync.
- Il numero di relazioni sane e malsane.
- Disgresso del numero di relazioni del volume. È possibile alternare i grafici in base al ritardo RPO e allo stato.
- Soglie di ritardo per la relazione non gestita. È possibile fare clic sull'icona delle impostazioni ( ) per configurare le impostazioni della soglia di ritardo. Per ulteriori informazioni, vedere "Configurazione delle impostazioni delle soglie di ritardo per le relazioni di protezione non gestite".

Punti da prendere in considerazione per le relazioni di SnapMirror

- Per il conteggio delle relazioni SnapMirror, vengono contati i volumi di origine, abilitati per la lettura e la scrittura. I volumi di destinazione e root non vengono presi in considerazione.
- Per la relazione SnapMirror, gli eventi vengono visualizzati per il cluster di origine.
- Il numero di relazioni di SnapMirror include il numero di volumi con origini e destinazioni sullo stesso cluster o su cluster diversi.
- La durata del ritardo dell'RPO nella replica dei dati si basa sulla relazione SnapMirror. Lo stato viene classificato come `ok`, `warning`, o. `error`, in base alla soglia di relazione impostata. È possibile controllare lo stato per determinare se i parametri funzionano come previsto o se è necessario risolvere qualsiasi problema.
- Se un volume ha più relazioni SnapMirror, ogni tipo di relazione viene conteggiato per il ritardo RPO.
- Le relazioni dei volumi sono considerate non integre in caso di problemi di replica dei dati tra l'origine e la destinazione, ad esempio quando la relazione viene interrotta.

Visualizzare i cluster protetti dalla configurazione MetroCluster

Il MetroCluster pannello **protezione dati** della pagina **protezione dati** visualizza il numero di cluster protetti o non protetti dalla configurazione MetroCluster over FC o IP del sito. Facendo clic sui grafici a barre di questo pannello, si accede alla pagina Clusters, in cui i dettagli del cluster vengono filtrati in base ai cluster protetti o non protetti. Per informazioni sul monitoraggio della configurazione di MetroCluster, vedere "Monitoraggio delle configurazioni MetroCluster".

Visualizzazione delle relazioni di protezione dei volumi

Dalla vista relazione: Tutte le relazioni e dalla pagina Relazioni volume, è possibile visualizzare lo stato delle relazioni SnapMirror e SnapVault del volume esistente. È inoltre possibile esaminare i dettagli relativi alle relazioni di protezione, tra cui lo stato di trasferimento e ritardo, i dettagli di origine e destinazione, le informazioni di pianificazione e policy e così via.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Da questa pagina è inoltre possibile avviare i comandi di relazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Dal menu Visualizza, selezionare **relazione** > **tutte le relazioni**.

   Viene visualizzata la vista relazione: Tutte le relazioni.

3. Scegliere uno dei seguenti metodi per visualizzare i dettagli della protezione del volume:
   - Per visualizzare le informazioni correnti su tutte le relazioni del volume, rimanere nella pagina predefinita **tutte le relazioni**.
   - Per visualizzare informazioni dettagliate sui trend di trasferimento dei volumi in un determinato periodo di tempo, nel menu View (Visualizza), selezionare Relationship (relazione): Last 1 Month Transfer Status (Stato trasferimento ultimo 1 mese) view (visualizzazione).
   - Per visualizzare informazioni dettagliate sull'attività di trasferimento del volume giorno per giorno, nel menu View (Visualizza), selezionare Relationship: Last 1 Month Transfer Rate view (relazione: Vista tasso di trasferimento ultimo 1 mese).

   Le viste di trasferimento dei volumi visualizzano le informazioni solo per i volumi nelle relazioni asincrone, i volumi nelle relazioni sincrone non vengono visualizzati.

Monitoraggio delle LUN in una relazione Consistency Group

Se l'ambiente ONTAP supporta la business continuity SnapMirror (SM-BC) per proteggere le applicazioni con LUN, è possibile visualizzare e monitorare tali LUN su Active IQ Unified Manager.

SM-BC garantisce l'obiettivo RTO (Zero Recovery Time Objective) durante il failover in ambienti SAN. In un'implementazione tipica che supporta SM-BC, le LUN sui volumi sono protette dalle relazioni del gruppo di coerenza.

Questi LUN primari e secondari sono LUN compositi o una coppia LUN replica con lo stesso UUID e numero di serie. Le operazioni di i/o (sia in lettura che in scrittura) vengono multiplate tra i siti di origine e di destinazione su queste LUN composite, garantendo la trasparenza.

Per la visualizzazione di LUN composite, è necessario aggiungere e rilevare i cluster primari e secondari con le LUN che fanno parte della relazione Consistency Group in Unified Manager. Sono supportati solo i LUN iSCSI e FCP.

Per informazioni su SM-BC, vedere "ONTAP 9, documentazione per SM-BC".

Per visualizzare LUN composite nel proprio ambiente, attenersi alla seguente procedura:

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **LUN**.
2. Dal menu View (Visualizza), selezionare **Relationship** (relazione) > **All LUN** (tutte le LUN).

   Viene visualizzata la vista Relationship: All LUN (relazione: Tutti i LUN).

È possibile visualizzare i dettagli del LUN, ad esempio il nome del LUN, il volume, la VM di storage che ospita il LUN, il cluster, il gruppo di coerenza e il LUN del partner. È possibile fare clic su ciascuno di questi componenti per visualizzare una vista dettagliata. Facendo clic sul gruppo di coerenza si accede alla pagina Relazioni.

Facendo clic sul LUN del partner è possibile visualizzare i dettagli di configurazione nella scheda SAN della pagina Storage VM Details (Dettagli VM storage) per la VM di storage su cui è ospitato il LUN del partner. Vengono visualizzate informazioni quali gli iniziatori e i gruppi di iniziatori e altri aspetti del LUN del partner.

È possibile eseguire le funzioni standard a livello di griglia di ordinamento, filtraggio, generazione e caricamento dei report per le LUN protette nel proprio ambiente.

Creazione di una relazione di protezione SnapVault dalla vista Salute: Tutti i volumi

È possibile utilizzare la vista Health: All Volumes (Salute: Tutti i volumi) per creare relazioni SnapVault per uno o più volumi sulla stessa Storage VM, in modo da abilitare i backup dei dati a scopo di protezione.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Il menu **Protect** non viene visualizzato nelle seguenti istanze:

- Se le impostazioni RBAC non consentono questa azione: Ad esempio, se si dispone solo di privilegi operatore
- Quando l'ID del volume è sconosciuto: Ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nella vista **Health: All Volumes** (Salute: Tutti i volumi), selezionare un volume che si desidera proteggere e fare clic su **Protect** (protezione).

   In alternativa, per creare più relazioni di protezione sulla stessa SVM (Storage Virtual Machine), selezionare uno o più volumi nella vista Health: All Volumes (Salute: Tutti i volumi) e fare clic su **Protect** (protezione) sulla barra degli strumenti.

3. Selezionare **SnapVault** dal menu.

   Viene visualizzata la finestra di dialogo Configura protezione.

4. Fare clic su **SnapVault** per visualizzare la scheda **SnapVault** e configurare le informazioni sul volume secondario.
5. Fare clic su **Advanced** (Avanzate) per impostare deduplica, compressione, crescita automatica e garanzia di spazio secondo necessità, quindi fare clic su **Apply** (Applica).
6. Completare l'area **informazioni destinazione** e l'area **Impostazioni relazione** nella scheda **SnapVault**.
7. Fare clic su **Apply** (Applica).

   Viene nuovamente visualizzato Health: All Volumes (Salute: Tutti i volumi).

8. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della vista **Health: All Volumes** (Salute: Tutti i volumi).

   Se si crea una sola relazione di protezione, viene visualizzata la pagina Dettagli lavoro; tuttavia, se si creano più relazioni di protezione, viene visualizzato un elenco filtrato di tutti i lavori associati all'operazione di protezione.

9. Effettuare una delle seguenti operazioni:
   - Se si dispone di un solo lavoro, fare clic su **Refresh** (Aggiorna) per aggiornare l'elenco delle attività e i dettagli delle attività associati al lavoro di configurazione della protezione e per determinare quando il lavoro è completo.
   - Se si dispone di più lavori:
     i. Fare clic su un lavoro nell'elenco dei lavori.
     ii. Fare clic su **Refresh** (Aggiorna) per aggiornare l'elenco delle attività e i dettagli delle attività associati al processo di configurazione della protezione e per determinare quando il processo è completo.
     iii. Utilizzare il pulsante **Indietro** per tornare all'elenco filtrato e visualizzare un altro processo.

Creazione di una relazione di protezione SnapVault dalla pagina dei dettagli relativi a volume/salute

È possibile creare una relazione SnapVault utilizzando la pagina dei dettagli relativi a volume/stato di salute in modo che i backup dei dati siano abilitati per scopi di protezione sui volumi.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- Per eseguire questa attività, è necessario aver impostato l'automazione del flusso di lavoro.

Il menu **Protect** non viene visualizzato nelle seguenti istanze:

- Se le impostazioni RBAC non consentono questa azione: Ad esempio, se si dispone solo di privilegi operatore
- Quando l'ID del volume è sconosciuto: Ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato

Fasi

1. Nella scheda **Protection** della pagina dei dettagli **Volume / Health**, fare clic con il pulsante destro del mouse su un volume nella vista della topologia che si desidera proteggere.

2. Selezionare **Protect** > **SnapVault** dal menu.

   Viene visualizzata la finestra di dialogo Configura protezione.

3. Fare clic su **SnapVault** per visualizzare la scheda **SnapVault** e configurare le informazioni sulle risorse secondarie.
4. Fare clic su **Advanced** (Avanzate) per impostare deduplica, compressione, crescita automatica e garanzia di spazio secondo necessità, quindi fare clic su **Apply** (Applica).
5. Completare l'area **Destination Information** (informazioni destinazione) e l'area **Relationship Settings** (Impostazioni relazione) nella finestra di dialogo **Configure Protection** (Configura protezione).
6. Fare clic su **Apply** (Applica).

   Viene visualizzata nuovamente la pagina dei dettagli relativi a volume/salute.

7. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della pagina dei dettagli **Volume / Health**.

   Viene visualizzata la pagina Dettagli lavoro.

8. Fare clic su **Refresh** (Aggiorna) per aggiornare l'elenco delle attività e i dettagli delle attività associati al processo di configurazione della protezione e per determinare quando il processo è completo.

   Una volta completate le attività di lavoro, le nuove relazioni vengono visualizzate nella vista topologia della pagina dei dettagli volume/salute.

Creazione di una relazione di protezione SnapMirror dalla vista Health: All Volumes (Salute: Tutti i volumi)

Utilizzando la vista Health: All Volumes (Salute: Tutti i volumi) è possibile creare diverse relazioni di protezione SnapMirror contemporaneamente selezionando più di un volume sulla stessa VM di storage.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Il menu **Protect** non viene visualizzato nelle seguenti istanze:

- Se le impostazioni RBAC non consentono questa azione: Ad esempio, se si dispone solo di privilegi operatore
- Quando l'ID del volume è sconosciuto: Ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato

Fasi

1. Nella vista **Health: All Volumes** (Salute: Tutti i volumi), selezionare un volume che si desidera proteggere.

   In alternativa, per creare più relazioni di protezione sulla stessa SVM, selezionare uno o più volumi nella vista Health: All Volumes (Salute: Tutti i volumi) e fare clic su **Protect** > **SnapMirror** nella barra degli strumenti.

Viene visualizzata la finestra di dialogo Configura protezione.

2. Fare clic su **SnapMirror** per visualizzare la scheda **SnapMirror** e configurare le informazioni di destinazione.
3. Fare clic su **Advanced** (Avanzate) per impostare la garanzia di spazio, secondo necessità, quindi fare clic su **Apply** (Applica).
4. Completare l'area **Destination Information** (informazioni destinazione) e l'area **Relationship Settings** (Impostazioni relazione) nella scheda **SnapMirror**.
5. Fare clic su **Apply** (Applica).

   Viene nuovamente visualizzato Health: All Volumes (Salute: Tutti i volumi).

6. Fare clic sul collegamento relativo al processo di configurazione della protezione nella parte superiore della vista **Health: All Volumes** (Salute: Tutti i volumi).

   Se si crea una sola relazione di protezione, viene visualizzata la pagina Dettagli lavoro; tuttavia, se si creano più relazioni di protezione, viene visualizzato un elenco di tutti i lavori associati all'operazione di protezione.

7. Effettuare una delle seguenti operazioni:
   - Se si dispone di un solo lavoro, fare clic su **Refresh** (Aggiorna) per aggiornare l'elenco delle attività e i dettagli delle attività associati al lavoro di configurazione della protezione e per determinare quando il lavoro è completo.
   - Se si dispone di più lavori:
     i. Fare clic su un lavoro nell'elenco dei lavori.
     ii. Fare clic su **Refresh** (Aggiorna) per aggiornare l'elenco delle attività e i dettagli delle attività associati al processo di configurazione della protezione e per determinare quando il processo è completo.
     iii. Utilizzare il pulsante **Indietro** per tornare all'elenco filtrato e visualizzare un altro processo.

A seconda della SVM di destinazione specificata durante la configurazione o delle opzioni attivate nelle impostazioni avanzate, la relazione SnapMirror risultante potrebbe essere una delle diverse possibili variazioni:

- Se è stata specificata una SVM di destinazione che viene eseguita con la stessa versione o una versione più recente di ONTAP rispetto a quella del volume di origine, il risultato predefinito è una relazione SnapMirror basata sulla replica a blocchi.
- Se è stata specificata una SVM di destinazione che viene eseguita con la stessa versione o una versione più recente di ONTAP rispetto a quella del volume di origine, ma è stata attivata la replica flessibile della versione nelle impostazioni avanzate, ne risulta una relazione SnapMirror con la replica flessibile della versione.
- Se è stata specificata una SVM di destinazione che viene eseguita con una versione precedente di ONTAP rispetto a quella del volume di origine e la versione precedente supporta la replica flessibile dalla versione, il risultato è automatico una relazione di SnapMirror con la replica flessibile dalla versione.

Creazione di una relazione di protezione SnapMirror dalla pagina dei dettagli relativi a volume/stato

È possibile utilizzare la pagina Dettagli volume/stato per creare una relazione SnapMirror in modo che la replica dei dati sia attivata per scopi di protezione. La replica di

SnapMirror consente di ripristinare i dati dal volume di destinazione in caso di perdita di dati sull'origine.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Il menu **Protect** non viene visualizzato nelle seguenti istanze:

- Se le impostazioni RBAC non consentono questa azione: Ad esempio, se si dispone solo di privilegi operatore
- Quando l'ID del volume è sconosciuto: Ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato

È possibile eseguire fino a 10 lavori di protezione contemporaneamente senza alcun impatto sulle performance. Si potrebbe riscontrare un certo impatto sulle performance quando si eseguono contemporaneamente da 11 a 30 job. Si sconsiglia di eseguire più di 30 lavori contemporaneamente.

Fasi

1. Nella scheda **protezione** della pagina dei dettagli **Volume / Health**, fare clic con il pulsante destro del mouse nella vista topologia per visualizzare il nome di un volume che si desidera proteggere.
2. Selezionare **Protect** > **SnapMirror** dal menu.

   Viene visualizzata la finestra di dialogo Configura protezione.

3. Fare clic su **SnapMirror** per visualizzare la scheda **SnapMirror** e configurare le informazioni di destinazione.
4. Fare clic su **Advanced** (Avanzate) per impostare la garanzia di spazio, secondo necessità, quindi fare clic su **Apply** (Applica).
5. Completare l'area **Destination Information** (informazioni destinazione) e l'area **Relationship Settings** (Impostazioni relazione) nella finestra di dialogo **Configure Protection** (Configura protezione).
6. Fare clic su **Apply** (Applica).

   Viene visualizzata nuovamente la pagina dei dettagli relativi a volume/salute.

7. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della pagina dei dettagli **Volume / Health**.

   Le attività e i dettagli del lavoro vengono visualizzati nella pagina Dettagli lavoro.

8. Nella pagina dei dettagli **lavoro**, fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al lavoro di configurazione della protezione e per determinare quando il lavoro è completo.
9. Una volta completate le attività di lavoro, fare clic su **Indietro** nel browser per tornare alla pagina dei dettagli **Volume / Health**.

   La nuova relazione viene visualizzata nella vista topologia della pagina dei dettagli volume/salute.

A seconda della SVM di destinazione specificata durante la configurazione o delle opzioni attivate nelle impostazioni avanzate, la relazione SnapMirror risultante potrebbe essere una delle diverse possibili variazioni:

- Se è stata specificata una SVM di destinazione che viene eseguita con la stessa versione o una versione più recente di ONTAP rispetto a quella del volume di origine, il risultato predefinito è una relazione SnapMirror basata sulla replica a blocchi.
- Se è stata specificata una SVM di destinazione che viene eseguita con la stessa versione o una versione più recente di ONTAP rispetto a quella del volume di origine, ma è stata attivata la replica flessibile della versione nelle impostazioni avanzate, ne risulta una relazione SnapMirror con la replica flessibile della versione.
- Se è stata specificata una SVM di destinazione che viene eseguita con una versione precedente di ONTAP o una versione superiore a quella del volume di origine e la versione precedente supporta la replica flessibile dalla versione, il risultato è automatico una relazione di SnapMirror con la replica flessibile dalla versione.

Creazione di una relazione SnapMirror con replica flessibile della versione

È possibile creare una relazione SnapMirror con replica flessibile della versione. La replica flessibile della versione consente di implementare la protezione SnapMirror anche se i volumi di origine e di destinazione vengono eseguiti con versioni diverse di ONTAP.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.
- Le SVM di origine e di destinazione devono disporre di una licenza SnapMirror abilitata.
- Le SVM di origine e di destinazione devono essere eseguite con una versione del software ONTAP che supporti la replica flessibile dalla versione.

SnapMirror con replica flessibile della versione consente di implementare la protezione di SnapMirror anche in ambienti di storage eterogenei in cui non tutto lo storage viene eseguito con una sola versione di ONTAP; tuttavia, le operazioni di mirroring eseguite con SnapMirror con replica flessibile della versione non vengono eseguite con la stessa velocità con la replica a blocchi tradizionale di SnapMirror.

Fasi

1. Visualizzare la finestra di dialogo **Configura protezione** per il volume che si desidera proteggere.
    - Se si visualizza la scheda protezione della pagina Dettagli volume/stato, fare clic con il pulsante destro del mouse nella vista topologia con il nome di un volume che si desidera proteggere e selezionare **Protect** > **SnapMirror** dal menu.
    - Se si visualizza la vista Health: All Volumes (Salute: Tutti i volumi), individuare un volume che si desidera proteggere e fare clic con il pulsante destro del mouse, quindi selezionare **Protect** > **SnapMirror** dal menu. Viene visualizzata la finestra di dialogo Configura protezione.
2. Fare clic su **SnapMirror** per visualizzare la scheda **SnapMirror**.
3. Completare l'area **Destination Information** (informazioni destinazione) e l'area **Relationship Settings** (Impostazioni relazione) nella finestra di dialogo **Configure Protection** (Configura protezione).

    Se si specifica una SVM di destinazione che viene eseguita con una versione precedente di ONTAP rispetto al volume di origine che si sta proteggendo e se tale versione precedente supporta la replica flessibile della versione, questa attività configura automaticamente SnapMirror con replica flessibile della versione.

4. Se si specifica una SVM di destinazione che viene eseguita con la stessa versione di ONTAP del volume di

origine, ma si desidera comunque configurare SnapMirror con la replica flessibile della versione, fare clic su **Avanzate** per attivare la replica flessibile della versione, quindi fare clic su **Applica**.

5. Fare clic su **Apply** (Applica).

   Viene visualizzata nuovamente la pagina dei dettagli relativi a volume/salute.

6. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della pagina dei dettagli **Volume / Health**.

   Le attività e i dettagli dei lavori vengono visualizzati nella pagina Dettagli lavoro.

7. Nella pagina dei dettagli **lavoro**, fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al lavoro di configurazione della protezione e per determinare quando il lavoro è completo.
8. Una volta completate le attività di lavoro, fare clic su **Indietro** nel browser per tornare alla pagina dei dettagli **Volume / Health**.

   La nuova relazione viene visualizzata nella vista topologia della pagina dei dettagli volume/salute.

Creazione di relazioni SnapMirror con replica flessibile della versione con opzione di backup

È possibile creare una relazione SnapMirror con funzionalità di replica e di backup flessibili per la versione. La funzione di opzione di backup consente di implementare la protezione SnapMirror e di conservare più versioni delle copie di backup nella posizione di destinazione.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.
- Le SVM di origine e di destinazione devono disporre di una licenza SnapMirror abilitata.
- Le SVM di origine e di destinazione devono disporre di una licenza SnapVault abilitata.
- Le SVM di origine e di destinazione devono essere eseguite con una versione del software ONTAP che supporti la replica flessibile dalla versione.

La configurazione di SnapMirror con funzionalità di opzione di backup consente di proteggere i dati con funzionalità di disaster recovery di SnapMirror, come la capacità di failover dei volumi, e allo stesso tempo fornisce funzionalità SnapVault, come la protezione di più copie di backup.

Fasi

1. Visualizzare la finestra di dialogo **Configura protezione** per il volume che si desidera proteggere.
   - Se si visualizza la scheda protezione della pagina Dettagli volume/stato di salute, fare clic con il pulsante destro del mouse nella topologia per visualizzare il nome di un volume che si desidera proteggere e selezionare **Protect** > **SnapMirror** dal menu.
   - Se si sta visualizzando la vista Health: All Volumes (Salute: Tutti i volumi), individuare il volume che si desidera proteggere e fare clic con il pulsante destro del mouse, quindi selezionare **Protect** > **SnapMirror** dal menu. Viene visualizzata la finestra di dialogo Configura protezione.
2. Fare clic su **SnapMirror** per visualizzare la scheda **SnapMirror**.

3. Completare l'area **Destination Information** (informazioni destinazione) e l'area **Relationship Settings** (Impostazioni relazione) nella finestra di dialogo **Configure Protection** (Configura protezione).
4. Fare clic su **Advanced** (Avanzate) per visualizzare la finestra di dialogo **Advanced Destination Settings** (Impostazioni di destinazione avanzate).
5. Se la casella di controllo **Version-Flexible Replication** non è già selezionata, selezionarla ora.
6. Selezionare la casella di controllo **con opzione di backup** per attivare la funzionalità di opzione di backup, quindi fare clic su **Applica**.
7. Fare clic su **Apply** (Applica).

   Viene visualizzata nuovamente la pagina dei dettagli relativi a volume/salute.

8. Fare clic sul collegamento al processo di configurazione della protezione nella parte superiore della pagina dei dettagli **Volume / Health**.

   Le attività e i dettagli dei lavori vengono visualizzati nella pagina Dettagli lavoro.

9. Nella pagina dei dettagli **lavoro**, fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al lavoro di configurazione della protezione e per determinare quando il lavoro è completo.
10. Una volta completate le attività di lavoro, fare clic su **Indietro** nel browser per tornare alla pagina dei dettagli **Volume / Health**.

    La nuova relazione viene visualizzata nella vista topologia della pagina dei dettagli volume/salute.

Configurazione delle impostazioni di efficienza della destinazione

È possibile configurare le impostazioni di efficienza della destinazione come deduplica, compressione, crescita automatica e garanzia di spazio su una destinazione di protezione utilizzando la finestra di dialogo Advanced Destination Settings (Impostazioni di destinazione avanzate). Queste impostazioni vengono utilizzate quando si desidera massimizzare l'utilizzo dello spazio su un volume di destinazione o secondario.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Per impostazione predefinita, le impostazioni di efficienza corrispondono a quelle del volume di origine, ad eccezione delle impostazioni di compressione in una relazione SnapVault, disattivate per impostazione predefinita.

Fasi

1. Fare clic sulla scheda **SnapMirror** o **SnapVault** nella finestra di dialogo **Configura protezione**, a seconda del tipo di relazione che si sta configurando.
2. Fare clic su **Advanced** (Avanzate) nell'area **Destination Information** (informazioni destinazione).

   Viene visualizzata la finestra di dialogo Advanced Destination Settings (Impostazioni di destinazione avanzate).

3. Attivare o disattivare le impostazioni di efficienza per deduplica, compressione, crescita automatica e garanzia di spazio, secondo necessità.

4. Fare clic su **Apply** (Applica) per salvare le selezioni e tornare alla finestra di dialogo **Configure Protection** (Configura protezione).

Creazione di pianificazioni SnapMirror e SnapVault

È possibile creare pianificazioni SnapMirror e SnapVault di base o avanzate per consentire trasferimenti automatici della protezione dei dati su un volume di origine o primario in modo che i trasferimenti vengano effettuati con maggiore frequenza o meno frequenza, a seconda della frequenza con cui i dati cambiano sui volumi.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver già completato l'area Destination Information (informazioni destinazione) nella finestra di dialogo Configure Protection (Configura protezione).
- Per eseguire questa attività, è necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Dalla scheda **SnapMirror** o **SnapVault** della finestra di dialogo **Configura protezione**, fare clic sul collegamento **Crea pianificazione** nell'area **Impostazioni relazione**.

   Viene visualizzata la finestra di dialogo Create Schedule (Crea pianificazione).

2. Nel campo **Nome pianificazione**, digitare il nome che si desidera assegnare alla pianificazione.
3. Selezionare una delle seguenti opzioni:
   - **Di base**

     Selezionare questa opzione se si desidera creare una pianificazione di base in stile intervallo.

   - **Avanzate**

     Selezionare se si desidera creare un programma in stile cron.

4. Fare clic su **Create** (Crea).

   La nuova pianificazione viene visualizzata nell'elenco a discesa Pianificazione SnapMirror o Pianificazione SnapVault.

Creazione di relazioni a cascata o fan-out per estendere la protezione da una relazione di protezione esistente

È possibile estendere la protezione da una relazione esistente creando un fanout dal volume di origine o una cascata dal volume di destinazione di una relazione esistente. Questa operazione può essere eseguita quando è necessario copiare i dati da un sito a più siti o per fornire una protezione aggiuntiva creando più backup.

È possibile estendere la protezione ai volumi utilizzando un gruppo di coerenza, un container che contiene diversi volumi in modo da poter gestire tutti i volumi come un'unica entità. Nella pagina Relazioni di Unified Manager è possibile visualizzare il gruppo di coerenza di SnapMirror Business Continuity (SM-BC) e la relazione del gruppo di coerenza sincrona.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Fare clic su **protezione** > **relazioni**. In alternativa, è possibile visualizzare le relazioni dalla pagina Dettagli volume.
2. Dalla pagina **Relazioni volume**, selezionare la relazione SnapMirror da cui si desidera estendere la protezione.
3. Sulla barra delle azioni, fare clic su **Estendi protezione**.
4. Nel menu, selezionare **da origine** o **da destinazione**, a seconda che si stia creando una relazione fanout dall'origine o una relazione a cascata dalla destinazione.
5. Selezionare **con SnapMirror** o **con SnapVault** a seconda del tipo di relazione di protezione che si sta creando.

   Viene visualizzata la finestra di dialogo **Configura protezione**.

   Ciò è possibile dalla pagina dei dettagli di rapporto unificato/rapporto volume e volume/salute.

6. Compilare le informazioni come indicato nella finestra di dialogo **Configura protezione**.

Modifica delle relazioni di protezione dalla pagina Relazioni volume

È possibile modificare le relazioni di protezione esistenti per modificare la velocità di trasferimento massima, la policy di protezione o la pianificazione della protezione. È possibile modificare una relazione per ridurre la larghezza di banda utilizzata per i trasferimenti o per aumentare la frequenza dei trasferimenti pianificati perché i dati cambiano spesso.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

I volumi selezionati devono essere destinazioni delle relazioni di protezione. Non è possibile modificare le relazioni quando sono selezionati volumi di origine, volumi di condivisione del carico o volumi che non sono la destinazione di una relazione SnapMirror o SnapVault.

Fasi

1. Nella pagina **Relazioni volume**, selezionare nell'elenco volumi uno o più volumi nella stessa SVM per cui si desidera modificare le impostazioni di relazione, quindi selezionare **Modifica** dalla barra degli strumenti.

   Viene visualizzata la finestra di dialogo Edit Relationship (Modifica relazione).

2. Nella finestra di dialogo **Edit Relationship** (Modifica relazione), modificare la velocità di trasferimento massima, la policy di protezione o la pianificazione di protezione, in base alle necessità.
3. Fare clic su **Apply** (Applica).

   Le modifiche vengono applicate alle relazioni selezionate.

Modifica delle relazioni di protezione dalla pagina Dettagli volume/salute

È possibile modificare le relazioni di protezione esistenti per modificare la velocità di trasferimento massima corrente, la policy di protezione o la pianificazione di protezione. È possibile modificare una relazione per ridurre la larghezza di banda utilizzata per i trasferimenti o per aumentare la frequenza dei trasferimenti pianificati perché i dati cambiano spesso.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver installato e configurato Workflow Automation.

I volumi selezionati devono essere destinazioni delle relazioni di protezione. Non è possibile modificare le relazioni quando sono selezionati volumi di origine, volumi di condivisione del carico o volumi che non sono la destinazione di una relazione SnapMirror o SnapVault.

Fasi

1. Dalla scheda **Protection** della pagina dei dettagli **Volume / Health**, individuare nella topologia la relazione di protezione che si desidera modificare e fare clic con il pulsante destro del mouse su di essa.
2. Selezionare **Edit** (Modifica) dal menu.

   In alternativa, dal menu **azioni**, selezionare **relazione** > **Modifica** per modificare la relazione per la quale si stanno visualizzando i dettagli.

   Viene visualizzata la finestra di dialogo **Modifica relazione**.
3. Nella finestra di dialogo Edit Relationship (Modifica relazione), modificare la velocità di trasferimento massima, la policy di protezione o la pianificazione di protezione, in base alle necessità.
4. Fare clic su **Apply** (Applica).

   Le modifiche vengono applicate alle relazioni selezionate.

Creazione di una policy SnapMirror per massimizzare l'efficienza del trasferimento

È possibile creare un criterio SnapMirror per specificare la priorità di trasferimento di SnapMirror per le relazioni di protezione. Le policy di SnapMirror consentono di massimizzare l'efficienza del trasferimento dall'origine alla destinazione assegnando priorità in modo che i trasferimenti a priorità inferiore vengano pianificati per essere eseguiti dopo i trasferimenti a priorità normale.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.
- Questa attività presuppone che l'area Destination Information (informazioni destinazione) sia già stata completata nella finestra di dialogo Configure Protection (Configura protezione).

Fasi

1. Dalla scheda **SnapMirror** della finestra di dialogo **Configura protezione**, fare clic sul collegamento **Crea policy** nell'area **Impostazioni relazione**.

   Viene visualizzata la finestra di dialogo Create SnapMirror Policy (Crea policy SnapMirror).

2. Nel campo **Policy Name** (Nome policy), digitare il nome che si desidera assegnare al criterio.
3. Nel campo **priorità trasferimento**, selezionare la priorità di trasferimento che si desidera assegnare al criterio.
4. Nel campo **Commento**, immettere un commento facoltativo per la policy.
5. Fare clic su **Create** (Crea).

   Il nuovo criterio viene visualizzato nell'elenco a discesa SnapMirror Policy (criterio SnapMirror).

Creazione di una policy SnapVault per massimizzare l'efficienza del trasferimento

È possibile creare un nuovo criterio SnapVault per impostare la priorità per un trasferimento SnapVault. Le policy vengono utilizzate per massimizzare l'efficienza dei trasferimenti dal primario al secondario in una relazione di protezione.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.
- È necessario aver già completato l'area Destination Information (informazioni destinazione) nella finestra di dialogo Configure Protection (Configura protezione).

Fasi

1. Dalla scheda **SnapVault** della finestra di dialogo **Configura protezione**, fare clic sul collegamento **Crea policy** nell'area **Impostazioni relazione**.

   Viene visualizzata la scheda SnapVault.

2. Nel campo **Policy Name**, digitare il nome che si desidera assegnare al criterio.
3. Nel campo **priorità trasferimento**, selezionare la priorità di trasferimento che si desidera assegnare al criterio.
4. **Opzionale:** nel campo **Commento**, inserire un commento per la policy.
5. Nell'area **Replication Label**, aggiungere o modificare un'etichetta di replica, se necessario.
6. Fare clic su **Create** (Crea).

   Il nuovo criterio viene visualizzato nell'elenco a discesa Crea criterio.

Interruzione di un trasferimento di protezione dei dati attivo dalla pagina Relazioni volume

È possibile interrompere un trasferimento di protezione dei dati attivo quando si desidera interrompere una replica SnapMirror in corso. È inoltre possibile cancellare il checkpoint di riavvio per i trasferimenti successivi al trasferimento di riferimento. È possibile

interrompere un trasferimento in caso di conflitto con un'altra operazione, ad esempio uno spostamento del volume.

Non è possibile interrompere le relazioni dei volumi protette dal gruppo di coerenza.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

L'azione di interruzione non viene visualizzata nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione: Ad esempio, se si dispone solo di privilegi operatore
- Quando l'ID del volume è sconosciuto: Ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato

Non è possibile cancellare il checkpoint di riavvio per un trasferimento di riferimento.

Fasi

1. Per interrompere i trasferimenti per una o più relazioni di protezione, dalla pagina **Relazioni volume**, selezionare uno o più volumi e, sulla barra degli strumenti, fare clic su **Interrompi**.

   Viene visualizzata la finestra di dialogo Interrompi trasferimento.

2. Se si desidera cancellare il checkpoint di riavvio per un trasferimento che non è un trasferimento di riferimento, selezionare **Clear Checkpoint**.
3. Fare clic su **continua**.

   La finestra di dialogo Interrompi trasferimento viene chiusa e lo stato del processo di interruzione viene visualizzato nella parte superiore della pagina Relazioni volume, insieme a un collegamento ai dettagli del processo.

4. **Opzionale:** fare clic sul collegamento **Visualizza dettagli** per accedere alla pagina **Dettagli lavoro** per ulteriori dettagli e per visualizzare l'avanzamento del lavoro.

Interruzione di un trasferimento di protezione dei dati attivo dalla pagina dei dettagli relativi a volume/salute

È possibile interrompere un trasferimento di protezione dei dati attivo quando si desidera interrompere una replica SnapMirror in corso. È inoltre possibile cancellare il checkpoint di riavvio per un trasferimento se non si tratta di un trasferimento di riferimento. È possibile interrompere un trasferimento in caso di conflitto con un'altra operazione, ad esempio uno spostamento del volume.

Non è possibile interrompere le relazioni dei volumi protette dal gruppo di coerenza.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

- È necessario aver impostato l'automazione del flusso di lavoro.

L'azione di interruzione non viene visualizzata nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione: Ad esempio, se si dispone solo di privilegi operatore
- Quando l'ID del volume è sconosciuto: Ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato

Non è possibile cancellare il checkpoint di riavvio per un trasferimento di riferimento.

Fasi

1. Nella scheda **Protection** della pagina dei dettagli **Volume / Health**, fare clic con il pulsante destro del mouse sulla relazione nella vista della topologia per il trasferimento dei dati che si desidera interrompere e selezionare **Abort** (Interrompi).

   Viene visualizzata la finestra di dialogo Interrompi trasferimento.

2. Se si desidera cancellare il checkpoint di riavvio per un trasferimento che non è un trasferimento di riferimento, selezionare **Clear Checkpoint**.
3. Fare clic su **continua**.

   La finestra di dialogo Interrompi trasferimento viene chiusa e lo stato dell'operazione di interruzione viene visualizzato nella parte superiore della pagina Dettagli volume/salute insieme a un link ai dettagli del lavoro.

4. **Opzionale:** fare clic sul collegamento **Visualizza dettagli** per accedere alla pagina **Dettagli lavoro** per ulteriori dettagli e per visualizzare l'avanzamento del lavoro.
5. Fare clic su ciascuna attività per visualizzarne i dettagli.
6. Fare clic sulla freccia Indietro del browser per tornare alla pagina dei dettagli **Volume / Health**.

   L'operazione di interruzione viene completata al termine di tutte le attività di lavoro.

Interrompere una relazione di protezione dalla pagina delle relazioni dei volumi

Dalla pagina Volume Relationship (Relazioni volume), è possibile interrompere una relazione di protezione per impedire temporaneamente il trasferimento dei dati. È possibile interrompere una relazione quando si desidera creare una copia Snapshot di un volume di destinazione SnapMirror che contiene un database e si desidera assicurarsi che il contenuto sia stabile durante l'operazione di copia Snapshot.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

L'azione di quiesce non viene visualizzata nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione, ad esempio se si dispone solo di privilegi operatore

- Quando l'ID del volume è sconosciuto, ad esempio quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato
- Se non si dispone dell'associazione tra Workflow Automation e Unified Manager

Fasi

1. Per interrompere i trasferimenti per una o più relazioni di protezione, dalla pagina **Relazioni volume**, selezionare uno o più volumi e, sulla barra degli strumenti, fare clic su **Quiesce**.

   Viene visualizzata la finestra di dialogo Quiesce.

2. Fare clic su **continua**.

   Lo stato del lavoro di quiete viene visualizzato nella parte superiore della pagina dei dettagli relativi a volume/salute, insieme a un collegamento ai dettagli del lavoro.

3. Fare clic sul collegamento **View details** (Visualizza dettagli) per accedere alla pagina **Job** Details (Dettagli lavoro) per ulteriori dettagli e avanzamento del lavoro.
4. **Opzionale:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina **Relazioni volume**.

   Il lavoro di quiesce viene terminato quando tutte le attività di lavoro vengono completate correttamente.

Interrompere una relazione di protezione dalla pagina dei dettagli relativi a volume/salute

È possibile interrompere una relazione di protezione per impedire temporaneamente il trasferimento dei dati. È possibile interrompere una relazione quando si desidera creare una copia Snapshot di un volume di destinazione SnapMirror che contiene un database e si desidera assicurarsi che il contenuto sia stabile durante la copia Snapshot.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

L'azione di quiesce non viene visualizzata nei seguenti casi:

- Se le impostazioni RBAC non consentono questa azione, ad esempio, se si dispone solo di privilegi operatore
- Quando l'ID del volume è sconosciuto, ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato
- Se non si dispone dell'associazione tra Workflow Automation e Unified Manager

Fasi

1. Nella scheda **Protection** della pagina dei dettagli **Volume / Health**, fare clic con il pulsante destro del mouse sulla relazione nella vista topologia per la relazione di protezione che si desidera interrompere.
2. Selezionare **Quiesce** dal menu.
3. Fare clic su **Sì** per continuare.

   Lo stato del lavoro di quiete viene visualizzato nella parte superiore della pagina dei dettagli relativi a volume/salute, insieme a un collegamento ai dettagli del lavoro.

4. Fare clic sul collegamento **View details** (Visualizza dettagli) per accedere alla pagina **Job** Details (Dettagli lavoro) per ulteriori dettagli e avanzamento del lavoro.
5. **Opzionale:** fare clic sulla freccia Indietro del browser per tornare alla pagina dei dettagli **Volume / Health**.

   Il lavoro di quiesce viene terminato quando tutte le attività di lavoro vengono completate correttamente.

Interruzione di una relazione SnapMirror dalla pagina Relazioni volume

È possibile interrompere una relazione di protezione per arrestare i trasferimenti di dati tra un volume di origine e un volume di destinazione in una relazione SnapMirror. È possibile interrompere una relazione quando si desidera migrare i dati, per il disaster recovery o per il test delle applicazioni. Il volume di destinazione viene modificato in un volume di lettura/scrittura. Non è possibile interrompere una relazione SnapVault.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Dalla pagina **Relazioni volume**, selezionare uno o più volumi con relazioni di protezione per i quali si desidera interrompere il trasferimento dei dati e, sulla barra degli strumenti, fare clic su **Interrompi**.

   Viene visualizzata la finestra di dialogo Interrompi relazione.

2. Fare clic su **continua** per interrompere la relazione.
3. Nella pagina **Volume Relationship**, verificare nella colonna **Relationship state** che la relazione sia interrotta.

   La colonna Relationship state (Stato relazione) è nascosta per impostazione predefinita, pertanto potrebbe essere necessario selezionarla nell'elenco show/hide column (Mostra/Nascondi colonna) .

Rimozione di una relazione di protezione dalla pagina Relazioni volume

Dalla pagina Relazioni volume, è possibile rimuovere una relazione di protezione per eliminare in modo permanente una relazione esistente tra l'origine e la destinazione selezionate, ad esempio quando si desidera creare una relazione utilizzando una destinazione diversa. Questa operazione rimuove tutti i metadati e non può essere annullata.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Dalla pagina **Relazioni volume**, selezionare uno o più volumi con relazioni di protezione da rimuovere e, sulla barra degli strumenti, fare clic su **Rimuovi**.

Viene visualizzata la finestra di dialogo Rimuovi relazione.

2. Fare clic su **continua** per rimuovere la relazione.

   La relazione viene rimossa dalla pagina Relazioni volume.

Ripresa dei trasferimenti pianificati su una relazione quiescente dalla pagina Volume Relationship (Relazioni volume)

Dopo aver interrotto una relazione per impedire il verificarsi di trasferimenti pianificati, è possibile utilizzare **Riprendi** per riattivare i trasferimenti pianificati in modo da proteggere i dati sul volume primario o di origine. I trasferimenti vengono ripristinati da un checkpoint, se presente, al successivo intervallo di trasferimento pianificato.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

È possibile selezionare non più di 10 relazioni in cui riprendere i trasferimenti.

Fasi

1. Dalla pagina Volume **Relointes** (Relazioni volume), selezionare uno o più volumi con relazioni in modalità di disattivazione e, sulla barra degli strumenti, fare clic su **Resume** (Riprendi).
2. Nella finestra di dialogo **Riprendi**, fare clic su **continua**.

   Viene visualizzata nuovamente la pagina Volume Relrelazione.

3. Per visualizzare le attività di lavoro correlate e monitorarne l'avanzamento, fare clic sul collegamento al lavoro visualizzato nella parte superiore della pagina **Relazioni volume**.
4. Effettuare una delle seguenti operazioni:
   - Se viene visualizzato un solo lavoro, nella pagina Dettagli lavoro fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al lavoro di configurazione della protezione e per determinare quando il lavoro è completo.
   - Se viene visualizzato più di un lavoro,
     i. Nella pagina lavori, fare clic sul lavoro per il quale si desidera visualizzare i dettagli.
     ii. Nella pagina Dettagli lavoro, fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al lavoro di configurazione della protezione e per determinare quando il lavoro è completo. Al termine dei lavori, i trasferimenti di dati vengono ripristinati al successivo intervallo di trasferimento pianificato.

Ripresa dei trasferimenti pianificati su una relazione quiescente dalla pagina dei dettagli relativi a volume/salute

Dopo aver interrotto una relazione per impedire il verificarsi di trasferimenti pianificati, è possibile utilizzare **Riprendi** nella pagina dei dettagli relativi a volume/salute per riabilitare i trasferimenti pianificati in modo da proteggere i dati sul volume di origine o primario. I trasferimenti vengono ripristinati da un checkpoint, se presente, al successivo

intervallo di trasferimento pianificato.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Nella scheda **Protection** della pagina dei dettagli **Volume / Health**, fare clic con il pulsante destro del mouse nella vista della topologia per visualizzare una relazione che si desidera riprendere.

   In alternativa, selezionare **Riprendi** dal menu **azioni** > **relazione**.

2. Nella finestra di dialogo **Riprendi**, fare clic su **continua**.

   Viene visualizzata nuovamente la pagina dei dettagli relativi a volume/salute.

3. Per visualizzare le attività di lavoro correlate e monitorarne l'avanzamento, fare clic sul collegamento visualizzato nella parte superiore della pagina dei dettagli **Volume / Health**.
4. Nella pagina dei dettagli **lavoro**, fare clic su **Aggiorna** per aggiornare l'elenco delle attività e i dettagli delle attività associati al lavoro di configurazione della protezione e per determinare quando il lavoro è completo.

   Una volta completati i lavori, i trasferimenti di dati vengono ripristinati al successivo intervallo di trasferimento pianificato.

Inizializzazione o aggiornamento delle relazioni di protezione dalla pagina Relazioni volume

Dalla pagina Volume Relationship (Relazioni volume), è possibile eseguire un primo trasferimento di riferimento su una nuova relazione di protezione o aggiornare una relazione se è già inizializzata e si desidera eseguire un aggiornamento incrementale manuale e non pianificato per il trasferimento immediato.

Non è possibile inizializzare o aggiornare i volumi protetti dai gruppi di coerenza.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver configurato OnCommand Workflow Automation.

Fasi

1. Nella pagina **Relazioni volume**, fare clic con il pulsante destro del mouse su un volume e selezionare uno o più volumi con relazioni che si desidera aggiornare o inizializzare, quindi fare clic su **Inizializza/Aggiorna** nella barra degli strumenti.

   Viene visualizzata la finestra di dialogo **Inizializza/Aggiorna**.

2. Nella scheda **Opzioni di trasferimento**, selezionare una priorità di trasferimento e la velocità di trasferimento massima.
3. Fare clic su **Source Snapshot Copies**, quindi nella colonna **Snapshot Copy**, fare clic su **Default**.

Viene visualizzata la finestra di dialogo Select Source Snapshot Copy (Seleziona copia snapshot di origine).

4. Se si desidera specificare una copia Snapshot esistente invece di trasferire la copia Snapshot predefinita, fare clic su **Existing Snapshot Copy** (Copia istantanea esistente) e selezionare una copia Snapshot dall'elenco.
5. Fare clic su **Invia**.

   Viene visualizzata nuovamente la finestra di dialogo **Inizializza/Aggiorna**.

6. Se sono state selezionate più origini da inizializzare o aggiornare, fare clic su **Default** per l'origine successiva per la quale si desidera specificare una copia Snapshot esistente.
7. Fare clic su **Submit** (Invia) per avviare il processo di inizializzazione o aggiornamento.

   Il processo di inizializzazione o aggiornamento viene avviato, viene visualizzata nuovamente la pagina rapporti volume e viene visualizzato un collegamento lavori nella parte superiore della pagina.

8. **Opzionale:** fare clic su **Visualizza processi** nella vista **Salute: Tutti i volumi** per tenere traccia dello stato di ogni processo di inizializzazione o di aggiornamento.

   Viene visualizzato un elenco filtrato di lavori.

9. **Opzionale:** fare clic su ciascun lavoro per visualizzarne i dettagli.
10. **Opzionale:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina **Relazioni volume**.

    Al termine di tutte le attività, l'operazione di inizializzazione o aggiornamento è terminata.

Inizializzazione o aggiornamento delle relazioni di protezione dalla pagina Dettagli volume/salute

È possibile eseguire un primo trasferimento baseline su una nuova relazione di protezione o aggiornare una relazione se è già inizializzata e si desidera eseguire un aggiornamento incrementale manuale e non pianificato per trasferire immediatamente i dati.

NOTA: Non è possibile inizializzare o aggiornare i volumi protetti dai gruppi di coerenza.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver configurato OnCommand Workflow Automation.

Fasi

1. Dalla scheda **Protection** della pagina dei dettagli **Volume / Health**, individuare nella topologia la relazione di protezione che si desidera inizializzare o aggiornare, quindi fare clic con il pulsante destro del mouse.
2. Selezionare **Inizializza/Aggiorna** dal menu.

   In alternativa, dal menu **azioni**, selezionare **relazione** > **Inizializza/Aggiorna** per inizializzare o aggiornare la relazione per la quale si stanno visualizzando i dettagli.

   Viene visualizzata la finestra di dialogo Inizializza/Aggiorna.

3. Nella scheda **Opzioni di trasferimento**, selezionare una priorità di trasferimento e la velocità di trasferimento massima.
4. Fare clic su **Source Snapshot Copies**, quindi nella colonna **Snapshot Copy**, fare clic su **Default**.

   Viene visualizzata la finestra di dialogo Select Source Snapshot Copy (Seleziona copia snapshot di origine).

5. Se si desidera specificare una copia Snapshot esistente invece di trasferire la copia Snapshot predefinita, fare clic su **Existing Snapshot Copy** (Copia istantanea esistente) e selezionare una copia Snapshot dall'elenco.
6. Fare clic su **Invia**.

   Viene visualizzata nuovamente la finestra di dialogo Inizializza/Aggiorna.

7. Se sono state selezionate più origini da inizializzare o aggiornare, fare clic su **Default** per la successiva origine di lettura/scrittura per la quale si desidera specificare una copia Snapshot esistente.

   Non è possibile selezionare una copia Snapshot diversa per i volumi di protezione dei dati.

8. Fare clic su **Submit** (Invia) per avviare il processo di inizializzazione o aggiornamento.

   Il processo di inizializzazione o aggiornamento viene avviato, viene visualizzata nuovamente la pagina dei dettagli relativi al volume/salute e viene visualizzato un collegamento ai processi nella parte superiore della pagina.

9. **Opzionale:** fare clic su **Visualizza processi** nella pagina dei dettagli **Volume / Health** per tenere traccia dello stato di ogni processo di inizializzazione o di aggiornamento.

   Viene visualizzato un elenco filtrato di lavori.

10. **Opzionale:** fare clic su ciascun lavoro per visualizzarne i dettagli.
11. **Opzionale:** fare clic sulla freccia Indietro del browser per tornare alla pagina dei dettagli **Volume / Health**.

    L'operazione di inizializzazione o aggiornamento viene completata al termine di tutte le attività del lavoro.

Risincronizzazione delle relazioni di protezione dalla pagina Relazioni volume

Dalla pagina Relazioni volume, è possibile risincronizzare una relazione per ripristinare da un evento che ha disattivato il volume di origine o quando si desidera modificare l'origine corrente in un volume diverso.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.

Fasi

1. Dalla pagina **Relazioni volume**, selezionare uno o più volumi con relazioni a quiete e, dalla barra degli strumenti, fare clic su **Risincronizza**.

   Viene visualizzata la finestra di dialogo risincronizza.

2. Nella scheda **Opzioni di risincronizzazione**, selezionare una priorità di trasferimento e la velocità di trasferimento massima.
3. Fare clic su **Source Snapshot Copies**, quindi nella colonna **Snapshot Copy**, fare clic su **Default**.

   Viene visualizzata la finestra di dialogo Select Source Snapshot Copy (Seleziona copia snapshot di origine).

4. Se si desidera specificare una copia Snapshot esistente invece di trasferire la copia Snapshot predefinita, fare clic su **Existing Snapshot Copy** (Copia istantanea esistente) e selezionare una copia Snapshot dall'elenco.
5. Fare clic su **Invia**.

   Viene visualizzata nuovamente la finestra di dialogo risincronizza.

6. Se sono state selezionate più origini da risincronizzare, fare clic su **Default** per l'origine successiva per la quale si desidera specificare una copia Snapshot esistente.
7. Fare clic su **Submit** (Invia) per avviare il processo di risincronizzazione.

   Viene avviato il processo di risincronizzazione, viene visualizzata la pagina rapporti volume e viene visualizzato un collegamento lavori nella parte superiore della pagina.

8. **Opzionale:** fare clic su **Visualizza processi** nella pagina **Relazioni volumi** per tenere traccia dello stato di ciascun processo di risincronizzazione.

   Viene visualizzato un elenco filtrato di lavori.

9. **Opzionale:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina **Relazioni volume**.

   L'operazione di risincronizzazione è terminata al termine di tutte le attività del lavoro.

Invertire le relazioni di protezione dalla pagina Relazioni volume

Quando un disastro disattiva il volume di origine nella relazione di protezione, è possibile utilizzare il volume di destinazione per fornire i dati convertendolo in un volume di lettura/scrittura durante la riparazione o la sostituzione dell'origine. Quando l'origine è nuovamente disponibile per ricevere i dati, è possibile utilizzare l'operazione di risincronizzazione inversa per stabilire la relazione nella direzione inversa, sincronizzando i dati sull'origine con i dati sulla destinazione di lettura/scrittura.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver impostato l'automazione del flusso di lavoro.
- La relazione non deve essere una relazione SnapVault.
- Una relazione di protezione deve già esistere.
- Il rapporto di protezione deve essere interrotto.
- Sia l'origine che la destinazione devono essere in linea.
- L'origine non deve essere la destinazione di un altro volume di protezione dei dati.

- Quando si esegue questa attività, i dati sull'origine più recenti dei dati sulla copia Snapshot comune vengono cancellati.
- Le policy e le pianificazioni create sulle relazioni di risincronizzazione inversa sono le stesse della relazione di protezione originale.

  Se le policy e le pianificazioni non esistono, vengono create.

Fasi

1. Dalla pagina **Relazioni volume**, selezionare uno o più volumi con relazioni da invertire e, sulla barra degli strumenti, fare clic su **Reverse Resync** (risincronizzazione inversa).

   Viene visualizzata la finestra di dialogo Reverse Resync (risincronizzazione inversa).

2. Verificare che le relazioni visualizzate nella finestra di dialogo **Reverse Resync** siano quelle per le quali si desidera eseguire l'operazione di risincronizzazione inversa, quindi fare clic su **Submit** (Invia).

   Viene avviata l'operazione di risincronizzazione inversa, viene visualizzata nuovamente la pagina rapporti volume e viene visualizzato un collegamento lavori nella parte superiore della pagina.

3. **Opzionale:** fare clic su **Visualizza processi** nella pagina **Relazioni volume** per tenere traccia dello stato di ciascun processo di risincronizzazione inversa.

   Viene visualizzato un elenco filtrato di lavori correlati a questa operazione.

4. **Opzionale:** fare clic sulla freccia **Indietro** del browser per tornare alla pagina **Relazioni volume**.

   L'operazione di risincronizzazione inversa viene completata al termine di tutte le attività del lavoro.

Ripristino dei dati mediante le pagine dei dettagli volume e volume/salute

È possibile ripristinare file, directory o un intero volume sovrascritti o cancellati da una copia Snapshot utilizzando la funzione di ripristino nelle pagine dei dettagli volume e volume/integrità.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Prendere nota dei seguenti punti:

- Non è possibile ripristinare i flussi di file NTFS.
- L'opzione di ripristino non è disponibile quando:
  - L'ID del volume è sconosciuto: Ad esempio, quando si dispone di una relazione tra cluster e il cluster di destinazione non è stato ancora rilevato.
  - Il volume viene configurato per la replica sincrona di SnapMirror.

Fasi

1. Dal riquadro di navigazione a sinistra, selezionare **Storage > Volumes** (archiviazione > volumi).
2. Selezionare il volume e fare clic sul pulsante **Restore** (Ripristina). In alternativa, fare clic sul volume per accedere a **Volume / Health details > Actions > Restore** (Dettagli volume/salute > azioni > Ripristino).

Viene visualizzata la finestra di dialogo Restore (Ripristino). Per informazioni su questa pagina, vedere "Finestra di dialogo Restore (Ripristina)".

3. Selezionare il volume e la copia Snapshot da cui si desidera ripristinare i dati, se diversi da quelli predefiniti.
4. Selezionare gli elementi da ripristinare, ad esempio il LUN di origine.

   È possibile ripristinare l'intero volume oppure specificare le cartelle e i file da ripristinare.

5. Selezionare la posizione in cui si desidera ripristinare gli elementi selezionati: **Posizione originale** o **posizione esistente alternativa**.
6. Se si seleziona una posizione esistente alternativa, effettuare una delle seguenti operazioni:
   - Nel campo di testo Restore Path (percorso di ripristino), digitare il percorso in cui si desidera ripristinare i dati, quindi fare clic su **Select Directory** (Seleziona directory).
   - Fare clic su **Browse** (Sfoglia) per aprire la finestra di dialogo Browse Directories (Sfoglia directory) e completare la seguente procedura:
     i. Selezionare il cluster di destinazione, la VM di storage (SVM) e il volume su cui si desidera eseguire il ripristino.
     ii. Nella tabella Name (Nome), selezionare un nome di directory da ripristinare.
     iii. Fare clic su **Select Directory** (Seleziona directory).
7. Fare clic su **Restore** (Ripristina).

   Viene avviato il processo di ripristino. Viene creato un lavoro nel back-end per completare il processo di ripristino.

8. Se si desidera visualizzare l'avanzamento del processo, dal riquadro di navigazione di sinistra, accedere a **protezione > processi** per visualizzare lo stato del processo di ripristino dall'elenco dei processi.

> Se un'operazione di ripristino tra cluster Cloud Volumes ONTAP HA non riesce con un errore NDMP, potrebbe essere necessario aggiungere una route AWS esplicita nel cluster di destinazione in modo che la destinazione possa comunicare con il LIF di gestione del cluster del sistema di origine. Per eseguire questa fase di configurazione, utilizzare la console NetApp .

Quali sono i pool di risorse

I pool di risorse sono gruppi di aggregati creati da un amministratore dello storage che utilizza Unified Manager per fornire il provisioning alle applicazioni partner per la gestione del backup.

È possibile raggruppare le risorse in base a attributi quali performance, costo, posizione fisica o disponibilità. Raggruppando le risorse correlate in un pool, è possibile trattare il pool come una singola unità per il monitoraggio e il provisioning. Ciò semplifica la gestione di queste risorse e consente un utilizzo dello storage più flessibile ed efficiente.

Durante il provisioning dello storage secondario, Unified Manager determina l'aggregato più adatto per la protezione nel pool di risorse utilizzando i seguenti criteri:

- L'aggregato è un aggregato di dati (non un aggregato root) ED è ONLINE.

- L’aggregato si trova su un nodo del cluster di destinazione la cui versione ONTAP è uguale o superiore alla versione principale del cluster di origine.
- L’aggregato dispone del più ampio spazio disponibile di tutti gli aggregati del pool di risorse.
- Dopo aver eseguito il provisioning del volume di destinazione, lo spazio aggregato rientra nella soglia quasi piena e quasi sovrascrivibile definita per l’aggregato (soglia globale o locale, a seconda di quale sia applicabile).
- Il numero di volumi FlexVol sul nodo di destinazione non deve superare il limite della piattaforma.

Creazione di pool di risorse

È possibile utilizzare la finestra di dialogo Crea pool di risorse per raggruppare gli aggregati a scopo di provisioning.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell’applicazione o di amministratore dello storage.

Fasi

I pool di risorse possono contenere aggregati di cluster diversi, ma lo stesso aggregato non può appartenere a pool di risorse diversi.

1. Nel riquadro di spostamento di sinistra, fare clic su **Protection** > **Resource Pools**.
2. Nella pagina **Resource Pools**, fare clic su **Create**.
3. Seguire le istruzioni nella finestra di dialogo **Crea pool di risorse** per fornire un nome e una descrizione e per aggiungere aggregati come membri al pool di risorse che si desidera creare.

Modifica dei pool di risorse

È possibile modificare un pool di risorse esistente quando si desidera modificare il nome e la descrizione del pool di risorse.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell’applicazione o di amministratore dello storage.

Il pulsante **Edit** (Modifica) viene attivato solo quando viene selezionato un pool di risorse. Se si seleziona più di un pool di risorse, il pulsante **Modifica** viene disattivato.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Protection** > **Resource Pools**.
2. Selezionare un pool di risorse dall’elenco.
3. Fare clic su **Edit** (Modifica).

   Viene visualizzata la finestra Edit Resource Pool (Modifica pool di risorse).

4. Modificare il nome e la descrizione del pool di risorse secondo necessità.
5. Fare clic su **Save** (Salva).

   Il nuovo nome e la nuova descrizione vengono visualizzati nell’elenco dei pool di risorse.

Visualizzazione dell'inventario dei pool di risorse

È possibile utilizzare la pagina Resource Pools per visualizzare l'inventario del pool di risorse e monitorare la capacità rimanente per ciascun pool di risorse.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fase

1. Nel riquadro di spostamento di sinistra, fare clic su **Protection** > **Resource Pools**.

   Viene visualizzato l'inventario del pool di risorse.

Aggiunta di membri del pool di risorse

Un pool di risorse è costituito da diversi aggregati di membri. È possibile aggiungere aggregati ai pool di risorse esistenti per aumentare la quantità di spazio disponibile per il provisioning di volumi secondari.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile aggiungere non più di 200 aggregati a un pool di risorse contemporaneamente. Gli aggregati visualizzati nella finestra di dialogo aggregati non appartengono ad altri pool di risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Protection** > **Resource Pools**.
2. Selezionare un pool di risorse dall'elenco **Resource Pools**.

   I membri del pool di risorse vengono visualizzati nell'area sotto l'elenco del pool di risorse.

3. Nell'area membro del pool di risorse, fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo aggregati.

4. Selezionare uno o più aggregati.
5. Fare clic su **Aggiungi**.

   La finestra di dialogo viene chiusa e gli aggregati vengono visualizzati nell'elenco dei membri per il pool di risorse selezionato.

Rimozione di aggregati dai pool di risorse

È possibile rimuovere gli aggregati da un pool di risorse esistente, ad esempio quando si desidera utilizzare un aggregato per altri scopi.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

I membri del pool di risorse vengono visualizzati solo quando viene selezionato un pool di risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Protection** > **Resource Pools**.
2. Selezionare il pool di risorse da cui si desidera rimuovere gli aggregati dei membri.

   L'elenco degli aggregati dei membri viene visualizzato nel pannello membri.

3. Selezionare uno o più aggregati.

   Il pulsante **Remove** (Rimuovi) è attivato.

4. Fare clic su **Rimuovi.**

   Viene visualizzata una finestra di dialogo di avviso.

5. Fare clic su **Sì** per continuare.

   Gli aggregati selezionati vengono rimossi dal pannello membri.

Eliminazione dei pool di risorse

È possibile eliminare i pool di risorse quando non sono più necessari. Ad esempio, è possibile ridistribuire gli aggregati dei membri da un pool di risorse a diversi altri pool di risorse, rendendo obsoleto il pool di risorse originale.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Il pulsante **Delete** (Elimina) è attivato solo quando è selezionato almeno un pool di risorse.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Protection** > **Resource Pools**.
2. Selezionare il pool di risorse che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).

   Il pool di risorse viene rimosso dall'elenco dei pool di risorse e i relativi aggregati vengono rimossi dall'elenco dei membri.

Monitoraggio delle relazioni di protezione di Storage VM Disaster Recovery

Active IQ Unified Manager supporta il monitoraggio delle relazioni di disaster recovery delle macchine virtuali dello storage, che offre disaster recovery alla granularità di un livello di storage VM. Il disaster recovery delle macchine virtuali dello storage consente il ripristino dei dati presenti nei volumi costitutivi della macchina virtuale dello storage e il ripristino della configurazione delle macchine virtuali dello storage.

Viene creata una relazione di DR tra la VM dello storage di origine e la VM dello storage di destinazione per fornire un disaster recovery asincrono. È possibile scegliere di replicare tutto o un sottoinsieme della

configurazione della macchina virtuale dello storage (esclusa la configurazione di rete e del protocollo) insieme ai volumi di dati in base all'impostazione del cluster.

Una volta configurata la relazione di disaster recovery per le macchine virtuali di storage, quando la macchina virtuale di storage di origine diventa non disponibile a causa di un guasto hardware o di un disastro ambientale, viene avviata la macchina virtuale di storage di destinazione, che fornisce accesso ai dati con la minima interruzione. Allo stesso modo, quando la VM di storage di origine diventa disponibile, viene risincronizzata con la VM di storage di destinazione, quindi l'origine viene riavviata per fornire i dati. È possibile utilizzare i comandi di SnapMirror per configurare e gestire la relazione di disaster recovery delle macchine virtuali dello storage.

Pagina Monitoring Storage VM Using Relinters (monitoraggio delle VM di storage

È possibile monitorare le relazioni di disaster recovery delle macchine virtuali dello storage dalla pagina delle relazioni nella sezione RELATIVA ALLA PROTEZIONE dell'INVENTARIO. Per impostazione predefinita, la pagina delle relazioni elenca solo le relazioni di primo livello quando viene applicato il filtro delle relazioni costitutive.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

I filtri vengono utilizzati per visualizzare le relazioni di disaster recovery delle macchine virtuali dello storage.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **PROTECTION** > **Relation**.

   La pagina visualizza tutti i tipi di relazioni: Volume, gruppo di coerenza e relazioni delle macchine virtuali di storage.

2. Fare clic su **Filter**, quindi selezionare **Relationship Object Type** e **Storage VM** per visualizzare solo le relazioni di disaster recovery delle macchine virtuali di storage.
3. Fare clic su **Applica filtro**.

   > È necessario deselezionare il filtro delle relazioni costitutive per visualizzare tutte le relazioni di protezione.

   La pagina visualizza solo le relazioni di disaster recovery delle macchine virtuali dello storage.

Visualizzazione delle relazioni di protezione dalla pagina Storage VM

Utilizzando la pagina Storage VM, è possibile visualizzare lo stato delle relazioni di disaster recovery delle macchine virtuali di storage esistenti`.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Puoi anche esaminare i dettagli delle relazioni di protezione, tra cui lo stato di trasferimento e ritardo, l'origine e i dettagli di destinazione. È possibile pianificare i report o scaricare quelli esistenti nel formato richiesto. Il pulsante **Mostra/Nascondi** consente di aggiungere le colonne richieste ai report, in quanto non vengono visualizzate per impostazione predefinita.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **STORAGE** > **Storage VM**.
2. Dal menu **VIEW**, selezionare **relazione** > **tutte le relazioni**.

   La vista relazione: Tutte le relazioni viene visualizzata con tutte le VM di storage configurate.

Visualizzazione delle VM di storage in base allo stato di protezione

È possibile utilizzare la pagina Storage VM dell'inventario per visualizzare tutte le VM di storage in Active IQ Unified Manager e filtrare le VM di storage in base al loro stato di protezione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Alla vista delle VM di storage viene aggiunto un nuovo ruolo di Column Protection che fornisce informazioni sulla protezione o meno della VM di storage.

Se un cluster di origine non viene aggiunto a Active IQ Unified Manager, tutte le informazioni relative a tale cluster non saranno disponibili nelle griglie.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **STORAGE** > **Storage VM**.
2. Dal menu **VIEW**, selezionare **Health** > **All Storage VMS**.

   Viene visualizzato il messaggio Health: All Storage VM (Stato: Tutte le macchine virtuali storage).

3. Fare clic su **Filter** (filtro) per visualizzare una delle seguenti macchine virtuali storage.

Per visualizzare	Valore del filtro
VM storage protette	**Ruolo di protezione protetto**
VM di storage non protette	**Ruolo di protezione non protetto**

Non è possibile visualizzare contemporaneamente le VM di storage protette e non protette. Per riapplicare un nuovo filtro, è necessario deselezionare il filtro esistente.

4. Fare clic su **Applica filtro**.

   La vista non salvata visualizza tutte le VM di storage protette o non protette dal disaster recovery delle VM di storage in base alle selezioni dei filtri.

Informazioni sulle associazioni di Storage VM

Le associazioni delle macchine virtuali di storage (VM di storage) sono mappature da una VM di storage di origine a una VM di storage di destinazione utilizzate dalle applicazioni partner per la selezione delle risorse e il provisioning di volumi secondari.

Vengono create associazioni tra una VM di storage di origine e una VM di storage di destinazione, indipendentemente dal fatto che la VM di storage di destinazione sia una destinazione secondaria o una destinazione terziaria. Non è possibile utilizzare una VM di storage di destinazione secondaria come origine per creare un'associazione con una VM di storage di destinazione terziaria.

In qualità di amministratore dell'applicazione o amministratore dello storage, è possibile visualizzare le associazioni delle macchine virtuali dello storage nel proprio ambiente nella pagina **protezione** > **Associazioni delle macchine virtuali dello storage**.

È possibile associare le SVM in tre modi:

- **Associa qualsiasi VM di storage**: Puoi creare un'associazione tra qualsiasi VM di storage di origine primaria e una o più SVM di destinazione. Ciò significa che tutte le SVM esistenti che attualmente richiedono protezione, nonché tutte le SVM create in futuro, sono associate alle SVM di destinazione specificate. Ad esempio, è possibile che venga eseguito il backup di applicazioni provenienti da diverse origini in posizioni diverse su una o più SVM di destinazione in un'unica posizione.
- **Associare una particolare VM di storage**: È possibile creare un'associazione tra una specifica VM di storage di origine e una o più SVM di destinazione specifiche. Ad esempio, se si forniscono servizi di storage a molti client i cui dati devono essere separati l'uno dall'altro, è possibile scegliere questa opzione per associare una specifica VM di storage di origine a una specifica VM di storage di destinazione assegnata solo a quel client.
- **Associare una VM di storage esterna**: È possibile creare un'associazione tra una VM di storage di origine e un volume flessibile esterno di una VM di storage di destinazione.

Creare associazioni di storage VM

La procedura guidata Crea associazioni di macchine virtuali di storage consente alle applicazioni di protezione dei partner di associare una macchina virtuale di storage di origine a una macchina virtuale di storage di destinazione da utilizzare con le relazioni SnapMirror e SnapVault. Le applicazioni partner utilizzano queste associazioni al momento del provisioning iniziale dei volumi di destinazione per determinare le risorse da selezionare.dd

Cosa ti serve

- La VM di storage che si sta associando deve già esistere.
- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Per qualsiasi tipo di relazione e VM di storage di origine, è possibile scegliere una sola VM di storage di destinazione per ogni cluster di destinazione.

La modifica delle associazioni che utilizzano le funzioni di eliminazione e creazione influisce solo sulle future operazioni di provisioning. Non sposta i volumi di destinazione esistenti.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **protezione** > **Storage VM Associations**.
2. Nella pagina **Storage VM Associations**, fare clic su **Create** (Crea).

   Viene avviata la procedura guidata **Create Storage Virtual Machine Associations**.

3. Selezionare una delle seguenti fonti:
   - **Qualsiasi**

     Scegliere questa opzione per creare un'associazione tra un'origine VM di storage primario e una o più

VM di storage di destinazione. Ciò significa che tutte le VM di storage esistenti che richiedono attualmente la protezione, nonché tutte le VM di storage create in futuro, sono associate alla VM di storage di destinazione specificata. Ad esempio, è possibile eseguire il backup di applicazioni provenienti da diverse origini in posizioni diverse su una o più macchine virtuali di storage di destinazione in un'unica posizione.

- **Singolo**

  Scegliere questa opzione se si desidera selezionare una VM storage di origine specifica associata a una o più VM storage di destinazione. Ad esempio, se si forniscono servizi di storage a molti client i cui dati devono essere separati l'uno dall'altro, scegliere questa opzione per associare una specifica origine della VM di storage a una specifica destinazione della VM di storage assegnata solo a quel client.

- **Nessuno (esterno)**

  Scegliere questa opzione per creare un'associazione tra una VM di storage di origine e un volume flessibile esterno di una VM di storage di destinazione.

4. Selezionare uno o entrambi i tipi di relazione di protezione che si desidera creare:
   - **SnapMirror**
   - **SnapVault**
5. Fare clic su **Avanti**.
6. Selezionare una o più destinazioni di protezione delle VM di storage.
7. Fare clic su **fine**.

Eliminare le associazioni di storage VM

È possibile eliminare le associazioni delle macchine virtuali di storage per le applicazioni partner per rimuovere la relazione di provisioning secondario tra le macchine virtuali di storage di origine e di destinazione; ad esempio, è possibile farlo quando la macchina virtuale di storage di destinazione è piena e si desidera creare nuove associazioni di protezione delle macchine virtuali di storage.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Il pulsante **Delete** (Elimina) viene disattivato fino a quando non viene selezionata almeno un'associazione di storage VM. La modifica delle associazioni che utilizzano le funzioni di eliminazione e creazione influisce solo sulle future operazioni di provisioning e non sposta i volumi di destinazione esistenti.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **protezione** > **Storage VM Associations**.
2. Selezionare almeno un'associazione di storage VM.

   Il pulsante **Delete** (Elimina) è attivato.

3. Fare clic su **Delete.** (Elimina)

   Viene visualizzata una finestra di dialogo di avviso.

4. Fare clic su **Sì** per continuare.

L’associazione delle macchine virtuali di storage selezionate viene rimossa dall’elenco.

Requisiti di SVM e pool di risorse per supportare i servizi di storage

È possibile garantire meglio la conformità nelle applicazioni dei partner se si osservano alcuni requisiti di associazione SVM e del pool di risorse specifici per i servizi di storage: Ad esempio, quando si associa SVM e si creano pool di risorse in Unified Manager per supportare una topologia di protezione in un servizio di storage fornito da un’applicazione partner.

Alcune applicazioni collaborano con il server Unified Manager per fornire servizi che configurano ed eseguono automaticamente la protezione di backup SnapMirror o SnapVault tra volumi di origine e volumi di protezione in ubicazioni secondarie o terziarie. Per supportare questi servizi storage di protezione, è necessario utilizzare Unified Manager per configurare le associazioni SVM e i pool di risorse necessari.

Per supportare la protezione single-hop o a cascata del servizio di storage, inclusa la replica da un volume principale SnapMirror o SnapVault di origine a SnapMirror di destinazione o a volumi di backup SnapVault che risiedono in ubicazioni secondarie o terziarie, attenersi ai seguenti requisiti:

- Le associazioni SVM devono essere configurate tra la SVM contenente l’origine SnapMirror o il volume primario SnapVault e qualsiasi SVM su cui risiede un volume secondario o un volume terzo.
  - Ad esempio, per supportare una topologia di protezione in cui il volume di origine Vol_A risiede su SVM_1 e il volume di destinazione secondario SnapMirror Vol_B risiede su SVM_2, E il volume di backup SnapVault terzo Vol_ C risiede su SVM_3, è necessario utilizzare l’interfaccia utente Web di Unified Manager per configurare un’associazione SnapMirror tra SVM_1 e SVM_2 e un’associazione di backup SnapVault tra SVM_1 e SVM_3.

    In questo esempio, qualsiasi associazione di backup SnapMirror o SnapVault tra SVM_2 e SVM_3 non è necessaria e non viene utilizzata.

  - Per supportare una topologia di protezione in cui il volume di origine Vol_A e il volume di destinazione SnapMirror Vol_B risiedono su SVM_1, è necessario configurare un’associazione SnapMirror tra SVM_1 e SVM_1.
- I pool di risorse devono includere le risorse aggregate del cluster disponibili per le SVM associate.

  È possibile configurare i pool di risorse tramite l’interfaccia utente Web di Unified Manager, quindi assegnare tramite l’applicazione partner la destinazione secondaria del servizio di storage e i nodi di destinazione terziari.

Quali sono i posti di lavoro

Un lavoro è una serie di attività che è possibile monitorare utilizzando Unified Manager. La visualizzazione dei job e delle attività associate consente di determinare se sono stati completati correttamente.

I lavori vengono avviati quando si creano relazioni SnapMirror e SnapVault, quando si eseguono operazioni di relazione (interruzione, modifica, interruzione, rimozione, ripresa, risincronizzare e risincronizzare all’inverso), quando si eseguono attività di ripristino dei dati, quando si accede a un cluster e così via.

Quando si avvia un lavoro, è possibile utilizzare la pagina lavori e la pagina Dettagli lavoro per monitorare il lavoro e l’avanzamento delle attività associate.

Monitoraggio dei lavori

È possibile utilizzare la pagina lavori per monitorare lo stato del lavoro e visualizzare le proprietà del lavoro, ad esempio il tipo di servizio di storage, lo stato, l'ora di inoltro e il tempo di completamento, per determinare se un lavoro è stato completato correttamente.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **protezione** > **lavori**.

   Viene visualizzata la pagina lavori.

2. Visualizzare la colonna **Stato** per determinare lo stato dei job attualmente in esecuzione.
3. Fare clic sul nome di un lavoro per visualizzare i dettagli relativi a tale lavoro.

   Viene visualizzata la pagina Dettagli lavoro.

Visualizzazione dei dettagli del lavoro

Dopo aver avviato un lavoro, è possibile monitorarne l'avanzamento dalla pagina Dettagli lavoro e monitorare le attività associate per individuare eventuali errori.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **protezione** > **lavori**.
2. Nella pagina lavori, fare clic sul nome di un lavoro nella colonna **Nome** per visualizzare l'elenco delle attività associate al lavoro.
3. Fare clic su un'attività per visualizzare ulteriori informazioni nel riquadro **Dettagli attività** e nel riquadro **messaggi attività** a destra dell'elenco attività.

Interruzione dei lavori

È possibile utilizzare la pagina lavori per interrompere un lavoro se il completamento del lavoro richiede troppo tempo, se si verificano troppi errori o se non è più necessario. È possibile interrompere un lavoro solo se lo stato e il tipo lo consentono. È possibile interrompere qualsiasi processo in esecuzione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **protezione** > **lavori**.

2. Dall'elenco dei job, selezionare un job, quindi fare clic su **Interrompi**.
3. Alla richiesta di conferma, fare clic su **Sì** per interrompere il lavoro selezionato.

Tentativo di nuovo di un processo di protezione non riuscito

Una volta adottate le misure necessarie per correggere un processo di protezione non riuscito, è possibile utilizzare **Riprova** per eseguire nuovamente il processo. Il nuovo tentativo di un lavoro crea un nuovo lavoro utilizzando l'ID lavoro originale.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile riprovare solo un processo non riuscito alla volta. Selezionando più di un lavoro, il pulsante **Riprova** viene disattivato. È possibile eseguire un nuovo processo solo per i job del tipo Configurazione protezione e relazione protezione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **protezione** > **lavori**.
2. Dall'elenco dei job, selezionare un singolo job di tipo operazione di configurazione di protezione o relazione di protezione non riuscita.

   Il pulsante **Riprova** è attivato.

3. Fare clic su **Riprova**.

   Il lavoro viene riavviato.

Descrizione delle finestre di dialogo e delle relazioni di protezione

È possibile visualizzare e gestire dettagli relativi alla protezione, ad esempio pool di risorse, associazioni SVM e processi di protezione. È possibile utilizzare la pagina soglie di integrità appropriata per configurare i valori delle soglie di integrità globali per aggregati, volumi e relazioni.

Pagina dei pool di risorse

La pagina Resource Pools visualizza i pool di risorse esistenti e i relativi membri e consente di creare, monitorare e gestire i pool di risorse a scopo di provisioning.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Crea**

  Apre la finestra di dialogo Crea pool di risorse, che è possibile utilizzare per creare pool di risorse.

- **Modifica**

  Consente di modificare il nome e la descrizione dei pool di risorse creati.

- **Elimina**

  Consente di eliminare uno o più pool di risorse.

Elenco dei pool di risorse

L'elenco dei pool di risorse visualizza (in formato tabulare) le proprietà dei pool di risorse esistenti.

- **Pool di risorse**

  Visualizza il nome del pool di risorse.

- **Descrizione**

  Descrive il pool di risorse.

- **Tipo SnapLock**

  Visualizza il tipo di SnapLock utilizzato dagli aggregati nel pool di risorse. I valori validi per il tipo di SnapLock sono Compliance, Enterprise e non SnapLock. Un pool di risorse può contenere aggregati di un solo tipo di SnapLock.

- **Capacità totale**

  Visualizza la capacità totale (in MB, GB e così via) del pool di risorse.

- **Capacità utilizzata**

  Visualizza la quantità di spazio (in MB, GB e così via) utilizzata nel pool di risorse.

- **Capacità disponibile**

  Visualizza la quantità di spazio (in MB, GB e così via) disponibile nel pool di risorse.

- **Utilizzato %**

  Visualizza la percentuale di spazio utilizzata nel pool di risorse.

I membri elencano i pulsanti di comando

I pulsanti di comando dell'elenco membri consentono di eseguire le seguenti operazioni:

- **Aggiungi**

  Consente di aggiungere membri al pool di risorse.

- **Elimina**

  Consente di eliminare uno o più membri dal pool di risorse.

Elenco dei membri

L'elenco membri visualizza (in formato tabulare) i membri del pool di risorse e le relative proprietà quando viene selezionato un pool di risorse.

- **Stato**

  Visualizza lo stato corrente dell'aggregato di membri. Lo stato può essere critico ( ), errore ( ), Avviso ( ), o normale ( ).

- **Nome aggregato**

  Visualizza il nome dell'aggregato di membri.

- **Stato**

  Visualizza lo stato corrente dell'aggregato, che può essere uno dei seguenti:

  - Offline

    Non è consentito l'accesso in lettura o scrittura.

  - Online

    È consentito l'accesso in lettura e scrittura ai volumi ospitati su questo aggregato.

  - Limitato

    Sono consentite operazioni limitate (come la ricostruzione della parità), ma non è consentito l'accesso ai dati.

  - Creazione in corso

    L'aggregato è in fase di creazione.

  - Distruggere

    L'aggregato viene distrutto.

  - Non riuscito

    L'aggregato non può essere portato online.

  - Congelato

    L'aggregato (temporaneamente) non fornisce richieste.

  - Incoerente

    L'aggregato è stato contrassegnato come corrotto; contattare il supporto tecnico.

  - Ferro limitato

    Gli strumenti di diagnostica non possono essere eseguiti sull'aggregato.

  - Montaggio

    L'aggregato è in fase di montaggio.

  - Parziale

È stato trovato almeno un disco per l'aggregato, ma mancano due o più dischi.

- Quiescing

  L'aggregato viene messo a punto.

- A Quiesced

  L'aggregato viene messo a punto.

- Invertito

  Il revert di un aggregato è stato completato.

- Non montato

  L'aggregato è stato dismontato.

- Smontaggio

  L'aggregato viene portato offline.

- Sconosciuto

  L'aggregato viene rilevato, ma le informazioni aggregate non vengono ancora recuperate dal server Unified Manager.

Per impostazione predefinita, questa colonna è nascosta.

- **Cluster**

  Visualizza il nome del cluster a cui appartiene l'aggregato.

- Nodo *

  Visualizza il nome del nodo su cui risiede l'aggregato.

- **Capacità totale**

  Visualizza la capacità totale (in MB, GB e così via) dell'aggregato.

- **Capacità utilizzata**

  Visualizza la quantità di spazio (in MB, GB e così via) utilizzata nell'aggregato.

- **Capacità disponibile**

  Visualizza la quantità di spazio (in MB, GB e così via) disponibile nell'aggregato.

- **Utilizzato %**

  Visualizza la percentuale di spazio utilizzata nell'aggregato.

- **Tipo di disco**

  Visualizza il tipo di configurazione RAID, che può essere uno dei seguenti:

- RAID0: Tutti i gruppi RAID sono di tipo RAID0.
- RAID4: Tutti i gruppi RAID sono di tipo RAID4.
- RAID-DP: Tutti i gruppi RAID sono di tipo RAID-DP.
- RAID-TEC: Tutti i gruppi RAID sono di tipo RAID-TEC.
- RAID misto: L'aggregato contiene gruppi RAID di diversi tipi RAID (RAID0, RAID4, RAID-DP e RAID-TEC). Per impostazione predefinita, questa colonna è nascosta.

Finestra di dialogo Crea pool di risorse

È possibile utilizzare la finestra di dialogo Crea pool di risorse per assegnare un nome a un nuovo pool di risorse e per aggiungere aggregati ed eliminare aggregati da tale pool di risorse.

Nome pool di risorse

Le caselle di testo consentono di aggiungere le seguenti informazioni per creare un pool di risorse:

Consente di specificare un nome di pool di risorse.

Descrizione

Consente di descrivere un pool di risorse.

Membri

Visualizza i membri del pool di risorse. Puoi anche aggiungere ed eliminare membri.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Aggiungi**

  Apre la finestra di dialogo aggregati, che consente di aggiungere aggregati da un cluster specifico al pool di risorse. È possibile aggiungere aggregati da cluster diversi, ma gli stessi aggregati non possono essere aggiunti a più di un pool di risorse.

- **Rimuovi**

  Consente di rimuovere gli aggregati selezionati dal pool di risorse.

- **Crea**

  Crea il pool di risorse. Questo pulsante non viene attivato fino a quando non vengono inserite informazioni nei campi Nome pool di risorse o Descrizione.

- **Annulla**

  Elimina le modifiche e chiude la finestra di dialogo Crea pool di risorse.

Finestra di dialogo Edit Resource Pool

È possibile utilizzare la finestra di dialogo Modifica pool di risorse per modificare il nome e la descrizione di un pool di risorse esistente. Ad esempio, se il nome e la descrizione originali sono imprecisi o non corretti, è possibile modificarli in modo che siano più precisi.

Caselle di testo

Le caselle di testo consentono di modificare le seguenti informazioni per il pool di risorse selezionato:

- **Nome pool di risorse**

  Consente di immettere un nuovo nome.

- **Descrizione**

  Consente di inserire una nuova descrizione.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Salva**

  Salva le modifiche apportate al nome e alla descrizione del pool di risorse.

- **Annulla**

  Elimina le modifiche e chiude la finestra di dialogo Modifica pool di risorse.

Finestra di dialogo aggregati

È possibile utilizzare la finestra di dialogo aggregati per selezionare gli aggregati che si desidera aggiungere al pool di risorse.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Aggiungi**

  Aggiunge gli aggregati selezionati al pool di risorse. Il pulsante Add (Aggiungi) non viene attivato fino a quando non viene selezionato almeno un aggregato.

- **Annulla**

  Elimina le modifiche e chiude la finestra di dialogo aggregati.

Elenco aggregati

L'elenco aggregati visualizza (in formato tabulare) i nomi e le proprietà degli aggregati monitorati.

- **Stato**

  Visualizza lo stato corrente di un volume. Lo stato può essere critico ( ), errore ( ), Avviso ( ), o normale ( ).

  È possibile spostare il puntatore sullo stato per visualizzare ulteriori informazioni sull'evento o sugli eventi generati per il volume.

- **Nome aggregato**

  Visualizza il nome dell'aggregato.

- **Stato**

  Visualizza lo stato corrente dell'aggregato, che può essere uno dei seguenti:

  - Offline

    Non è consentito l'accesso in lettura o scrittura.

  - Limitato

    Sono consentite operazioni limitate (come la ricostruzione della parità), ma non è consentito l'accesso ai dati.

  - Online

    È consentito l'accesso in lettura e scrittura ai volumi ospitati su questo aggregato.

  - Creazione in corso

    L'aggregato è in fase di creazione.

  - Distruggere

    L'aggregato viene distrutto.

  - Non riuscito

    L'aggregato non può essere portato online.

  - Congelato

    L'aggregato (temporaneamente) non fornisce richieste.

  - Incoerente

    L'aggregato è stato contrassegnato come corrotto; contattare il supporto tecnico.

  - Ferro limitato

    Gli strumenti di diagnostica non possono essere eseguiti sull'aggregato.

  - Montaggio

    L'aggregato è in fase di montaggio.

- Parziale

  È stato trovato almeno un disco per l'aggregato, ma mancano due o più dischi.

- Quiescing

  L'aggregato viene messo a punto.

- A Quiesced

  L'aggregato viene messo a punto.

- Invertito

  Il revert di un aggregato è stato completato.

- Non montato

  L'aggregato non è in linea.

- Smontaggio

  L'aggregato viene portato offline.

- Sconosciuto

  L'aggregato viene rilevato, ma le informazioni aggregate non vengono ancora recuperate dal server Unified Manager.

- **Cluster**

  Visualizza il nome del cluster in cui risiede l'aggregato.

- Nodo *

  Visualizza il nome dello storage controller che contiene l'aggregato.

- **Capacità totale**

  Visualizza le dimensioni totali dei dati (in MB, GB e così via) dell'aggregato. Per impostazione predefinita, questa colonna è nascosta.

- **Capacità impegnata**

  Visualizza lo spazio totale (in MB, GB e così via) impegnato per tutti i volumi nell'aggregato. Per impostazione predefinita, questa colonna è nascosta.

- **Capacità utilizzata**

  Visualizza la quantità di spazio (in MB, GB e così via) utilizzata nell'aggregato.

- **Capacità disponibile**

  Visualizza la quantità di spazio (in MB, GB e così via) disponibile per i dati nell'aggregato. Per impostazione predefinita, questa colonna è nascosta.

- **Disponibile %**

  Visualizza la percentuale di spazio disponibile per i dati nell'aggregato. Per impostazione predefinita, questa colonna è nascosta.

- **Utilizzato %**

  Visualizza la percentuale di spazio utilizzata dai dati nell'aggregato.

- **Tipo RAID**

  Visualizza il tipo di RAID del volume selezionato. Il tipo di RAID può essere RAID0, RAID4, RAID-DP, RAID-TEC o RAID misto.

Pagina lavori

La pagina lavori consente di visualizzare lo stato corrente e altre informazioni su tutti i processi di protezione delle applicazioni partner attualmente in esecuzione, nonché i processi completati. È possibile utilizzare queste informazioni per verificare quali lavori sono ancora in esecuzione e se un lavoro ha avuto esito positivo o negativo.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Interrompi**

  Interrompe il lavoro selezionato. Questa opzione è disponibile solo se il processo selezionato è in esecuzione.

- **Riprova**

  Riavvia un processo non riuscito di tipo Configurazione protezione o operazione relazione protezione. È possibile riprovare solo un processo non riuscito alla volta. Se vengono selezionati più processi non riusciti, il pulsante **Riprova** viene disattivato. Non è possibile riprovare i processi del servizio di storage non riusciti.

- **Aggiorna**

  Aggiorna l'elenco dei job e le informazioni ad essi associate.

Elenco dei job

L'elenco lavori visualizza, in formato tabulare, un elenco dei lavori in corso. Per impostazione predefinita, l'elenco visualizza solo i lavori generati nell'ultima settimana. È possibile utilizzare l'ordinamento e il filtraggio delle colonne per personalizzare i lavori da visualizzare.

- **Stato**

  Visualizza lo stato corrente di un lavoro. Lo stato può essere Error (⚠️) O normale (✅).

- **ID lavoro**

  Visualizza il numero di identificazione del lavoro. Per impostazione predefinita, questa colonna è nascosta.

Il numero di identificazione del lavoro è univoco e viene assegnato dal server all'avvio del lavoro. È possibile cercare un lavoro specifico immettendo il numero di identificazione del lavoro nella casella di testo fornita dal filtro di colonna.

- **Nome**

  Visualizza il nome del lavoro.

- **Tipo**

  Visualizza il tipo di lavoro. I tipi di lavoro sono i seguenti:

  - **Cluster Acquisition** (acquisizione cluster)

    Un lavoro di Workflow Automation sta riscoprendo un cluster.

  - **Configurazione della protezione**

    Un processo di protezione sta avviando i flussi di lavoro di Workflow Automation, ad esempio pianificazioni cron, creazione di policy SnapMirror e così via.

  - **Operazione di relazione di protezione**

    Un processo di protezione esegue le operazioni SnapMirror.

  - **Catena del flusso di lavoro di protezione**

    Un lavoro di automazione del flusso di lavoro sta eseguendo più flussi di lavoro.

  - **Ripristina**

    Processo di ripristino in esecuzione.

  - **Pulizia**

    Il processo sta eliminando gli elementi del membro del servizio di storage che non sono più necessari per il ripristino.

  - **Conforme**

    Il lavoro sta verificando la configurazione dei membri del servizio di storage per verificarne la conformità.

  - **Distruggere**

    Il lavoro sta distruggendo un servizio di storage.

  - **Importa**

    Il processo sta importando oggetti di storage non gestiti in un servizio di storage esistente.

  - **Modifica**

    Il processo sta modificando gli attributi di un servizio di storage esistente.

  - **Iscriviti**

Il processo sta sottoscrivendo i membri a un servizio di storage.

- **Annulla iscrizione**

  Il processo sta annullando l'iscrizione dei membri a un servizio di storage.

- **Aggiorna**

  È in esecuzione un processo di aggiornamento della protezione.

- **Configurazione WFA**

  Un lavoro di automazione del flusso di lavoro sta spingendo le credenziali del cluster e sincronizzando le cache del database.

- **Stato**

  Visualizza lo stato di esecuzione del lavoro. Le opzioni di stato sono le seguenti:

  - **Interrotto**

    Il lavoro è stato interrotto.

  - **Aborting**

    Il lavoro è in fase di interruzione.

  - **Completato**

    Il lavoro è terminato.

  - **In esecuzione**

    Il processo è in esecuzione.

- **Ora di invio**

  Visualizza l'ora in cui il lavoro è stato inoltrato.

- **Durata**

  Visualizza la quantità di tempo necessaria per il completamento del lavoro. Questa colonna viene visualizzata per impostazione predefinita.

- **Tempo di completamento**

  Visualizza l'ora in cui il lavoro è stato completato. Per impostazione predefinita, questa colonna è nascosta.

Pagina dei dettagli del lavoro

La pagina Dettagli lavoro consente di visualizzare lo stato e altre informazioni su specifiche attività di protezione in esecuzione, in coda o completate. È possibile utilizzare queste informazioni per monitorare lo stato di avanzamento dei lavori di protezione e per risolvere i problemi relativi agli errori dei lavori.

Riepilogo del lavoro

Il riepilogo dei lavori visualizza le seguenti informazioni:

- ID lavoro
- Tipo
- Stato
- Tempo di invio
- Tempo di completamento
- Durata

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Aggiorna**

  Aggiorna l'elenco delle attività e le proprietà associate a ciascuna attività.

- **Visualizza job**

  Consente di tornare alla pagina lavori.

Elenco delle attività lavorative

L'elenco Job Tasks (attività lavoro) visualizza in una tabella tutte le attività associate a un lavoro specifico e le proprietà correlate a ciascuna attività.

- **Ora di inizio**

  Visualizza il giorno e l'ora di inizio dell'attività. Per impostazione predefinita, le attività più recenti vengono visualizzate nella parte superiore della colonna e quelle meno recenti nella parte inferiore.

- **Tipo**

  Visualizza il tipo di attività.

- **Stato**

  Stato di un'attività specifica:

  - **Completato**

    L'attività è terminata.

  - **In coda**

    L'attività sta per essere eseguita.

  - **In esecuzione**

    L'attività è in esecuzione.

- **In attesa**

  Un lavoro è stato inoltrato e alcune attività associate sono in attesa di essere accodate ed eseguite.

- **Stato**

  Visualizza lo stato dell'attività:

  - **Errore (❗)**

    Operazione non riuscita.

  - **Normale (✅)**

    Operazione riuscita.

  - **Saltato (↪)**

    Un'attività non è riuscita, con conseguente omissione delle attività successive.

- **Durata**

  Visualizza il tempo trascorso dall'inizio dell'attività.

- **Tempo di completamento**

  Visualizza l'ora in cui l'attività è stata completata. Per impostazione predefinita, questa colonna è nascosta.

- **ID attività**

  Visualizza il GUID che identifica una singola attività per un lavoro. La colonna può essere ordinata e filtrata. Per impostazione predefinita, questa colonna è nascosta.

- **Ordine di dipendenza**

  Visualizza un numero intero che rappresenta la sequenza di attività in un grafico, con zero assegnato alla prima attività. Per impostazione predefinita, questa colonna è nascosta.

- **Riquadro Dettagli attività**

  Visualizza informazioni aggiuntive su ciascuna attività di lavoro, tra cui il nome dell'attività, la descrizione dell'attività e, in caso di errore, il motivo dell'errore.

- **Task messages pane**

  Visualizza i messaggi specifici dell'attività selezionata. I messaggi potrebbero includere un motivo dell'errore e suggerimenti per risolverlo. Non tutte le attività visualizzano messaggi di attività.

Finestra di dialogo Advanced Secondary Settings (Impostazioni secondarie avanzate

È possibile utilizzare la finestra di dialogo Advanced Secondary Settings (Impostazioni secondarie avanzate) per attivare la replica flessibile della versione, il backup di più copie e le impostazioni relative allo spazio su un volume secondario. È possibile utilizzare la finestra di dialogo Advanced Secondary Settings (Impostazioni secondarie avanzate) per

modificare le impostazioni correnti.

Le impostazioni relative allo spazio massimizzano la quantità di dati memorizzati, tra cui: Deduplica, compressione dei dati, crescita automatica e garanzia di spazio.

La finestra di dialogo include i seguenti campi:

- **Abilita replica flessibile versione**

  Attiva SnapMirror con replica flessibile della versione. La replica flessibile della versione consente la protezione SnapMirror di un volume di origine anche se il volume di destinazione viene eseguito con una versione precedente di ONTAP rispetto a quella del volume di origine.

  - Abilitare il backup

    Se è attivata la replica flessibile della versione, consente anche il trasferimento e la conservazione di più copie Snapshot dei dati di origine di SnapMirror nella destinazione di SnapMirror.

- **Attiva deduplica**

  Consente la deduplica sul volume secondario in una relazione SnapVault in modo da eliminare i blocchi di dati duplicati per ottenere risparmi di spazio. È possibile utilizzare la deduplica quando i risparmi di spazio sono pari almeno al 10% e quando il tasso di sovrascrittura dei dati non è rapido. La deduplica viene spesso utilizzata per ambienti virtualizzati, condivisioni di file e dati di backup. Questa impostazione è disattivata per impostazione predefinita. Se attivata, questa operazione viene avviata dopo ogni trasferimento.

  - Attiva compressione

    Consente la compressione trasparente dei dati. È possibile utilizzare la compressione quando i risparmi di spazio sono pari ad almeno il 10%, quando il potenziale overhead è accettabile e quando sono disponibili risorse di sistema sufficienti per il completamento della compressione durante le ore non di punta. In una relazione SnapVault, questa impostazione è disattivata per impostazione predefinita. La compressione è disponibile solo quando è selezionata la deduplica.

  - Compressione in linea

    Consente risparmi immediati di spazio comprimendo i dati prima di scrivere i dati su disco. È possibile utilizzare la compressione inline quando il sistema non ha più del 50% di utilizzo durante le ore di punta e quando il sistema può ospitare nuove scritture e CPU aggiuntive durante le ore di punta. Questa impostazione è disponibile solo se è selezionato “Enable Compression” (Abilita compressione).

- **Attiva crescita automatica**

  Consente di espandere automaticamente il volume di destinazione quando la percentuale di spazio libero è inferiore alla soglia specificata, purché lo spazio sia disponibile sull’aggregato associato.

- **Dimensione massima**

  Imposta la percentuale massima alla quale un volume può crescere. Il valore predefinito è superiore del 20% rispetto alle dimensioni del volume di origine. Un volume non cresce automaticamente se la dimensione corrente è maggiore o uguale alla percentuale massima di crescita automatica. Questo campo è attivato solo quando è attivata l’impostazione di crescita automatica.

- **Dimensione incremento**

Specifica l'incremento percentuale in base al quale il volume cresce automaticamente prima di raggiungere la percentuale massima del volume di origine.

- **Garanzia di spazio**

  Garantisce che sul volume secondario sia allocato spazio sufficiente per garantire il successo dei trasferimenti di dati. L'impostazione della garanzia di spazio può essere una delle seguenti:

  - File
  - Volume
  - Nessuno + ad esempio, è possibile che si disponga di un volume da 200 GB contenente file per un totale di 50 GB; tuttavia, tali file contengono solo 10 GB di dati. La garanzia del volume assegna 200 GB al volume di destinazione, indipendentemente dal contenuto dell'origine. La garanzia del file assegna 50 GB per garantire che lo spazio riservato ai file sull'origine sia sufficiente; selezionando Nessuno in questo scenario, sulla destinazione vengono allocati solo 10 GB per lo spazio effettivo utilizzato dai dati del file sull'origine.

  La garanzia di spazio è impostata su Volume per impostazione predefinita.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Applica**

  Salva le impostazioni di efficienza selezionate e le applica facendo clic su **Apply** (Applica) nella finestra di dialogo Configure Protection (Configura protezione).

- **Annulla**

  Elimina le selezioni e chiude la finestra di dialogo Advanced Destination Settings (Impostazioni di destinazione avanzate).

Finestra di dialogo Advanced Destination Settings

È possibile utilizzare la finestra di dialogo Advanced Destination Settings (Impostazioni destinazione avanzate) per attivare le impostazioni di garanzia dello spazio su un volume di destinazione. È possibile selezionare le impostazioni avanzate quando la garanzia di spazio è disattivata sull'origine, ma si desidera attivarla sulla destinazione. Le impostazioni di deduplica, compressione e crescita automatica in una relazione SnapMirror vengono ereditate dal volume di origine e non possono essere modificate.

Garanzia di spazio

Garantisce che sul volume di destinazione sia allocato spazio sufficiente per garantire il successo dei trasferimenti di dati. L'impostazione della garanzia di spazio può essere una delle seguenti:

- File
- Volume
- Nessuno

Ad esempio, è possibile che si disponga di un volume da 200 GB contenente file per un totale di 50 GB;

tuttavia, tali file contengono solo 10 GB di dati. La garanzia del volume assegna 200 GB al volume di destinazione, indipendentemente dal contenuto dell'origine. La garanzia del file assegna 50 GB per garantire che lo spazio riservato ai file di origine sulla destinazione sia sufficiente; selezionando **Nessuno** in questo scenario, sulla destinazione vengono allocati solo 10 GB per lo spazio effettivo utilizzato dai dati del file sull'origine.

La garanzia di spazio è impostata su Volume per impostazione predefinita.

Finestra di dialogo Restore (Ripristina)

È possibile utilizzare la finestra di dialogo Restore (Ripristina) per ripristinare i dati in un volume da una copia Snapshot specifica.

Ripristina da

L'area Restore from (Ripristina da) consente di specificare da dove si desidera ripristinare i dati.

- **Volume**

  Specifica il volume dal quale si desidera ripristinare i dati. Per impostazione predefinita, viene selezionato il volume su cui è stata avviata l'azione di ripristino. È possibile selezionare un volume diverso dall'elenco a discesa contenente tutti i volumi con relazioni di protezione con il volume su cui è stata avviata l'azione di ripristino.

- **Copia Snapshot**

  Specifica quale copia Snapshot si desidera utilizzare per ripristinare i dati. Per impostazione predefinita, viene selezionata la copia Snapshot più recente. È inoltre possibile selezionare una copia Snapshot diversa dall'elenco a discesa. L'elenco di copie Snapshot cambia in base al volume selezionato.

- **Elenca un massimo di 995 file e directory**

  Per impostazione predefinita, nell'elenco vengono visualizzati un massimo di 995 oggetti. È possibile deselezionare questa casella di controllo se si desidera visualizzare tutti gli oggetti all'interno del volume selezionato. Questa operazione potrebbe richiedere del tempo se il numero di elementi è molto elevato.

Selezionare gli elementi da ripristinare

L'area Select ITEMS to restore (Seleziona elementi da ripristinare) consente di selezionare l'intero volume o i file e le cartelle specifici da ripristinare. È possibile selezionare un massimo di 10 file, cartelle o una combinazione di entrambi. Quando si seleziona il numero massimo di elementi, le caselle di controllo per la selezione degli elementi vengono disattivate.

- **Campo percorso**

  Visualizza il percorso dei dati che si desidera ripristinare. È possibile accedere alla cartella e ai file da ripristinare oppure digitare il percorso. Questo campo è vuoto fino a quando non si seleziona o si digita un percorso. Fare clic su dopo aver scelto un percorso, si passa a un livello superiore nella struttura delle directory.

- **Elenco cartelle e file**

  Visualizza il contenuto del percorso immesso. Per impostazione predefinita, viene visualizzata inizialmente la cartella root. Facendo clic sul nome di una cartella, viene visualizzato il contenuto della cartella.

È possibile selezionare gli elementi da ripristinare nel modo seguente:

- Quando si immette il percorso con un nome di file specifico specificato nel campo percorso, il file specificato viene visualizzato in cartelle e file.
- Quando si immette un percorso senza specificare un determinato file, il contenuto della cartella viene visualizzato nell'elenco cartelle e file ed è possibile selezionare fino a 10 file, cartelle o una combinazione di entrambi da ripristinare.

  Se una cartella contiene più di 995 elementi, viene visualizzato un messaggio per indicare che sono presenti troppi elementi da visualizzare e, se si procede con l'operazione, vengono ripristinati tutti gli elementi della cartella specificata. Se si desidera visualizzare tutti gli oggetti all'interno del volume selezionato, è possibile deselezionare la casella di controllo "Elenca un massimo di 995 file e directory".

Non è possibile ripristinare i flussi di file NTFS.

Ripristinare a.

L'area Restore To (Ripristina in) consente di specificare dove si desidera ripristinare i dati.

- **Posizione originale in Nome_volume**

  Ripristina i dati selezionati nella directory dell'origine da cui è stato eseguito il backup dei dati.

- **Posizione alternativa**

  Ripristina i dati selezionati in una nuova posizione:

  - Percorso di ripristino

    Specifica un percorso alternativo per il ripristino dei dati selezionati. Il percorso deve già esistere. È possibile utilizzare il pulsante **Browse** (Sfoglia) per raggiungere la posizione in cui si desidera ripristinare i dati oppure inserire il percorso manualmente utilizzando il formato cluster://svm/volume/path.

  - Preservare la gerarchia di directory

    Quando questa opzione è selezionata, mantiene la struttura del file o della directory originale. Ad esempio, se l'origine è /A/B/C/myfile.txt e la destinazione è /X/Y/Z, Unified Manager ripristina i dati utilizzando la seguente struttura di directory sulla destinazione: /X/Y/Z/A/B/C/myfile.txt.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Annulla**

  Elimina le selezioni e chiude la finestra di dialogo Restore (Ripristina).

- **Ripristina**

  Applica le selezioni e avvia il processo di ripristino.

Finestra di dialogo Sfoglia directory

È possibile utilizzare la finestra di dialogo Sfoglia directory per ripristinare i dati in una directory di un cluster e in una SVM diversa dall'origine originale. Il cluster e il volume di origine originali vengono selezionati per impostazione predefinita.

La finestra di dialogo Sfoglia directory consente di selezionare il cluster, la SVM, il volume e il percorso della directory in cui si desidera ripristinare i dati.

- **Cluster**

  Elenca le destinazioni cluster disponibili per il ripristino. Per impostazione predefinita, viene selezionato il cluster del volume di origine originale.

- **Elenco a discesa SVM**

  Elenca le SVM disponibili per il cluster selezionato. Per impostazione predefinita, viene selezionata la SVM del volume di origine originale.

- **Volume**

  Elenca tutti i volumi di lettura/scrittura in una SVM selezionata. È possibile filtrare i volumi in base al nome e allo spazio disponibile. Il volume con più spazio viene elencato per primo, e così via, in ordine decrescente. Per impostazione predefinita, viene selezionato il volume di origine originale.

- **Casella di testo percorso file**

  Consente di digitare il percorso del file in cui si desidera ripristinare i dati. Il percorso immesso deve già esistere.

- **Nome**

  Visualizza i nomi delle cartelle disponibili per il volume selezionato. Se si fa clic su una cartella nell'elenco Nome, vengono visualizzate le eventuali sottocartelle. I file contenuti nelle cartelle non vengono visualizzati. Fare clic su una volta selezionata, una cartella si sposta verso l'alto di un livello nella struttura di directory.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Selezionare la directory**

  Applica le selezioni e chiude la finestra di dialogo Sfoglia directory. Se non è selezionata alcuna directory, questo pulsante è disattivato.

- **Annulla**

  Elimina le selezioni e chiude la finestra di dialogo Sfoglia directory.

Finestra di dialogo Configure Protection (Configura protezione)

È possibile utilizzare la finestra di dialogo Configura protezione per creare relazioni

SnapMirror e SnapVault per tutti i volumi di protezione dati, lettura e scrittura sui cluster, in modo da garantire la replica dei dati su un volume di origine o su un volume primario.

Scheda Source (origine)

- **Vista topologia**

  Visualizza una rappresentazione visiva della relazione che si sta creando. L'origine nella topologia viene evidenziata per impostazione predefinita.

- **Informazioni origine**

  Visualizza i dettagli sui volumi di origine selezionati, incluse le seguenti informazioni:

  - Nome del cluster di origine
  - Nome SVM di origine
  - Dimensione totale del volume cumulativo

    Visualizza le dimensioni totali di tutti i volumi di origine selezionati.

  - Volume cumulativo utilizzato

    Visualizza le dimensioni del volume cumulativo utilizzato per tutti i volumi di origine selezionati.

  - Volume di origine

    Visualizza le seguenti informazioni in una tabella:

    - Volume di origine

      Visualizza i nomi dei volumi di origine selezionati.

    - Tipo

      Visualizza il tipo di volume.

    - Tipo di SnapLock

      Visualizza il tipo di SnapLock del volume. Le opzioni disponibili sono Compliance, Enterprise e non-SnapLock.

    - Copia Snapshot

      Visualizza la copia Snapshot utilizzata per il trasferimento di riferimento. Se il volume di origine è di lettura/scrittura, il valore predefinito nella colonna Snapshot copy (Copia snapshot) indica che viene creata una nuova copia Snapshot per impostazione predefinita e che viene utilizzata per il trasferimento di riferimento. Se il volume di origine è un volume di protezione dei dati, il valore Default nella colonna Snapshot copy (Copia Snapshot) indica che non viene creata alcuna nuova copia Snapshot e che tutte le copie Snapshot esistenti vengono trasferite alla destinazione. Facendo clic sul valore della copia Snapshot viene visualizzato un elenco di copie Snapshot da cui è possibile selezionare una copia Snapshot esistente da utilizzare per il trasferimento di riferimento. Non è possibile selezionare una copia Snapshot predefinita diversa se il tipo di origine è data Protection.

Scheda SnapMirror

Consente di specificare un cluster di destinazione, una SVM (Storage Virtual Machine) e un aggregato per una relazione di protezione, nonché una convenzione di denominazione per le destinazioni durante la creazione di una relazione SnapMirror. È inoltre possibile specificare una pianificazione e un criterio SnapMirror.

- **Vista topologia**

  Visualizza una rappresentazione visiva della relazione che si sta creando. La risorsa di destinazione di SnapMirror nella topologia viene evidenziata per impostazione predefinita.

- **Informazioni sulla destinazione**

  Consente di selezionare le risorse di destinazione per una relazione di protezione:

  - Link avanzato

    Apre la finestra di dialogo Advanced Destination Settings (Impostazioni di destinazione avanzate) quando si crea una relazione SnapMirror.

  - Cluster

    Elenca i cluster disponibili come host di destinazione della protezione. Questo campo è obbligatorio.

  - SVM (Storage Virtual Machine)

    Elenca le SVM disponibili nel cluster selezionato. È necessario selezionare un cluster prima di completare l'elenco SVM. Questo campo è obbligatorio.

  - Aggregato

    Elenca gli aggregati disponibili sulla SVM selezionata. È necessario selezionare un cluster prima di completare l'elenco degli aggregati. Questo campo è obbligatorio. L'elenco degli aggregati visualizza le seguenti informazioni:

    - Classifica

      Quando gli aggregati multipli soddisfano tutti i requisiti per una destinazione, il rank indica la priorità in cui l'aggregato è elencato, secondo le seguenti condizioni:

      A. Un aggregato che si trova su un nodo diverso dal nodo del volume di origine è preferibile per attivare la separazione del dominio di errore.
      B. Si preferisce un aggregato su un nodo con meno volumi per consentire il bilanciamento del carico tra i nodi di un cluster.
      C. Un aggregato che ha più spazio libero rispetto ad altri aggregati è preferibile per consentire il bilanciamento della capacità. Un rango di 1 indica che l'aggregato è il più preferito in base ai tre criteri.

    - Nome aggregato

      Nome dell'aggregato

    - Capacità disponibile
    - Quantità di spazio disponibile sull'aggregato per i dati

        - Pool di risorse

          Nome del pool di risorse a cui appartiene l'aggregato

    - Convenzione di naming

      Specifica la convenzione di naming predefinita applicata al volume di destinazione. È possibile accettare la convenzione di naming fornita oppure crearne una personalizzata. La convenzione di denominazione può avere i seguenti attributi: %C, %M, %V e %N, dove %C è il nome del cluster, %M è il nome SVM, %V è il volume di origine e %N è il nome del nodo di destinazione della topologia.

  Il campo Naming Convention (convenzione di naming) viene evidenziato in rosso se la voce non è valida. Facendo clic sul collegamento "Nome anteprima" viene visualizzata un'anteprima della convenzione di denominazione immessa e il testo dell'anteprima viene aggiornato dinamicamente durante la digitazione di una convenzione di denominazione nel campo di testo. Un suffisso compreso tra 001 e 999 viene aggiunto al nome di destinazione al momento della creazione della relazione, sostituendo il nnn visualizzato nel testo di anteprima, con 001 assegnato per primo, 002 assegnato per secondo e così via.

- **Impostazioni di relazione**

  Consente di specificare la velocità di trasferimento massima, il criterio SnapMirror e la pianificazione utilizzati dalla relazione di protezione:

    - Velocità di trasferimento massima

      Specifica la velocità massima con cui i dati vengono trasferiti tra cluster sulla rete. Se si sceglie di non utilizzare una velocità di trasferimento massima, il trasferimento di riferimento tra le relazioni è illimitato.

    - Policy di SnapMirror

      Specifica il criterio SnapMirror di ONTAP per la relazione. L'impostazione predefinita è DPDefault.

    - Crea policy

      Apre la finestra di dialogo Create SnapMirror Policy (Crea policy SnapMirror), che consente di creare e utilizzare un nuovo criterio SnapMirror.

    - Pianificazione di SnapMirror

      Specifica il criterio SnapMirror di ONTAP per la relazione. Le pianificazioni disponibili includono Nessuna, 5 minuti, 8 ore, giornaliera, oraria, e settimanalmente. L'impostazione predefinita è Nessuno, a indicare che non è associata alcuna pianificazione alla relazione. Le relazioni senza pianificazioni non hanno valori di stato di ritardo a meno che non appartengano a un servizio di storage.

    - Crea pianificazione

      Apre la finestra di dialogo Create Schedule (Crea pianificazione), che consente di creare una nuova pianificazione SnapMirror.

Scheda SnapVault

Consente di specificare un cluster secondario, una SVM e un aggregato per una relazione di protezione, nonché una convenzione di denominazione per i volumi secondari durante la creazione di una relazione SnapVault. È inoltre possibile specificare una pianificazione e un criterio SnapVault.

- **Vista topologia**

  Visualizza una rappresentazione visiva della relazione che si sta creando. La risorsa secondaria SnapVault nella topologia viene evidenziata per impostazione predefinita.

- **Informazioni secondarie**

  Consente di selezionare le risorse secondarie per una relazione di protezione:

  - Link avanzato

    Apre la finestra di dialogo Advanced Secondary Settings (Impostazioni secondarie avanzate).

  - Cluster

    Elenca i cluster disponibili come host di protezione secondari. Questo campo è obbligatorio.

  - SVM (Storage Virtual Machine)

    Elenca le SVM disponibili nel cluster selezionato. È necessario selezionare un cluster prima di completare l'elenco SVM. Questo campo è obbligatorio.

  - Aggregato

    Elenca gli aggregati disponibili sulla SVM selezionata. È necessario selezionare un cluster prima di completare l'elenco degli aggregati. Questo campo è obbligatorio. L'elenco degli aggregati visualizza le seguenti informazioni:

    - Classifica

      Quando gli aggregati multipli soddisfano tutti i requisiti per una destinazione, il rank indica la priorità in cui l'aggregato è elencato, secondo le seguenti condizioni:

      A. Un aggregato che si trova su un nodo diverso dal nodo del volume primario è preferibile per abilitare la separazione del dominio di errore.
      B. Si preferisce un aggregato su un nodo con meno volumi per consentire il bilanciamento del carico tra i nodi di un cluster.
      C. Un aggregato che ha più spazio libero rispetto ad altri aggregati è preferibile per consentire il bilanciamento della capacità. Un rango di 1 indica che l'aggregato è il più preferito in base ai tre criteri.

    - Nome aggregato

      Nome dell'aggregato

    - Capacità disponibile
    - Quantità di spazio disponibile sull'aggregato per i dati
    - Pool di risorse

      Nome del pool di risorse a cui appartiene l'aggregato

  - Convenzione di naming

    Specifica la convenzione di naming predefinita applicata al volume secondario. È possibile accettare la

convenzione di naming fornita oppure crearne una personalizzata. La convenzione di denominazione può avere i seguenti attributi: %C, %M, %V e %N, dove %C è il nome del cluster, %M è il nome SVM, %V è il volume di origine e %N è il nome del nodo secondario della topologia.

Il campo Naming Convention (convenzione di naming) viene evidenziato in rosso se la voce non è valida. Facendo clic sul collegamento “Nome anteprima” viene visualizzata un’anteprima della convenzione di denominazione immessa e il testo dell’anteprima viene aggiornato dinamicamente durante la digitazione di una convenzione di denominazione nel campo di testo. Se si immette un valore non valido, le informazioni non valide vengono visualizzate come punti interrogativi rossi nell’area di anteprima. Un suffisso compreso tra 001 e 999 viene aggiunto al nome secondario quando viene creata la relazione, sostituendo il nnn visualizzato nel testo di anteprima, con 001 assegnato per primo, 002 assegnato per secondo e così via.

- **Impostazioni di relazione**

  Consente di specificare la velocità di trasferimento massima, il criterio SnapVault e la pianificazione SnapVault utilizzati dalla relazione di protezione:

  - Velocità di trasferimento massima

    Specifica la velocità massima con cui i dati vengono trasferiti tra cluster sulla rete. Se si sceglie di non utilizzare una velocità di trasferimento massima, il trasferimento di riferimento tra le relazioni è illimitato.

  - Policy SnapVault

    Specifica il criterio ONTAP SnapVault per la relazione. L’impostazione predefinita è XDPDefault.

  - Crea policy

    Apre la finestra di dialogo Crea policy SnapVault, che consente di creare e utilizzare un nuovo policy SnapVault.

  - Programma SnapVault

    Specifica la pianificazione ONTAP SnapVault per la relazione. Le pianificazioni disponibili includono Nessuna, 5 minuti, 8 ore, giornaliera, oraria, e settimanalmente. L’impostazione predefinita è Nessuno, a indicare che non è associata alcuna pianificazione alla relazione. Le relazioni senza pianificazioni non hanno valori di stato di ritardo a meno che non appartengano a un servizio di storage.

  - Crea pianificazione

    Apre la finestra di dialogo Crea pianificazione, che consente di creare una pianificazione SnapVault.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Annulla**

  Elimina le selezioni e chiude la finestra di dialogo Configura protezione.

- **Applica**

  Applica le selezioni e avvia il processo di protezione.

Finestra di dialogo Crea pianificazione

La finestra di dialogo Crea pianificazione consente di creare una pianificazione di protezione di base o avanzata per i trasferimenti di relazione SnapMirror e SnapVault. È possibile creare una nuova pianificazione per aumentare la frequenza dei trasferimenti di dati a causa di frequenti aggiornamenti dei dati oppure creare una pianificazione meno frequente quando i dati cambiano di rado.

Impossibile configurare le pianificazioni per le relazioni sincroni di SnapMirror.

- **Cluster di destinazione**

  Il nome del cluster selezionato nella scheda SnapVault o SnapMirror della finestra di dialogo Configura protezione.

- **Nome pianificazione**

  Il nome fornito per la pianificazione. I nomi delle pianificazioni possono essere costituiti dai caratteri Da A a Z, da a a z, da 0 a 9, nonché da uno qualsiasi dei seguenti caratteri speciali: ! @ n.} % {caret e * ( ) _ -. I nomi delle pianificazioni non possono includere i seguenti caratteri: < >.

- **Di base o avanzato**

  La modalità di pianificazione che si desidera utilizzare.

  La modalità di base include i seguenti elementi:

  ◦ Ripetere

    Con quale frequenza si verifica un trasferimento pianificato. Le opzioni disponibili sono orarie, giornaliere e settimanali.

  ◦ Giorno

    Quando si seleziona una ripetizione settimanale, si verifica il giorno della settimana in cui viene effettuato il trasferimento.

  ◦ Ora

    Quando si seleziona Daily (giornaliero) o Weekly (Settimanale), si verifica l'ora del trasferimento.

    La modalità avanzata include i seguenti elementi:

  ◦ Mesi

    Un elenco numerico separato da virgole che rappresenta i mesi dell'anno. I valori validi vanno da 0 a 11, con zero che rappresenta gennaio e così via. Questo elemento è facoltativo. Lasciare vuoto il campo significa che i trasferimenti avvengono ogni mese.

  ◦ Giorni

    Un elenco numerico separato da virgole che rappresenta il giorno del mese. I valori validi vanno da 1 a 31. Questo elemento è facoltativo. Lasciare vuoto il campo significa che il trasferimento avviene ogni giorno del mese.

◦ Giorni feriali

Un elenco numerico separato da virgole che rappresenta i giorni della settimana. I valori validi sono da 0 a 6, con 0 che rappresenta la domenica e così via. Questo elemento è facoltativo. Lasciare vuoto il campo significa che il trasferimento avviene ogni giorno della settimana. Se viene specificato un giorno della settimana ma non un giorno del mese, il trasferimento avviene solo il giorno della settimana specificato e non ogni giorno.

◦ Ore

Un elenco numerico separato da virgole che rappresenta il numero di ore in un giorno. I valori validi vanno da 0 a 23, con 0 che rappresenta la mezzanotte. Questo elemento è facoltativo.

◦ Minuti

Un elenco numerico separato da virgole che rappresenta i minuti in un'ora. I valori validi vanno da 0 a 59. Questo elemento è obbligatorio.

Finestra di dialogo Create SnapMirror Policy

La finestra di dialogo Create SnapMirror Policy (Crea policy SnapMirror) consente di creare un criterio per impostare la priorità per i trasferimenti SnapMirror. Le policy vengono utilizzate per massimizzare l'efficienza dei trasferimenti dall'origine alla destinazione.

- **Cluster di destinazione**

  Il nome del cluster selezionato nella scheda SnapMirror della finestra di dialogo Configura protezione.

- **SVM di destinazione**

  Il nome della SVM selezionata nella scheda SnapMirror della finestra di dialogo Configura protezione.

- **Nome policy**

  Il nome fornito per la nuova policy. I nomi dei criteri possono essere costituiti dai caratteri Da A a Z, da a a z, da 0 a 9, punto (.), trattino (-), e il carattere di sottolineatura (_).

- **Priorità trasferimento**

  La priorità con cui viene eseguito un trasferimento per le operazioni asincrone. È possibile selezionare normale o basso. Relazioni di trasferimento con policy che specificano una normale priorità di trasferimento eseguite prima di quelle con policy che specificano una bassa priorità di trasferimento.

- **Commento**

  Un campo facoltativo in cui è possibile aggiungere commenti sulla policy.

- **Transfer Restart** (riavvio trasferimento)

  Indica l'azione di riavvio da eseguire quando un trasferimento viene interrotto da un'operazione di interruzione o da qualsiasi tipo di errore, ad esempio un'interruzione di rete. È possibile selezionare una delle seguenti opzioni:

◦ Sempre

Specifica che viene creata una nuova copia Snapshot prima di riavviare un trasferimento, quindi, se ne esiste una, il trasferimento viene riavviato da un checkpoint, seguito da un trasferimento incrementale dalla copia Snapshot appena creata.

◦ Mai

Specifica che i trasferimenti interrotti non vengono mai riavviati.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Annulla**

  Elimina le selezioni e chiude la finestra di dialogo Configura protezione.

- **Applica**

  Applica le selezioni e avvia il processo di protezione.

Finestra di dialogo Crea policy SnapVault

La finestra di dialogo Crea criterio SnapVault consente di creare un criterio per impostare la priorità per i trasferimenti SnapVault. Le policy vengono utilizzate per massimizzare l'efficienza dei trasferimenti dal volume primario al volume secondario.

- **Cluster di destinazione**

  Il nome del cluster selezionato nella scheda SnapVault della finestra di dialogo Configura protezione.

- **SVM di destinazione**

  Il nome della SVM selezionata nella scheda SnapVault della finestra di dialogo Configura protezione.

- **Nome policy**

  Il nome fornito per la nuova policy. I nomi dei criteri possono essere costituiti dai caratteri Da A a Z, da a a z, da 0 a 9, punto (.), trattino (-), e il carattere di sottolineatura (_).

- **Priorità trasferimento**

  La priorità di esecuzione del trasferimento. È possibile selezionare normale o basso. Relazioni di trasferimento con policy che specificano una normale priorità di trasferimento eseguite prima di quelle con policy che specificano una bassa priorità di trasferimento. L'impostazione predefinita è normale.

- **Commento**

  Un campo facoltativo in cui è possibile aggiungere un commento di massimo 255 caratteri sulla policy SnapVault.

- **Ignora tempo di accesso**

Specifica se i trasferimenti incrementali vengono ignorati per i file che hanno modificato solo il tempo di accesso.

- **Etichetta di replica**

  Elenca in una tabella le regole associate alle copie Snapshot selezionate da ONTAP che hanno un'etichetta di replica specifica in un criterio. Sono inoltre disponibili le seguenti informazioni e azioni:

  - Pulsanti di comando

    I pulsanti di comando consentono di eseguire le seguenti operazioni:

    - Aggiungi

      Consente di creare un'etichetta di copia Snapshot e un numero di conservazione.

    - Modifica Conteggio conservazione

      Consente di modificare il numero di conservazione per un'etichetta di copia Snapshot esistente. Il numero di conservazione deve essere compreso tra 1 e 251. La somma di tutti i conteggi di conservazione per tutte le regole non può superare 251.

    - Eliminare

      Consente di eliminare un'etichetta di copia Snapshot esistente.

  - Etichetta di copia Snapshot

    Visualizza l'etichetta della copia Snapshot. Se si seleziona uno o più volumi con la stessa policy di copia Snapshot locale, viene visualizzata una voce per ciascuna etichetta della policy. Se si selezionano più volumi con due o più criteri di copia Snapshot locali, la tabella visualizza tutte le etichette di tutti i criteri

  - Pianificazione

    Visualizza la pianificazione associata a ciascuna etichetta di copia Snapshot. Se a un'etichetta sono associati più piani di lavoro, i piani di lavoro per tale etichetta vengono visualizzati in un elenco separato da virgole. Se si selezionano più volumi con la stessa etichetta ma con pianificazioni diverse, la pianificazione visualizza "varie" per indicare che più di una pianificazione è associata ai volumi selezionati.

  - Destination Retention Count

    Visualizza il numero di copie Snapshot con l'etichetta specificata che vengono conservate sul secondario SnapVault. Conteggi di conservazione per etichette con pianificazioni multiple Visualizza la somma dei conteggi di conservazione di ciascuna coppia di etichette e pianificazioni. Se si selezionano più volumi con due o più policy di copia Snapshot locali, il conteggio delle trattenuta è vuoto.

Finestra di dialogo Modifica relazione

È possibile modificare una relazione di protezione esistente per modificare la velocità di trasferimento massima, il criterio di protezione o il programma di protezione.

Informazioni di destinazione

- **Cluster di destinazione**

  Il nome del cluster di destinazione selezionato.

- **SVM di destinazione**

  Il nome della SVM selezionata

- **Impostazioni di relazione**

  Consente di specificare la velocità di trasferimento massima, il criterio SnapMirror e la pianificazione utilizzati dalla relazione di protezione:

  - Velocità di trasferimento massima

    Specifica la velocità massima alla quale i dati di riferimento vengono trasferiti tra cluster sulla rete. Se selezionata, la larghezza di banda della rete è limitata al valore specificato. È possibile immettere un valore numerico e selezionare kilobyte per second (kbps), megabyte per second (Mbps), gigabyte per second (Gbps) o terabyte per second (Tbps). La velocità di trasferimento massima specificata deve essere superiore a 1 kbps e inferiore a 4 Tbps. Se si sceglie di non utilizzare una velocità di trasferimento massima, il trasferimento di riferimento tra le relazioni è illimitato. Se il cluster primario e il cluster secondario sono identici, questa impostazione viene disattivata.

  - Policy di SnapMirror

    Specifica il criterio SnapMirror di ONTAP per la relazione. L'impostazione predefinita è DPDefault.

  - Crea policy

    Apre la finestra di dialogo Create SnapMirror Policy (Crea policy SnapMirror), che consente di creare e utilizzare un nuovo criterio SnapMirror.

  - Pianificazione di SnapMirror

    Specifica il criterio SnapMirror di ONTAP per la relazione. Le pianificazioni disponibili includono Nessuna, 5 minuti, 8 ore, giornaliera, oraria, e settimanalmente. L'impostazione predefinita è Nessuno, a indicare che non è associata alcuna pianificazione alla relazione. Le relazioni senza pianificazioni non hanno valori di stato di ritardo a meno che non appartengano a un servizio di storage.

  - Crea pianificazione

    Apre la finestra di dialogo Create Schedule (Crea pianificazione), che consente di creare una nuova pianificazione SnapMirror.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Annulla**

  Elimina le selezioni e chiude la finestra di dialogo Configura protezione.

- **Invia**

Applica le selezioni e chiude la finestra di dialogo Modifica relazione.

Finestra di dialogo Initialize/Update

La finestra di dialogo Initialize/Update (Inizializza/Aggiorna) consente di eseguire un primo trasferimento baseline su una nuova relazione di protezione o di aggiornare una relazione se è già inizializzata e si desidera eseguire un aggiornamento incrementale manuale, non pianificato.

Scheda Transfer Options (Opzioni di trasferimento)

La scheda Transfer Options (Opzioni di trasferimento) consente di modificare la priorità di inizializzazione di un trasferimento e la larghezza di banda utilizzata durante i trasferimenti.

- **Priorità trasferimento**

  La priorità di esecuzione del trasferimento. È possibile selezionare normale o basso. Relazioni con policy che specificano una normale priorità di trasferimento eseguite prima di quelle che specificano una bassa priorità di trasferimento. Normal (normale) è selezionato per impostazione predefinita.

- **Velocità di trasferimento massima**

  Specifica la velocità massima con cui i dati vengono trasferiti tra cluster sulla rete. Se si sceglie di non utilizzare una velocità di trasferimento massima, il trasferimento di riferimento tra le relazioni è illimitato. Se si seleziona più di una relazione con diverse velocità di trasferimento massime, è possibile specificare una delle seguenti impostazioni relative alla velocità di trasferimento massima:

  - Utilizzare i valori specificati durante la configurazione o la modifica delle singole relazioni

    Quando questa opzione è selezionata, le operazioni di inizializzazione e aggiornamento utilizzano la velocità di trasferimento massima specificata al momento della creazione o della modifica di ciascuna relazione. Questo campo è disponibile solo quando vengono inizializzate o aggiornate più relazioni con velocità di trasferimento diverse.

  - Senza limiti

    Indica che non esiste alcun limite di larghezza di banda per i trasferimenti tra le relazioni. Questo campo è disponibile solo quando vengono inizializzate o aggiornate più relazioni con velocità di trasferimento diverse.

  - Limitare la larghezza di banda a.

    Se selezionata, la larghezza di banda della rete è limitata al valore specificato. È possibile immettere un valore numerico e selezionare kilobyte per second (kbps), Megabyte per second (Mbps), Gigabyte per second (Gbps) o Terabyte per second (Tbps). La velocità di trasferimento massima specificata deve essere superiore a 1 kbps e inferiore a 4 Tbps.

Scheda copie Snapshot di origine

La scheda Source Snapshot Copies (copie Snapshot di origine) visualizza le seguenti informazioni sulla copia Snapshot di origine utilizzata per il trasferimento di riferimento:

- **Volume di origine**

Visualizza i nomi dei volumi di origine corrispondenti.

- **Volume di destinazione**

  Visualizza i nomi dei volumi di destinazione selezionati.

- **Tipo di origine**

  Visualizza il tipo di volume. Il tipo può essere lettura/scrittura o protezione dati.

- **Snapshot Copy**

  Visualizza la copia Snapshot utilizzata per il trasferimento dei dati. Facendo clic sul valore della copia Snapshot viene visualizzata la finestra di dialogo Select Source Snapshot Copy (Seleziona copia Snapshot di origine), in cui è possibile selezionare una copia Snapshot specifica per il trasferimento, a seconda del tipo di relazione di protezione in uso e dell'operazione che si sta eseguendo. L'opzione per specificare una copia Snapshot diversa non è disponibile per le origini del tipo di protezione dei dati.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Annulla**

  Elimina le selezioni e chiude la finestra di dialogo Inizializza/Aggiorna.

- **Invia**

  Salva le selezioni e avvia il processo di inizializzazione o aggiornamento.

Finestra di dialogo di risincronizzazione

La finestra di dialogo risincronizza consente di risincronizzare i dati su una relazione SnapMirror o SnapVault precedentemente interrotta e quindi la destinazione è stata creata come volume di lettura/scrittura. È inoltre possibile risincronizzare quando viene eliminata una copia Snapshot comune richiesta sul volume di origine, causando il mancato aggiornamento di SnapMirror o SnapVault.

Scheda Opzioni di risincronizzazione

La scheda Opzioni di risincronizzazione consente di impostare la priorità di trasferimento e la velocità di trasferimento massima per la relazione di protezione che si sta risincronizzando.

- **Priorità trasferimento**

  La priorità di esecuzione del trasferimento. È possibile selezionare normale o basso. Relazioni con policy che specificano una normale priorità di trasferimento eseguite prima di quelle con policy che specificano una bassa priorità di trasferimento.

- **Velocità di trasferimento massima**

  Specifica la velocità massima con cui i dati vengono trasferiti tra cluster sulla rete. Se selezionata, la larghezza di banda della rete è limitata al valore specificato. È possibile immettere un valore numerico e selezionare kilobyte per second (kbps), megabyte per second (Mbps), gigabyte per second (Gbps) o Tbps.

Se si sceglie di non utilizzare una velocità di trasferimento massima, il trasferimento di riferimento tra le relazioni è illimitato.

Scheda copie Snapshot di origine

La scheda Source Snapshot Copies (copie Snapshot di origine) visualizza le seguenti informazioni sulla copia Snapshot di origine utilizzata per il trasferimento di riferimento:

- **Volume di origine**

  Visualizza i nomi dei volumi di origine corrispondenti.

- **Volume di destinazione**

  Visualizza i nomi dei volumi di destinazione selezionati.

- **Tipo di origine**

  Visualizza il tipo di volume: Lettura/scrittura o protezione dati.

- **Snapshot Copy**

  Visualizza la copia Snapshot utilizzata per il trasferimento dei dati. Facendo clic sul valore della copia Snapshot viene visualizzata la finestra di dialogo Select Source Snapshot Copy (Seleziona copia Snapshot di origine), in cui è possibile selezionare una copia Snapshot specifica per il trasferimento, a seconda del tipo di relazione di protezione in uso e dell'operazione che si sta eseguendo.

Pulsanti di comando

- **Invia**

  Avvia il processo di risincronizzazione e chiude la finestra di dialogo risincronizzazione.

- **Annulla**

  Annulla le selezioni e chiude la finestra di dialogo Risincronizza.

Finestra di dialogo Select Source Snapshot Copy (Seleziona copia snapshot di origine

La finestra di dialogo Seleziona copia snapshot di origine consente di selezionare una copia Snapshot specifica per trasferire i dati tra relazioni di protezione oppure di selezionare il comportamento predefinito, che varia a seconda che si stia inizializzando, aggiornando o risincronizzando una relazione e se la relazione è SnapMirror o SnapVault.

Predefinito

Consente di selezionare il comportamento predefinito per determinare quale copia Snapshot utilizzare per inizializzare, aggiornare e risincronizzare i trasferimenti per le relazioni SnapVault e SnapMirror.

Se si sta eseguendo un trasferimento SnapVault, il comportamento predefinito per ciascuna operazione è il seguente:

Operazione	Comportamento SnapVault predefinito quando l'origine è in lettura/scrittura	Comportamento SnapVault predefinito quando l'origine è protezione dati (DP)
Inizializzare	Crea una nuova copia Snapshot e la trasferisce.	Trasferisce l'ultima copia Snapshot esportata.
Aggiornare	Trasferisce solo le copie Snapshot etichettate, come specificato nel criterio.	Trasferisce l'ultima copia Snapshot esportata.
Risincronizzare	Trasferisce tutte le copie Snapshot etichettate create dopo la più recente copia Snapshot comune.	Trasferisce la copia Snapshot più recente.

Se si esegue un trasferimento SnapMirror, il comportamento predefinito per ciascuna operazione è il seguente:

Operazione	Comportamento predefinito di SnapMirror	Comportamento predefinito di SnapMirror quando la relazione è un secondo hop in una cascata di SnapMirror con SnapMirror
Inizializzare	Crea una nuova copia Snapshot e la trasferisce e tutte le copie Snapshot create prima della nuova copia Snapshot.	Trasferisce tutte le copie Snapshot dall'origine.
Aggiornare	Crea una nuova copia Snapshot e la trasferisce e tutte le copie Snapshot create prima della nuova copia Snapshot.	Trasferisce tutte le copie Snapshot.
Risincronizzare	Crea una nuova copia Snapshot e trasferisce tutte le copie Snapshot dall'origine.	Trasferisce tutte le copie Snapshot dal volume secondario al volume terzo ed elimina tutti i dati aggiunti dopo la creazione della copia Snapshot comune più recente.

Copia Snapshot esistente

Consente di selezionare una copia Snapshot esistente dall'elenco se è consentita la selezione della copia Snapshot per tale operazione.

- **Snapshot Copy**

  Visualizza le copie Snapshot esistenti da cui è possibile selezionare per un trasferimento.

- **Data di creazione**

  Visualizza la data e l'ora di creazione della copia Snapshot. Le copie Snapshot sono elencate dal più recente al meno recente, con il più recente in cima all'elenco.

Se si sta eseguendo un trasferimento SnapVault e si desidera selezionare una copia Snapshot esistente da trasferire da un'origine a una destinazione, il comportamento di ciascuna operazione è il seguente:

Operazione	Comportamento di SnapVault quando si specifica una copia Snapshot	Comportamento di SnapVault quando si specifica una copia Snapshot in una cascata
Inizializzare	Trasferisce la copia Snapshot specificata.	La selezione della copia Snapshot di origine non è supportata per i volumi di protezione dei dati.
Aggiornare	Trasferisce la copia Snapshot specificata.	La selezione della copia Snapshot di origine non è supportata per i volumi di protezione dei dati.
Risincronizzare	Trasferisce la copia Snapshot selezionata.	La selezione della copia Snapshot di origine non è supportata per i volumi di protezione dei dati.

Se si sta eseguendo un trasferimento SnapMirror e si desidera selezionare una copia Snapshot esistente da trasferire da un'origine a una destinazione, il comportamento di ciascuna operazione è il seguente:

Operazione	Comportamento di SnapMirror quando si specifica una copia Snapshot	Comportamento di SnapMirror quando si specifica una copia Snapshot in una cascata
Inizializzare	Trasferisce tutte le copie Snapshot sull'origine, fino alla copia Snapshot specificata.	La selezione della copia Snapshot di origine non è supportata per i volumi di protezione dei dati.
Aggiornare	Trasferisce tutte le copie Snapshot sull'origine, fino alla copia Snapshot specificata.	La selezione della copia Snapshot di origine non è supportata per i volumi di protezione dei dati.
Risincronizzare	Trasferisce tutte le copie Snapshot dall'origine, fino alla copia Snapshot selezionata, quindi elimina tutti i dati aggiunti dopo la creazione della copia Snapshot comune più recente.	La selezione della copia Snapshot di origine non è supportata per i volumi di protezione dei dati.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Invia**

  Invia le selezioni e chiude la finestra di dialogo Select Source Snapshot Copy (Seleziona copia snapshot di origine).

- **Annulla**

Elimina le selezioni e chiude la finestra di dialogo Select Source Snapshot Copy (Seleziona copia snapshot di origine).

Risincronizzazione inversa

Quando si dispone di una relazione di protezione interrotta perché il volume di origine è disattivato e la destinazione viene creata come volume di lettura/scrittura, la risincronizzazione inversa consente di invertire la direzione della relazione in modo che la destinazione diventi la nuova origine e l'origine diventi la nuova destinazione.

Quando un disastro disattiva il volume di origine nella relazione di protezione, è possibile utilizzare il volume di destinazione per fornire i dati convertendolo in lettura/scrittura, mentre si ripara o si sostituisce l'origine, si aggiorna l'origine e si ristabilisce la relazione. Quando si esegue un'operazione di risincronizzazione inversa, i dati sull'origine più recenti dei dati sulla copia Snapshot comune vengono cancellati.

Prima della risincronizzazione inversa

Visualizza l'origine e la destinazione di una relazione prima di un'operazione di risincronizzazione inversa.

- **Volume di origine**

  Il nome e la posizione del volume di origine prima di un'operazione di risincronizzazione inversa.

- **Volume di destinazione**

  Il nome e la posizione del volume di destinazione prima di un'operazione di risincronizzazione inversa.

Dopo risincronizzazione inversa

Visualizza l'origine e la destinazione di una relazione dopo un'operazione di risincronizzazione di riserva.

- **Volume di origine**

  Il nome e la posizione del volume di origine dopo un'operazione di risincronizzazione inversa.

- **Volume di destinazione**

  Il nome e la posizione del volume di destinazione dopo un'operazione di risincronizzazione inversa.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Invia**

  Avvia il processo di risincronizzazione inversa.

- **Annulla**

  Chiude la finestra di dialogo Reverse Resync (risincronizzazione inversa) senza avviare un'operazione di risincronizzazione inversa.

Relazione: Vista tutte le relazioni

La vista relazione: Tutte le relazioni visualizza informazioni sulle relazioni di protezione nel sistema di storage.

Per impostazione predefinita, quando si accede alla pagina delle relazioni, il report visualizzato include le relazioni di protezione di livello superiore per volumi e macchine virtuali di storage. I controlli nella parte superiore della pagina consentono di selezionare una vista particolare, eseguire ricerche per individuare oggetti specifici, creare e applicare filtri per restringere l'elenco dei dati visualizzati, aggiungere/rimuovere/riordinare le colonne della pagina ed esportare i dati della pagina in un file .csv, .pdf, o file .xlsx. Dopo aver personalizzato la pagina, è possibile salvare i risultati come vista personalizzata e pianificare un report dei dati da generare e inviare via email a intervalli regolari. Per impostazione predefinita, quando si seleziona il menu **Relazioni**, il report visualizzato include le relazioni di protezione per volumi e macchine virtuali di storage nel data center. È possibile utilizzare l'opzione **Filter** per visualizzare solo i sistemi storage selezionati, ad esempio solo i volumi o solo le macchine virtuali storage. Lo stesso report viene visualizzato nella pagina Storage e solo per l'entità di storage selezionata. Se si desidera visualizzare le relazioni tra volumi o macchine virtuali di storage, è possibile accedere alla pagina **Storage** > **Volumes** > **Relationship: All relationship** o accedere a **Protection** > **Relationship** > **Relationship: Tutte le relazioni** e utilizzare l'opzione **Relationship Object Type** nel filtro * per filtrare solo i dati dei volumi o delle VM di storage.

La pagina Relazioni che elenca tutte le relazioni di protezione ha il collegamento **Visualizza in Gestione sistema** per il cluster di destinazione che consente di visualizzare gli stessi oggetti in Gestione sistema di ONTAP.

- **Stato**

  Visualizza lo stato corrente della relazione di protezione.

  Lo stato può essere Error ( ), Avviso ( ) O OK ( ).

- **Storage VM di origine**

  Visualizza il nome della SVM di origine. È possibile visualizzare ulteriori dettagli sulla SVM di origine facendo clic sul nome della SVM.

  Se nel cluster esiste una SVM ma non è stata ancora aggiunta all'inventario di Unified Manager o se la SVM è stata creata dopo l'ultimo aggiornamento del cluster, questo campo sarà vuoto. Per aggiornare l'elenco delle risorse, è necessario assicurarsi che la SVM esista o eseguire una nuova ricerca nel cluster.

- **Origine**

  Visualizza il volume di origine o la VM di storage di origine protetti in base alla selezione effettuata. È possibile visualizzare ulteriori dettagli sul volume di origine o sulla VM di storage facendo clic sul nome del volume o della VM di storage.

  Se il messaggio `Resource-key not discovered` Potrebbe indicare che il volume esiste nel cluster ma non è stato ancora aggiunto all'inventario di Unified Manager o che il volume è stato creato dopo l'ultimo aggiornamento del cluster. Per aggiornare l'elenco delle risorse, è necessario assicurarsi che il volume esista o eseguire una nuova ricerca nel cluster.

- **Storage VM di destinazione**

  Visualizza il nome della SVM di destinazione. È possibile visualizzare ulteriori dettagli sulla SVM di destinazione facendo clic sul nome della SVM.

- **Destinazione**

  Visualizza il nome del volume di destinazione o della VM di storage in base alla selezione effettuata. È possibile visualizzare ulteriori dettagli sul volume di destinazione o sulla VM di storage facendo clic sul relativo nome dell'oggetto.

- **Tipo di oggetto relazione**

  Visualizza il tipo di oggetto utilizzato nella relazione, ad esempio VM di storage, volume e gruppo di coerenza. Per gli oggetti in una relazione di coerenza, l'origine e le destinazioni della relazione visualizzano il gruppo di coerenza e facendo clic su di essi si accede alla pagina LUN per visualizzare la relazione.

- **Policy**

  Visualizza il nome del criterio di protezione per la relazione SnapMirror. È possibile fare clic sul nome del criterio per visualizzare i dettagli associati a tale criterio, incluse le seguenti informazioni:

  - Priorità di trasferimento

    Specifica la priorità di esecuzione di un trasferimento per le operazioni asincrone. La priorità di trasferimento è normale o bassa. I trasferimenti con priorità normale vengono pianificati prima dei trasferimenti con priorità bassa. L'impostazione predefinita è normale.

  - Ignorare il tempo di accesso

    Si applica solo alle relazioni SnapVault. Specifica se i trasferimenti incrementali ignorano i file che hanno modificato solo il tempo di accesso. I valori sono vero o Falso. L'impostazione predefinita è Falso.

  - Quando la relazione non è sincronizzata

    Specifica l'azione che ONTAP esegue quando non è possibile sincronizzare una relazione sincrona. Le relazioni StrictSync limitano l'accesso al volume primario in caso di mancata sincronizzazione con il volume secondario. Le relazioni di sincronizzazione non limitano l'accesso al primario in caso di mancata sincronizzazione con il secondario.

  - Limite di tentativi

    Specifica il numero massimo di tentativi di trasferimento manuale o pianificato per una relazione SnapMirror. Il valore predefinito è 8.

  - Commenti

    Fornisce un campo di testo per i commenti specifici per il criterio selezionato.

  - Etichetta SnapMirror

    Specifica l'etichetta SnapMirror per la prima pianificazione associata alla policy di copia Snapshot. L'etichetta SnapMirror viene utilizzata dal sottosistema SnapVault quando si esegue il backup delle copie Snapshot in una destinazione SnapVault.

  - Impostazione di conservazione

    Specifica il tempo di conservazione dei backup, in base al tempo o al numero di backup.

- Copie Snapshot effettive

  Specifica il numero di copie Snapshot su questo volume che corrispondono all'etichetta specificata.

- Conservare le copie Snapshot

  Specifica il numero di copie Snapshot di SnapVault che non vengono eliminate automaticamente anche se viene raggiunto il limite massimo per il criterio. I valori sono vero o Falso. L'impostazione predefinita è Falso.

- Soglia di avviso di conservazione

  Specifica il limite di copia Snapshot al quale viene inviato un avviso per indicare che il limite massimo di conservazione è quasi raggiunto.

- **Durata ritardo**

  Visualizza il periodo di tempo in cui i dati sul mirror si trovano indietro rispetto all'origine.

  La durata del ritardo deve essere vicina o uguale a 0 secondi per le relazioni StrictSync.

- **Stato Lag**

  Visualizza lo stato di ritardo per le relazioni gestite e per le relazioni non gestite che hanno una pianificazione associata a tale relazione. Lo stato di ritardo può essere:

  - Errore

    La durata del ritardo è maggiore o uguale alla soglia di errore del ritardo.

  - Attenzione

    La durata del ritardo è maggiore o uguale alla soglia di avviso del ritardo.

  - OK

    La durata del ritardo rientra nei limiti normali.

  - Non applicabile

    Lo stato di ritardo non è applicabile per le relazioni sincrone perché non è possibile configurare una pianificazione.

- **Ultimo aggiornamento riuscito**

  Visualizza l'ora dell'ultima operazione SnapMirror o SnapVault eseguita correttamente.

  L'ultimo aggiornamento riuscito non è applicabile per le relazioni sincrone.

- **Relazioni costitutive**

  Visualizza se sono presenti volumi nell'oggetto selezionato.

- **Tipo di relazione**

  Visualizza il tipo di relazione utilizzato per replicare un volume. I tipi di relazione includono:

- Mirror asincrono
- Vault asincrono
- MirrorVault asincrono
- StrictSync
- Sincronizza

- **Stato trasferimento**

  Visualizza lo stato di trasferimento per la relazione di protezione. Lo stato del trasferimento può essere uno dei seguenti:

  - Interruzione

    I trasferimenti SnapMirror sono attivati; tuttavia, è in corso un'operazione di interruzione del trasferimento che potrebbe includere la rimozione del checkpoint.

  - Verifica in corso

    Il volume di destinazione è sottoposto a un controllo diagnostico e non è in corso alcun trasferimento.

  - Finalizzazione

    I trasferimenti SnapMirror sono attivati. Il volume è attualmente in fase di post-trasferimento per i trasferimenti incrementali SnapVault.

  - Inattivo

    I trasferimenti sono attivati e non è in corso alcun trasferimento.

  - In-Sync

    I dati nei due volumi nella relazione sincrona vengono sincronizzati.

  - Out-of-Sync

    I dati nel volume di destinazione non vengono sincronizzati con il volume di origine.

  - Preparazione in corso

    I trasferimenti SnapMirror sono attivati. Il volume è attualmente in fase di pre-trasferimento per i trasferimenti incrementali SnapVault.

  - In coda

    I trasferimenti SnapMirror sono attivati. Nessun trasferimento in corso.

  - A Quiesced

    I trasferimenti SnapMirror sono disattivati. Nessun trasferimento in corso.

  - Quiescing

    È in corso un trasferimento SnapMirror. I trasferimenti aggiuntivi sono disattivati.

- Trasferimento in corso

  I trasferimenti SnapMirror sono attivati e il trasferimento è in corso.

- In transizione

  Il trasferimento asincrono dei dati dal volume di origine al volume di destinazione è completo e la transizione all'operazione sincrona è iniziata.

- In attesa

  È stato avviato un trasferimento SnapMirror, ma alcune attività associate sono in attesa di essere accodate.

- **Durata ultimo trasferimento**

  Visualizza il tempo necessario per il completamento dell'ultimo trasferimento dei dati.

  La durata del trasferimento non è applicabile per le relazioni StrictSync perché il trasferimento deve essere simultaneo.

- **Dimensione ultimo trasferimento**

  Visualizza le dimensioni, in byte, dell'ultimo trasferimento di dati.

  La dimensione del trasferimento non è applicabile per le relazioni StrictSync.

- **Mediatori**

  Visualizza lo stato del mediatore.

  - Non applicabile

    Se il cluster non supporta SnapMirror Business Continuity.

  - Non configurato

    Se non è configurato, o se è configurato, ma viene aggiunto solo il cluster di destinazione e il cluster di origine non viene aggiunto in Unified Manager.

  - Indirizzo IP del mediatore

    Se è configurato, e i cluster di origine e di destinazione vengono aggiunti in Unified Manager.

- **Stato**

  Visualizza lo stato della relazione SnapMirror o SnapVault. Lo stato può essere non inizializzato, SnapMirrored o interrotto. Se si seleziona un volume di origine, lo stato di relazione non è applicabile e non viene visualizzato.

- **Relationship Health**

  Visualizza l'heath di relazione del cluster.

- **Motivo non corretto**

Il motivo per cui la relazione si trova in uno stato malsano.

- **Priorità trasferimento**

  Visualizza la priorità di esecuzione di un trasferimento. La priorità di trasferimento è normale o bassa. I trasferimenti con priorità normale vengono pianificati prima dei trasferimenti con priorità bassa.

  La priorità di trasferimento non è applicabile per le relazioni sincrone perché tutti i trasferimenti sono trattati con la stessa priorità.

- **Pianificazione**

  Visualizza il nome del programma di protezione assegnato alla relazione.

  La pianificazione non è applicabile per le relazioni sincrone.

- **Replica flessibile versione**

  Visualizza Sì, Sì con opzione di backup o Nessuno.

- **Cluster di origine**

  Visualizza l'FQDN, il nome breve o l'indirizzo IP del cluster di origine per la relazione SnapMirror.

- **FQDN del cluster di origine**

  Visualizza il nome del cluster di origine per la relazione SnapMirror.

- **Nodo di origine**

  Visualizza il nome del collegamento del nome del nodo di origine per la relazione SnapMirror di un volume e il collegamento del numero di nodi di relazione SnapMirror quando l'oggetto è una Storage VM o un gruppo di coerenza.

Nella vista personalizzata, facendo clic sul collegamento del nome del nodo, è possibile visualizzare ed estendere la protezione per gli oggetti di storage su cui i volumi di quei gruppi di coerenza che appartengono alla relazione SM-BC.

Quando si fa clic sul collegamento Node count (numero di nodi), viene visualizzata la pagina Node (nodo) con i rispettivi nodi associati a tale relazione. Quando il numero di nodi è 0, non viene visualizzato alcun valore in quanto non vi sono nodi associati alla relazione.

- **Nodo di destinazione**

  Visualizza il nome del collegamento del nome del nodo di destinazione per la relazione SnapMirror di un volume e il collegamento del numero di nodi della relazione SnapMirror quando l'oggetto è una Storage VM o un gruppo di coerenza.

  Quando si fa clic sul collegamento Node count (numero di nodi), viene visualizzata la pagina Node (nodo) con i rispettivi nodi associati a tale relazione. Quando il numero di nodi è 0, non viene visualizzato alcun valore in quanto non vi sono nodi associati alla relazione.

- **Cluster di destinazione**

  Visualizza il nome del cluster di destinazione per la relazione SnapMirror.

- **FQDN cluster di destinazione**

  Visualizza l'FQDN, il nome breve o l'indirizzo IP del cluster di destinazione per la relazione SnapMirror.

- **Protetto da**

  Visualizza le diverse relazioni. In questa colonna, è possibile visualizzare le relazioni di volumi e gruppi di coerenza per cluster e ordine delle macchine virtuali di storage, tra cui:

  - SnapMirror
  - Dr. VM storage
  - SnapMirror, Storage VM DR
  - Gruppo di coerenza
  - SnapMirror, Consistency Group.

Informazioni correlate

- Per informazioni sulla vista **Relationship: MetroCluster**, vedere "Monitoraggio delle configurazioni MetroCluster".
- Per informazioni sulla vista **Relationship: Last 1 Month Transfer Status** (relazione: Stato trasferimento ultimo 1 mese), vedere "Relazione: Vista Stato trasferimento ultimo 1 mese".
- Per informazioni sulla vista **relazione: Tutte le relazioni**, vedere "Relazione: Vista tasso di trasferimento dell'ultimo mese".

Relazione: Vista Stato trasferimento ultimo 1 mese

La relazione: La vista Stato trasferimento dell'ultimo mese consente di analizzare i trend di trasferimento in un determinato periodo di tempo per volumi e macchine virtuali di storage in relazioni asincrone. Questa pagina visualizza anche se il trasferimento è stato un successo o un errore.

I controlli nella parte superiore della pagina consentono di eseguire ricerche per individuare oggetti specifici, creare e applicare filtri per restringere l'elenco dei dati visualizzati, aggiungere/rimuovere/riordinare le colonne della pagina ed esportare i dati della pagina in un `.csv`, `.pdf`, o. `.xlsx` file. Dopo aver personalizzato la pagina, è possibile salvare i risultati come vista personalizzata e pianificare un report dei dati da generare e inviare via email a intervalli regolari. È possibile utilizzare l'opzione **Filter** per visualizzare solo i sistemi storage selezionati, ad esempio solo i volumi o solo le Storage VM. Lo stesso report viene visualizzato nella pagina Storage e solo per l'entità di storage selezionata. Ad esempio, se si desidera visualizzare le relazioni dei volumi, è possibile accedere al report Relationship: Last 1 Month Transfer Status per le Storage VM dal menu **Storage** > **Storage VMS** > **Relationship: Last 1 Month Transfer Status** o da **Protection** > **Relationship** > **Relationship: Menu Transfer Status** dell'ultimo mese e utilizzare **Filter** per visualizzare solo i dati dei volumi.

- **Volume di origine**

  Visualizza il nome del volume di origine.

- **Volume di destinazione**

  Visualizza il nome del volume di destinazione.

- **Tipo di operazione**

Visualizza il tipo di trasferimento del volume.

- **Risultato dell'operazione**

  Visualizza se il trasferimento del volume è stato eseguito correttamente.

- **Ora di inizio trasferimento**

  Visualizza l'ora di inizio del trasferimento del volume.

- **Ora di fine trasferimento**

  Visualizza l'ora di fine del trasferimento del volume.

- **Durata trasferimento**

  Visualizza il tempo impiegato (in ore) per completare il trasferimento del volume.

- **Dimensione trasferimento**

  Visualizza le dimensioni (in MB) del volume trasferito.

- **SVM di origine**

  Visualizza il nome della SVM (Storage Virtual Machine).

- **Cluster di origine**

  Visualizza il nome del cluster di origine.

- **SVM di destinazione**

  Visualizza il nome SVM di destinazione.

- **Cluster di destinazione**

  Visualizza il nome del cluster di destinazione.

Informazioni correlate

- Per informazioni sulla vista **relazione: Tutte le relazioni**, vedere "Relazione: Vista tutte le relazioni".
- Per informazioni sulla vista **Relationship:MetroCluster**, vedere "Monitoraggio delle configurazioni MetroCluster".
- Per informazioni sulla vista **relazione: Tutte le relazioni**, vedere "Relazione: Vista tasso di trasferimento dell'ultimo mese".

Relazione: Vista tasso di trasferimento dell'ultimo mese

La vista Relationship: Last 1 Month Transfer Rate consente di analizzare la quantità di volume di dati che viene trasferita giorno per giorno per i volumi in relazioni asincrone. Questa pagina fornisce inoltre informazioni dettagliate sui trasferimenti giornalieri e sul tempo necessario per completare l'operazione di trasferimento per volumi e macchine virtuali di storage.

I controlli nella parte superiore della pagina consentono di eseguire ricerche per individuare oggetti specifici, creare e applicare filtri per restringere l'elenco dei dati visualizzati, aggiungere/rimuovere/riordinare le colonne della pagina ed esportare i dati della pagina in un file .csv, .pdf o .xlsx. Dopo aver personalizzato la pagina, è possibile salvare i risultati come vista personalizzata e pianificare un report dei dati da generare e inviare via email a intervalli regolari. Ad esempio, se si desidera visualizzare le relazioni dei volumi, è possibile accedere al menu **Storage** > **Volumes** > **Relationship: Last 1 Month Transfer Rate** (velocità di trasferimento ultimo 1 mese) oppure al menu **Protection** > **Relationship** > **Relationship:Last 1 Month Transfer Rate** (protezione* > **Relazioni** > **rapporti** > *rapporti: Velocità di trasferimento ultimo 1 mese) e utilizzare

- **Dimensione trasferimento totale**

  Visualizza le dimensioni totali del trasferimento del volume in gigabyte.

- **Giorno**

  Visualizza il giorno in cui è stato avviato il trasferimento del volume.

- **Ora di fine**

  Visualizza l'ora di fine del trasferimento del volume con la data.

Informazioni correlate

- Per informazioni sulla vista **Relationship:MetroCluster**, vedere "Monitoraggio delle configurazioni MetroCluster".
- Per informazioni sulla vista **Relationship: Last 1 Month Transfer Status** (relazione: Stato trasferimento ultimo 1 mese), vedere "Relazione: Vista Stato trasferimento ultimo 1 mese".
- Per informazioni sulla vista **relazione: Tutte le relazioni**, vedere "Relazione: Vista tasso di trasferimento dell'ultimo mese"

Generare report personalizzati

Reporting di Unified Manager

Active IQ Unified Manager (in precedenza Unified Manager di OnCommand) consente di visualizzare, personalizzare, scaricare e pianificare report per i sistemi storage ONTAP. I report possono fornire dettagli sulla capacità, lo stato di salute, le performance, la sicurezza e le relazioni di protezione del sistema di storage.

La nuova funzionalità di reporting e scheduling di Unified Manager introdotta in Active IQ Unified Manager 9.6 sostituisce il precedente motore di reporting che era stato ritirato nella versione 9.5 di Unified Manager.

Il reporting offre diverse viste della rete, offrendo informazioni pratiche su capacità, stato di salute, performance, sicurezza e dati di protezione. È possibile personalizzare le visualizzazioni visualizzando, nascondendo e riordinando le colonne, filtrando i dati, ordinando i dati, e la ricerca dei risultati. È possibile salvare visualizzazioni personalizzate per il riutilizzo, scaricarle come report e pianificarle come report ricorrenti da distribuire tramite e-mail.

È possibile scaricare le viste in formato Microsoft® Excel e personalizzarle. È possibile utilizzare funzionalità avanzate di Excel, come ordinamento complesso, filtri a più livelli, tabelle pivot e grafici. Una volta soddisfatto del report Excel risultante, è possibile caricare il file Excel per utilizzarlo ogni volta che il report viene pianificato e condiviso.

Oltre a generare report dall'interfaccia utente, è possibile estrarre dati relativi a stato, sicurezza e performance da Unified Manager utilizzando i seguenti metodi aggiuntivi:

- Utilizzo degli strumenti ODBC (Open Database Connectivity) e ODBC per accedere direttamente al database per ottenere informazioni sul cluster
- Esecuzione delle API REST di Unified Manager per restituire le informazioni che si desidera esaminare

Da questa release di Active IQ Unified Manager, i report sono stati migliorati in base ai seguenti miglioramenti:

- Viene inviato un messaggio di posta elettronica per un report in base alla pianificazione configurata. Anche quando si genera un report on-demand, si riceverà un'e-mail.
- Il nome file del report e i metadati del report includono il nome host da cui è stato generato il report. Anche se qualcuno cambia il nome del file, è comunque possibile identificare il nome host da cui è stato generato il report a causa di questo miglioramento.

Access point per la generazione di report

È possibile raccogliere informazioni in Unified Manager sui cluster per creare report dall'interfaccia utente, dalle query del database MySQL e dalle API REST.

Queste sezioni descrivono la creazione di report e la pianificazione di Unified Manager attraverso l'interfaccia utente.

Sono disponibili tre modi per accedere alle funzionalità di reporting fornite da Unified Manager:

- Estrazione dei dati direttamente dalle pagine di inventario nell'interfaccia utente.
- Utilizzo degli strumenti ODBC (Open Database Connectivity) e ODBC per accedere a tutti gli oggetti disponibili.

- Esecuzione delle API REST di Unified Manager per restituire le informazioni che si desidera esaminare.

Queste sezioni descrivono la creazione di report e la pianificazione di Unified Manager attraverso l'interfaccia utente.

Database di Unified Manager accessibili per la creazione di report personalizzati

Unified Manager utilizza un database MySQL per memorizzare i dati dei cluster monitorati. I dati vengono memorizzati in diversi schemi nel database MySQL.

Sono disponibili tutti i dati delle tabelle dei seguenti database:

Database	Descrizione
modello_netapp	Dati sugli oggetti nei controller ONTAP.
vista_modello_netapp	Dati sugli oggetti sui controller ONTAP, adatti per il consumo degli strumenti di report.
netapp_performance	Contatori delle performance specifici del cluster.
ocum	Dati e informazioni dell'applicazione Unified Manager per supportare il filtraggio, l'ordinamento e il calcolo di alcuni campi derivati dell'interfaccia utente.
ocum_report	Dati per la configurazione dell'inventario e informazioni relative alla capacità.
ocum_report_birt	Viste per la configurazione dell'inventario e i dati relativi alla capacità, adatte per il consumo degli strumenti di report.
opm	Impostazioni di configurazione delle performance e informazioni sulle soglie.
scalemonitor	Dati relativi allo stato di salute e ai problemi di performance dell'applicazione Unified Manager.
modello_vmware	Dati a oggetti VMware per datastore ospitati sullo storage NetApp.
vista_modello_vmware	Viste per i dati a oggetti VMware per datastore ospitati sullo storage NetApp, adatte per l'utilizzo dei tool di report.
vmware_performance	Dati del contatore delle performance VMware per datastore ospitati sullo storage NetApp.

Un utente di reporting — un utente di database con il ruolo Schema report — è in grado di accedere ai dati in

queste tabelle. Questo utente ha accesso in sola lettura ai report e ad altre viste del database direttamente dal database di Unified Manager. Si noti che questo utente non dispone dell'autorizzazione per accedere alle tabelle che contengono dati utente o informazioni sulle credenziali del cluster.

API REST di Unified Manager che possono essere utilizzate per il reporting

È possibile utilizzare le API REST per gestire i cluster visualizzando le informazioni relative a stato, capacità, performance e sicurezza acquisite da Unified Manager.

Le API REST sono esposte attraverso la pagina web di Swagger. È possibile accedere alla pagina Web di Swagger per visualizzare la documentazione dell'API REST di Unified Manager e per eseguire manualmente una chiamata API. Dall'interfaccia utente Web di Unified Manager, nella barra dei menu, fare clic sul pulsante **Help** (Guida), quindi selezionare **API Documentation** (documentazione API). Per informazioni sulle API REST di Unified Manager, vedere "Introduzione alle API REST di Active IQ Unified Manager".

Per accedere alle API REST, è necessario disporre del ruolo di operatore, amministratore dello storage o amministratore dell'applicazione.

Informazioni sui report

I report visualizzano informazioni dettagliate su storage, rete, qualità del servizio e relazioni di protezione, aiutandoti a identificare e risolvere potenziali problemi prima che si verifichino.

Quando si personalizza una vista, è possibile salvarla con un nome univoco per un utilizzo futuro. È possibile pianificare l'esecuzione regolare di un report basato su tale visualizzazione e condividerlo con altri utenti. È inoltre possibile scaricare la vista in Excel per personalizzarla utilizzando le funzionalità avanzate di Excel, quindi caricare nuovamente il file in Unified Manager . Se si pianifica un report utilizzando tale vista, verrà utilizzato il file Excel caricato per creare report affidabili che è possibile condividere.

È possibile gestire tutti i report pianificati dalla pagina Report Schedules.

> Per gestire i report, è necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile scaricare i report come file CSV (comma-Separated Values), Excel o PDF.

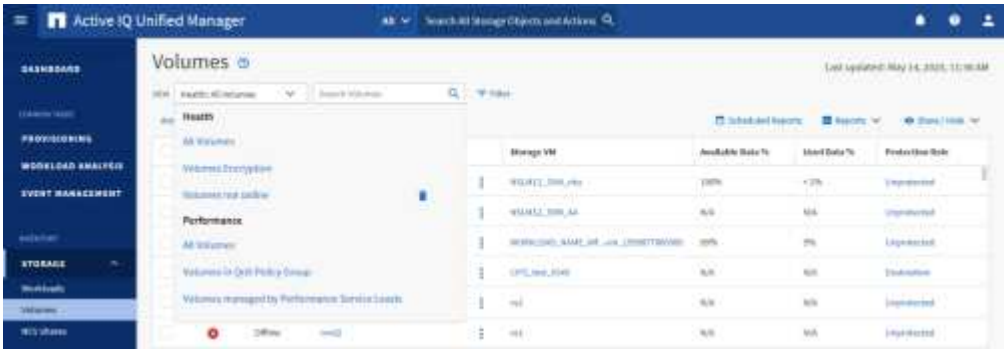
Comprensione della relazione tra visualizzazione e report

Le visualizzazioni e le pagine di inventario diventano report quando vengono scaricate o programmate.

È possibile personalizzare e salvare viste e pagine di inventario per il riutilizzo. Quasi tutto ciò che è possibile visualizzare in Unified Manager può essere salvato, riutilizzato, personalizzato, pianificato e condiviso come report.

Nell'elenco a discesa della vista, gli elementi con l'icona di eliminazione sono viste personalizzate esistenti create dall'utente o da un altro utente. Gli elementi senza icona sono viste predefinite fornite con Unified Manager. Le viste predefinite non possono essere modificate o eliminate.

- Se si elimina una vista personalizzata dall'elenco, vengono eliminati anche i file Excel o i report pianificati che utilizzano tale vista.
- Se si modifica una vista personalizzata, i report che utilizzano tale vista rifletteranno la modifica alla successiva generazione e invio del report tramite e-mail in base alla pianificazione del report. Quando si modificano le viste, assicurarsi che le modifiche funzionino con le personalizzazioni Excel associate utilizzate per i report. Se necessario, è possibile aggiornare il file Excel scaricandolo, apportando le modifiche necessarie e caricandolo come nuova personalizzazione Excel per la vista.



Solo gli utenti con il ruolo di amministratore dell'applicazione o di amministratore dello storage possono visualizzare l'icona di eliminazione, modificare o eliminare una vista o modificare o eliminare un report pianificato.

Tipi di report

Questa tabella fornisce un elenco completo delle visualizzazioni e delle pagine di inventario disponibili come report personalizzabili, scaricabili e pianificati.

Report Active IQ Unified Manager

Tipo	Oggetto di storage o di rete
Capacità	Cluster Aggregati Volumi Qtree

Tipo	Oggetto di storage o di rete
Salute	Cluster Nodi Aggregati VM di storage Volumi Condivisioni SMB/CIFS Condivisioni NFS
Performance	Cluster Nodi Aggregati VM di storage Volumi LUN Spazi dei nomi NVMe Interfacce di rete (LIF) Porte
Qualità del servizio	Gruppi di policy QoS tradizionali Gruppi di policy QoS adattivi Gruppi di criteri del livello di servizio delle performance
Relazioni di protezione dei volumi (disponibili nella pagina volumi)	Tutte le relazioni Stato del trasferimento degli ultimi 1 mese Tasso di trasferimento degli ultimi 1 mese
Sicurezza	VM di storage Cluster

Limiti di reporting

La nuova funzionalità di reporting di Active IQ Unified Manager presenta alcuni limiti di cui si dovrebbe essere a conoscenza.

Report esistenti delle versioni precedenti di Unified Manager

È possibile modificare solo la pianificazione e i destinatari dei report esistenti creati e importati (come file .rptdesign) in Unified Manager 9.5 e versioni precedenti. Se si personalizzano i report standard forniti con Unified Manager 9.5 o versioni precedenti, questi report personalizzati non vengono importati nel nuovo tool di reporting.

Se è necessario modificare i report esistenti importati dai file .rptdesign, eseguire una delle seguenti operazioni e rimuovere il report importato:

- creare una nuova vista e pianificare un report da tale vista (preferita)
- Passare il mouse sul report, copiare SQL ed estrarre i dati utilizzando uno strumento esterno

Le viste predefinite possono essere generate come report senza la necessità di alcuna personalizzazione. È possibile utilizzare la nuova soluzione di reporting per ricreare i report personalizzati.

Pianificazione e relazione

È possibile creare diverse pianificazioni con qualsiasi combinazione di destinatari per ciascun report salvato. Tuttavia, non è possibile riutilizzare la pianificazione per più report.

Protezione dei report

Qualsiasi utente con le autorizzazioni appropriate può modificare o eliminare i report. Non esiste alcun modo per impedire ad altri utenti di rimuovere o apportare modifiche alle viste o alle pianificazioni salvate.

Report sugli eventi

Sebbene sia possibile personalizzare la visualizzazione degli eventi e scaricare il report risultante in formato CSV, non è possibile pianificare report di eventi ricorrenti per la generazione e la distribuzione.

Allegati dei report

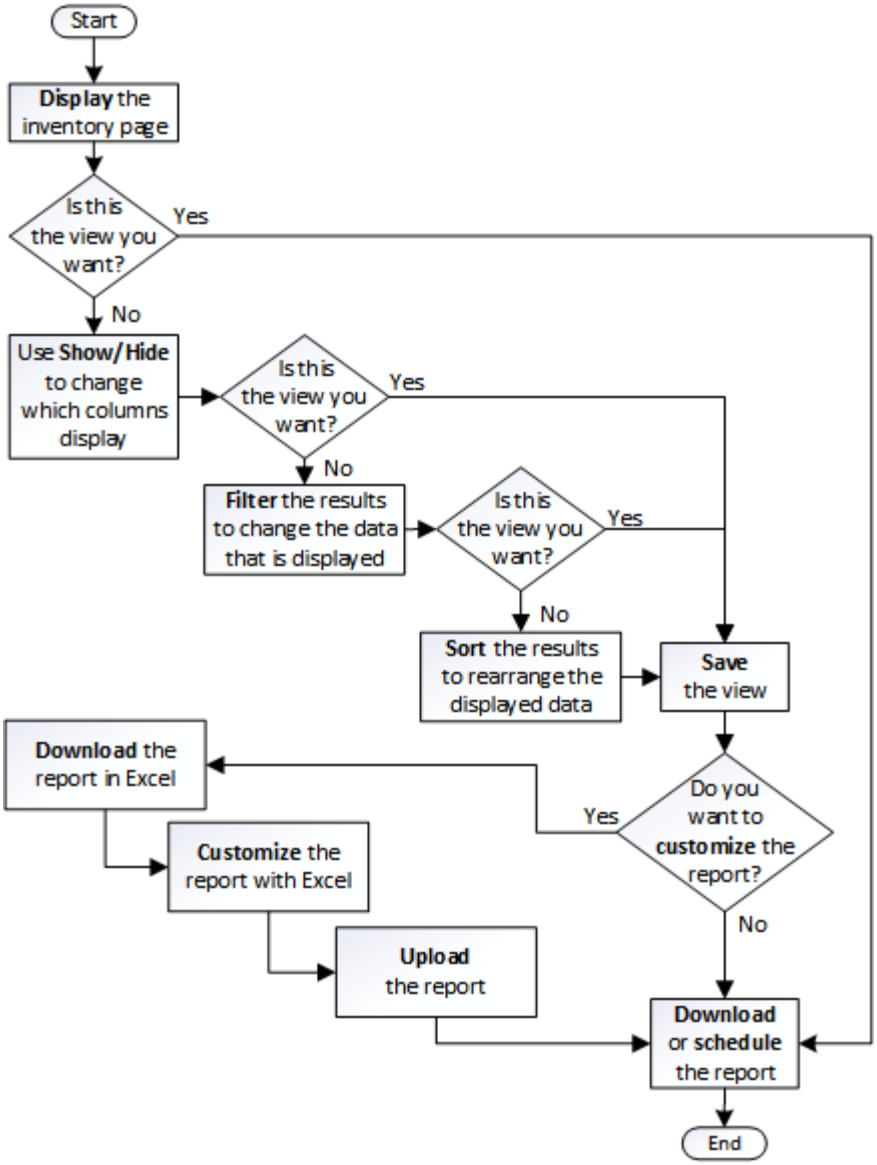
I report non possono essere inviati nel corpo di un messaggio e-mail. I report vengono invece inviati solo come allegati PDF, Excel o CSV.

Utilizzo dei report

Scopri come trovare e personalizzare le visualizzazioni delle pagine di inventario in report pianificati condivisibili.

Workflow dei report

Struttura decisionale che descrive il flusso di lavoro del report.



Avvio rapido dei report

Crea un report personalizzato di esempio per esplorare le viste e pianificare i report. Questo report di avvio rapido trova un elenco di volumi che potresti voler spostare al livello cloud perché esiste una quantità sufficiente di dati inattivi (cold). Si apre la vista Performance: All Volumes (prestazioni: Tutti i volumi), si personalizza la vista utilizzando filtri e colonne, si salva la vista personalizzata come report e si pianifica la condivisione del report una volta alla settimana.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver configurato gli aggregati FabricPool e avere volumi su tali aggregati.

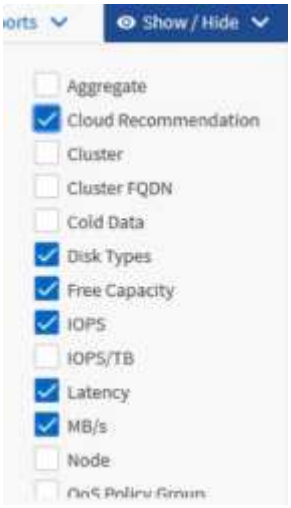
Attenersi alla procedura riportata di seguito per:

- Aprire la vista predefinita

- Personalizzare le colonne filtrando e ordinando i dati
- Salvare la vista
- Pianificare la creazione di un report per la visualizzazione personalizzata

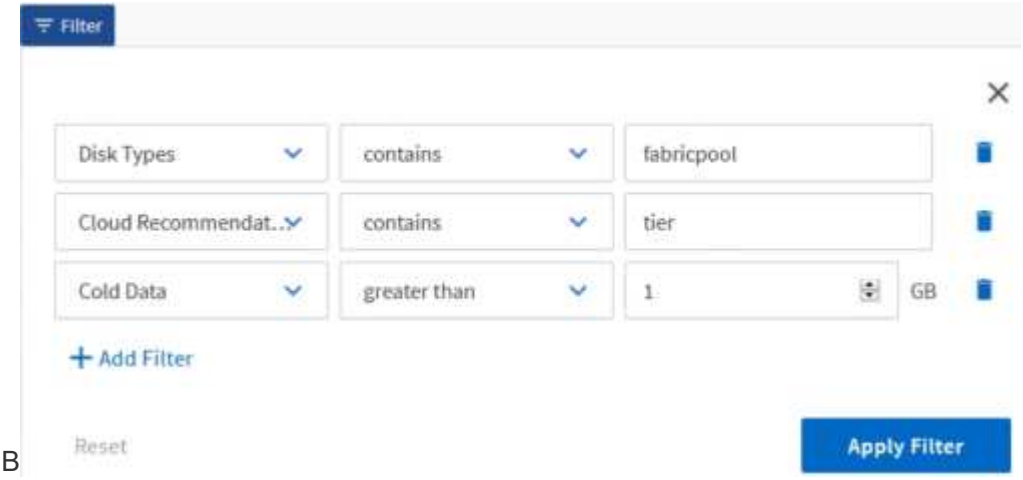
Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu View (Visualizza), selezionare **Performance** (prestazioni) > **All Volumes** (tutti i volumi).
3. Fare clic su **Show/Hide** (Mostra/Nascondi) per assicurarsi che la colonna "isk Types `D`" (tipi di disco) venga visualizzata nella vista.



Aggiungere o rimuovere altre colonne per creare una vista contenente i campi importanti per il report.

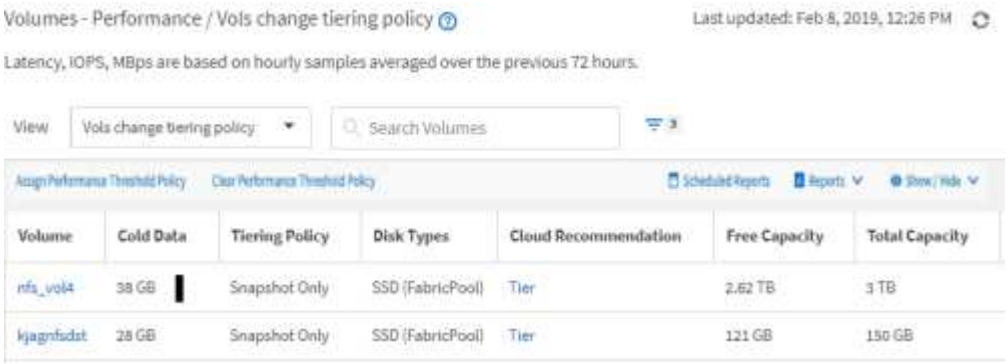
4. Trascina la colonna “Disk types” accanto alla colonna “Cloud Recommendation”.
5. Fare clic sull’icona del filtro per aggiungere i tre filtri seguenti, quindi fare clic su **Apply Filter** (Applica filtro):
   - I tipi di disco contengono FabricPool
   - Cloud Recommendation contiene Tier
   - Cold Data superiore a 10



GB

Si noti che ogni filtro viene Unito a un logico E che tutti i volumi restituiti devono soddisfare tutti i criteri. È possibile aggiungere un massimo di cinque filtri.

6. Fare clic sulla parte superiore della colonna Cold Data (dati a freddo) per ordinare i risultati in modo che i volumi con i dati più a freddo vengano visualizzati nella parte superiore della vista.
7. Quando la vista viene personalizzata, il nome della vista è Vista non salvata. Assegnare un nome alla vista in modo che rifletta ciò che viene visualizzato, ad esempio “VOL change Tiering policy”. Al termine, fare clic sul segno di spunta o premere **Invio** per salvare la vista con il nuovo nome.



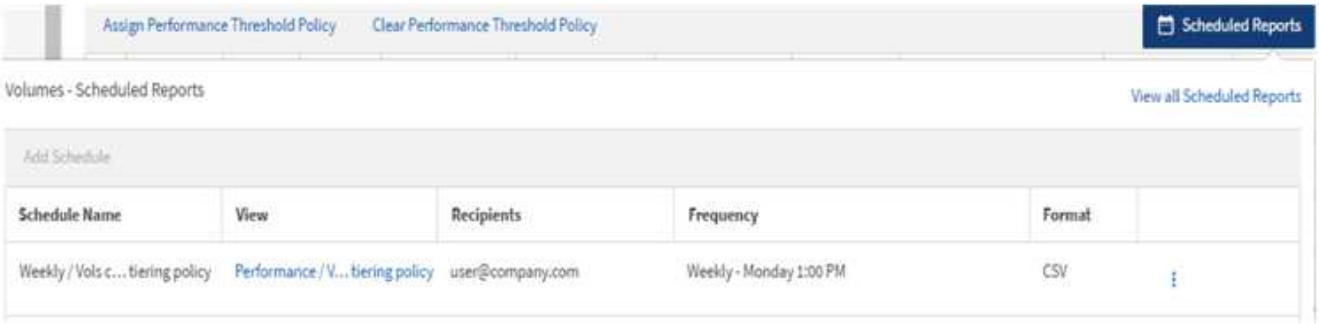
8. Scarica il report come file **CSV**, **Excel** o **PDF** per visualizzare l’output prima di programmarlo o condividerlo.

   Aprire il file con un’applicazione installata, ad esempio Microsoft Excel (CSV o Excel) o Adobe Acrobat (PDF), oppure salvarlo.

   È possibile personalizzare ulteriormente il report utilizzando filtri, ordinazioni, tabelle pivot o grafici complessi scaricando la vista come file Excel. Dopo aver aperto il file in Excel, utilizzare le funzionalità avanzate per personalizzare il report. Quando soddisfatto, caricare il file Excel. Questo file, con le sue personalizzazioni, viene applicato alla vista quando viene eseguito il report.

   Per ulteriori informazioni sulla personalizzazione dei report con Excel, consulta *esempi di report Microsoft Excel*.

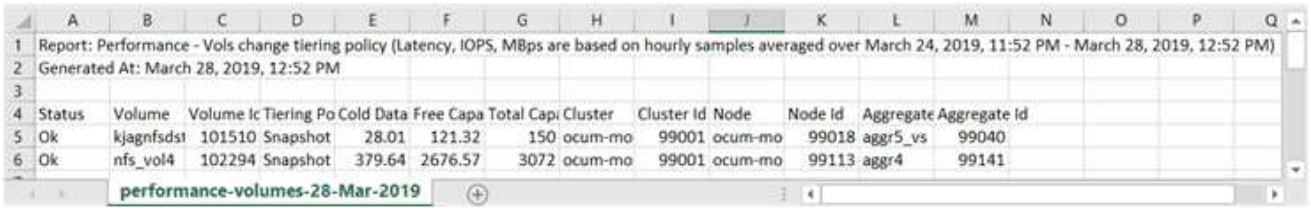
9. Fare clic sul pulsante **Report pianificati** nella pagina dell’inventario. Tutti i report pianificati relativi all’oggetto, in questo caso i volumi, vengono visualizzati nell’elenco.



10. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report Schedule (Pianificazioni report) in modo da definire le caratteristiche di pianificazione per il nuovo report.
11. Immettere un nome per il report e completare gli altri campi, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

Il seguente report di esempio è in formato CSV:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:52 PM - March 28, 2019, 12:52 PM)																
2	Generated At: March 28, 2019, 12:52 PM																
3																	
4	Status	Volume	Volume Ic	Tiering Po	Cold Data	Free Capa	Total Capi	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id				
5	Ok	kjagnfsdst	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040				
6	Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141				

performance-volumes-28-Mar-2019

Il seguente report di esempio è in formato PDF:

Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:51 PM - March 28, 2019, 12:51 PM)
Generated At: March 28, 2019, 12:51 PM

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok								
Ok								

In base ai risultati mostrati nel report, è possibile utilizzare Gestione di sistema di ONTAP o l'interfaccia CLI di ONTAP per modificare la policy di tiering in "auto" o "all" per alcuni volumi per trasferire più dati cold al livello cloud.

Ricerca di un report pianificato

È possibile cercare i report pianificati per nome, nome della vista, tipo di oggetto o destinatari.

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Report Schedules**.
2. Utilizzare il campo di testo **Cerca report pianificati**.

Per trovare i report in base a…	**Prova…**
Nome pianificazione	Digitare parte del nome della pianificazione del report.
Nome della vista	Digitare parte del nome della vista del report. Le viste predefinite e personalizzate vengono visualizzate nell'elenco delle viste.
Destinatario	Digitare parte dell'indirizzo e-mail.
Tipo di file	Digitare "PDF", "CSV" o "XLSX".

3. È possibile fare clic sull'intestazione di una colonna per ordinare i report in ordine crescente o decrescente in base alla colonna, ad esempio il nome o il formato del programma.

Personalizzazione dei report

Esistono diversi modi per personalizzare le viste in modo da poter creare un report contenente tutte le informazioni necessarie per gestire i cluster ONTAP.

Iniziare con una pagina di inventario predefinita o una vista personalizzata, quindi personalizzarla aggiungendo o rimuovendo colonne, modificando l'ordine delle colonne, filtrando i dati o ordinando una colonna specifica in ordine crescente o decrescente.

A partire da Unified Manager 9.8, è anche possibile scaricare la vista in Excel per personalizzarla utilizzando funzionalità avanzate. Al termine, caricare il file Excel personalizzato. Se si pianifica un report utilizzando tale vista, il report viene utilizzato dal file Excel personalizzato per creare report affidabili che è possibile condividere.

Per ulteriori informazioni sulla personalizzazione dei report con Excel, consulta *esempi di report Microsoft Excel*.

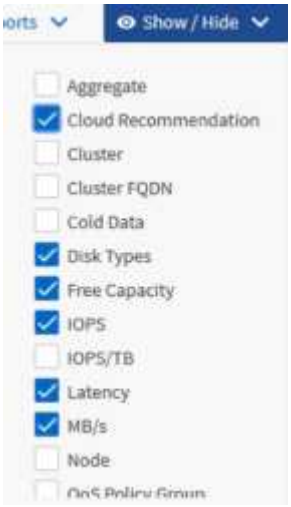
Per gestire i report, è necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Personalizzazione delle colonne

Utilizzare **Mostra/Nascondi** per scegliere le colonne da utilizzare nel report. Trascinare le colonne nella pagina di inventario per riorganizzarle.

Fasi

1. Fare clic su **Mostra/Nascondi** per aggiungere o rimuovere le colonne.



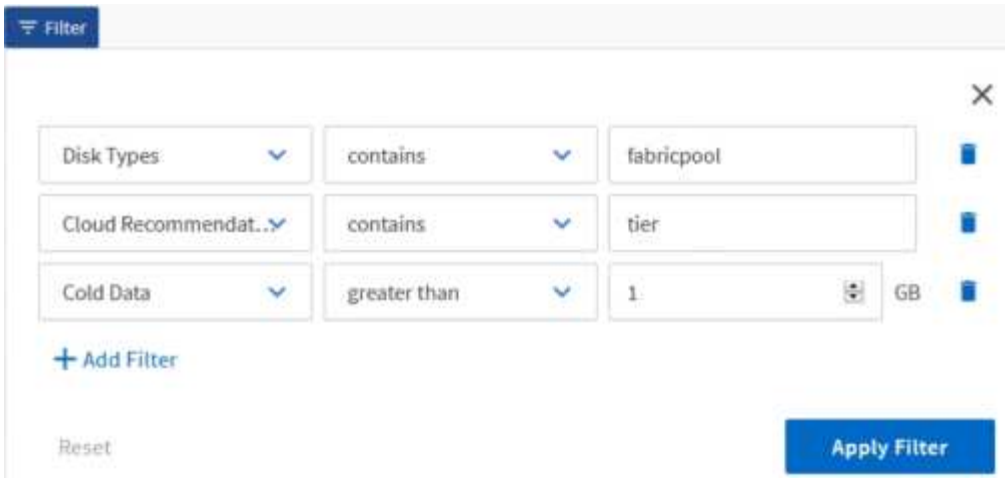
2. Nella pagina di inventario, trascinare le colonne per riorganizzarle nell'ordine desiderato nel report.
3. Assegnare un nome alla vista non salvata per salvare le modifiche.

Filtraggio dei dati

Filtrare i dati per assicurarsi che i risultati corrispondano ai requisiti del report. Il filtraggio consente di visualizzare solo i dati interessati.

Fasi

1. Fare clic sull'icona del filtro per aggiungere filtri per mettere a fuoco i risultati da visualizzare, quindi fare clic su **Applica filtro**.



2. Assegnare un nome alla vista non salvata per salvare le modifiche.

Ordinamento dei dati

Per ordinare i risultati, fare clic su una colonna e indicare l'ordine crescente o decrescente. L'ordinamento dei dati assegna la priorità alle informazioni necessarie per il report.

Fasi

1. Fare clic sulla parte superiore di una colonna per ordinare i risultati in modo che le informazioni più importanti siano visualizzate nella parte superiore della vista.
2. Assegnare un nome alla vista non salvata per salvare le modifiche.

Utilizzare la funzione di ricerca per perfezionare la visualizzazione

Dopo aver ottenuto la visualizzazione desiderata, è possibile perfezionare ulteriormente i risultati utilizzando il campo Cerca per concentrarsi sui risultati che si desidera includere nel report.

Fasi

1. Aprire la vista personalizzata o predefinita che si desidera utilizzare come base del report.
2. Digitare il campo Search (Cerca) per perfezionare i dati elencati nella vista. È possibile inserire dati parziali in una qualsiasi delle colonne visualizzate. Ad esempio, se si desidera cercare i nodi che includono "US_East" nel nome, è possibile perfezionare l'elenco completo dei nodi.

   I risultati della ricerca vengono salvati nella vista personalizzata e utilizzati nel report pianificato risultante.

3. Assegnare un nome alla vista non salvata per salvare le modifiche.

Utilizzo di Excel per personalizzare il report

Dopo aver salvato la vista, è possibile scaricarla in formato Excel Workbook (.xlsx). Quando si apre il file Excel, è possibile utilizzare le funzionalità avanzate di Excel per personalizzare il report.

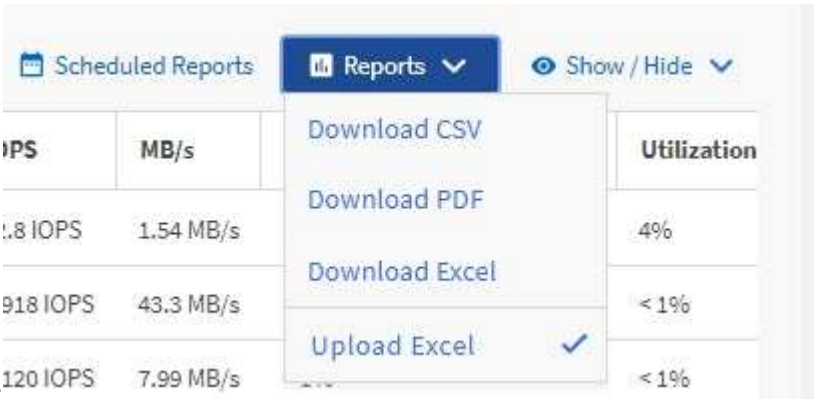
Cosa ti serve

È possibile caricare un file Excel Workbook solo con estensione xlsx.

Ad esempio, alcune funzionalità avanzate di Excel che è possibile utilizzare nel report includono:

- Ordinamento a più colonne
- Filtraggio complesso
- Tavole pivot
- Grafici

- Il file Excel scaricato utilizza il nome file predefinito per la vista, non il nome salvato.
  - Il formato è `<View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx`.
  - Ad esempio, una vista salvata personalizzata denominata `Volumes-not online` ha un nome file di `health-volumes-05-May-2020-19-18-00.xlsx` se salvato in quel giorno e in quel momento.
- È possibile aggiungere fogli al file Excel, ma non modificare i fogli esistenti.
  - Non modificare i fogli, i dati e le informazioni esistenti. Copiare invece i dati in una nuova pagina creata.
  - Un'eccezione alla regola sopra indicata è la possibilità di creare formule nella pagina "data". Utilizzare le formule della pagina dati per creare grafici sulle nuove pagine.
  - Non assegnare un nome a nuovi dati o informazioni del foglio.
- Se esiste un file Excel personalizzato, è presente un segno di spunta accanto alla voce di menu **Report** > **carica Excel**. Quando si scarica il file Excel, viene utilizzata la versione con le personalizzazioni.



Fasi

1. Aprire la vista predefinita, personalizzata o salvata che si desidera utilizzare come base del report.
2. Selezionare **Report** > **Download Excel**.
3. Salvare il file. Il file viene salvato nella cartella dei download.
4. Aprire il file salvato in Excel. Non spostare il file in una nuova posizione o, se si lavora in un'altra posizione, salvarlo nuovamente nella posizione originale utilizzando il nome del file originale prima di caricarlo.
5. Personalizzare il file utilizzando le funzionalità di Excel, ad esempio ordinazioni complesse, filtri stratificati, tabelle pivot o grafici. Per ulteriori informazioni, consultare la documentazione di Microsoft® Excel.
6. Selezionare **Report** > **carica Excel** e selezionare il file modificato. Il file scaricato più di recente viene caricato dalla stessa posizione del file.

7. Inviare un report di test utilizzando la funzione **Report pianificati**.

Download di report

È possibile scaricare report e salvare i dati su un'unità locale o di rete come file CSV (comma-Separated Values), Microsoft Excel (.XLSX) o PDF. È possibile aprire file CSV e XLSX con applicazioni per fogli di calcolo, come Microsoft Excel, e file PDF con lettori come Adobe Acrobat.

Fasi

1. Fare clic sul pulsante **Report** per scaricare il report come indicato di seguito:

Scegliere	Per…
Scarica CSV	Salvare il report come file CSV (comma-Separated Values).
Scarica il PDF	Salvare il report come file .pdf.
Scarica Excel	Salvare il report come file Microsoft Excel (XLSX).

Pianificazione dei report

Una volta che si desidera riutilizzare una vista e condividerla come report, è possibile pianificarla utilizzando Active IQ Unified Manager. È possibile gestire i report pianificati, modificando i destinatari e la frequenza di distribuzione per ogni pianificazione del report.

È possibile pianificare la maggior parte delle visualizzazioni o delle pagine di inventario in Unified Manager. Le eccezioni sono gli eventi, ovvero i report che è possibile scaricare come file CSV, ma non è possibile pianificare gli eventi per la rigenerazione e la condivisione. Non è inoltre possibile scaricare o pianificare dashboard, preferiti o pagine di configurazione.

A partire da Active IQ Unified Manager 9.8, è possibile scaricare le viste in formato Microsoft® Excel e personalizzarle. È possibile utilizzare funzionalità avanzate di Excel come ordinamento complesso, filtri a livelli, tabelle pivot e grafici. Una volta soddisfatto del report Excel risultante, è possibile caricare il file Excel per utilizzarlo ogni volta che il report viene pianificato e condiviso.

È possibile pianificare le viste incorporate o personalizzate. È possibile scegliere il tipo di file da inviare, CSV, PDF o XSLX. Quando si pianifica un report per la prima volta, è possibile scaricarlo e assegnarlo come unico destinatario per visualizzare il report come verrà visualizzato dai destinatari.

Pianificazione di un report

Dopo aver creato una vista o un file Excel che si desidera pianificare per la generazione e la distribuzione regolari, è possibile pianificare il report.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

- È necessario aver configurato le impostazioni del server SMTP nella pagina **Generale** > **Notifiche** in modo che il motore di reporting possa inviare i report come allegati e-mail all'elenco di destinatari dal server Unified Manager.
- Il server di posta elettronica deve essere configurato per consentire l'invio degli allegati con i messaggi di posta elettronica generati.

Per verificare e pianificare la creazione di un report per una visualizzazione, procedere come segue. Selezionare o personalizzare la vista che si desidera utilizzare. La procedura seguente utilizza una vista di rete che mostra le prestazioni delle interfacce di rete, ma è possibile utilizzare qualsiasi vista desiderata.

Fasi

1. Aprire la vista. In questo esempio viene utilizzata la vista di rete predefinita che mostra le prestazioni LIF. Nel riquadro di spostamento a sinistra, fare clic su **Network > Network Interfaces** (rete > interfacce di rete).
2. Personalizzare la vista in base alle esigenze utilizzando le funzionalità integrate di Unified Manager.
3. Dopo aver personalizzato la vista, è possibile specificare un nome univoco nel campo **View** (Visualizza) e fare clic sul segno di spunta per salvarla.

4. È possibile utilizzare le funzionalità avanzate di Microsoft® Excel per personalizzare il report. Per ulteriori informazioni, vedere "Utilizzo di Excel per personalizzare il report".
5. Per visualizzare l'output prima di pianificarlo o condividerlo:

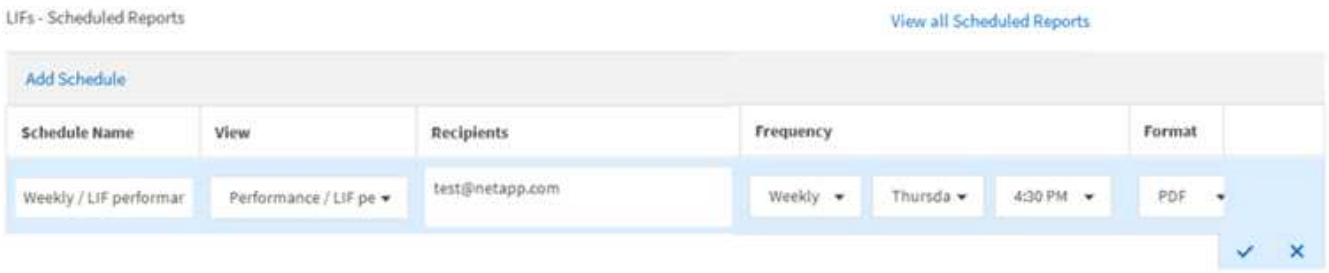
Opzione	Descrizione
Se si è utilizzato Excel per personalizzare il report	Visualizzare il file Excel scaricato esistente.
Se non si utilizza Excel per personalizzare il report	Scarica il report come file **CSV**, **PDF** o **XLSX**.

   Aprire il file con un'applicazione installata, ad esempio Microsoft Excel (CSV/XSLX) o Adobe Acrobat (PDF).

6. Se si è soddisfatti del report, fare clic su **Report pianificati**.
7. Nella pagina Report Schedules, fare clic su **Add Schedule** (Aggiungi pianificazione).
8. Accettare il nome predefinito, che è una combinazione del nome della vista e della frequenza, oppure personalizzare il nome del programma*.
9. Per eseguire il test del report pianificato per la prima volta, aggiungersi solo come **destinatario**. Se soddisfatto, aggiungere gli indirizzi e-mail per tutti i destinatari del report.
10. Specificare la frequenza con cui il report verrà generato e inviato ai destinatari. È possibile scegliere tra **giornaliero**, **settimanale** o **mensile**.
11. Selezionare il formato **PDF**, **CSV** o **XSLX**.

Per i report in cui è stato utilizzato Excel per personalizzare il contenuto, selezionare sempre **XSLX**.

12. Fare clic sul segno di spunta (✓) per salvare la pianificazione del report.



Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza pianificata.

Pianificazione dei report .rptdesign importati

È possibile pianificare i report esistenti creati e importati in una release precedente di Unified Manager.

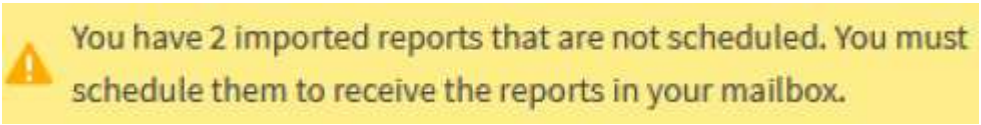
La pianificazione dei report importati richiede quanto segue:

- Report dei file .rptdesign progettati da BIRT importati in una release precedente di Unified Manager
- Applicabile quando si esegue l'aggiornamento a Unified Manager 9.6 GA o versione successiva

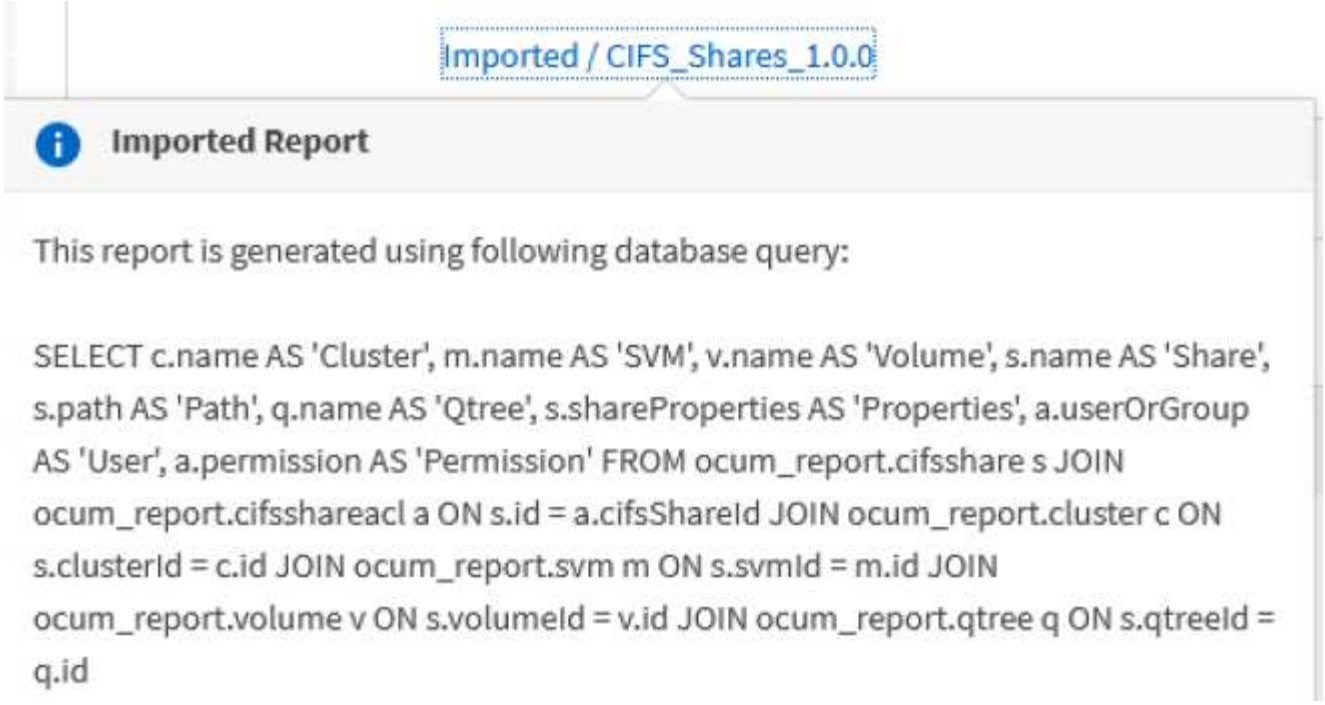
Dopo aver eseguito l'aggiornamento a Unified Manager 9.6 GA o versioni successive, la pagina Report Schedules elenca i report importati. È possibile modificare la pianificazione di questi report per specificare gli indirizzi e-mail, la frequenza e il formato del destinatario (PDF o CSV). In caso contrario, questi report non possono essere modificati o visualizzati nell'interfaccia utente di Unified Manager.

Fasi

1. Aprire la pagina Report Schedules. Se sono stati importati report, viene visualizzato un messaggio.



2. Fare clic sul nome **View** per visualizzare la query SQL utilizzata per generare il report.



3. Fare clic sull'icona Altro ⋮, Fare clic su **Edit** (Modifica), definire i dettagli della pianificazione del report e salvare il report.

   È inoltre possibile eliminare i report indesiderati dall'icona Altro ⋮.

Gestione delle pianificazioni dei report

È possibile gestire le pianificazioni dei report dalla pagina Report Schedules (Pianificazioni report). È possibile visualizzare, modificare o eliminare le pianificazioni esistenti.

Cosa ti serve

Non è possibile pianificare nuovi report dalla pagina Report Schedules. È possibile aggiungere solo report pianificati dalle pagine di inventario degli oggetti.

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Report Schedules**.
2. Nella pagina Report Schedules:

Se si desidera…	Quindi…
Visualizzare una pianificazione esistente	Scorrere l'elenco dei report esistenti utilizzando le barre di scorrimento e i controlli delle pagine.

Se si desidera…	Quindi…
Modificare una pianificazione esistente	a. Fare clic sull'icona Altro ⋮ per la pianificazione che si desidera utilizzare. b. Fare clic su **Edit** (Modifica). c. Apportare le modifiche necessarie. d. Fare clic sul segno di spunta per salvare le modifiche.
Eliminare una pianificazione esistente	a. Fare clic sull'icona Altro ⋮ per la pianificazione che si desidera utilizzare. b. Fare clic su **Delete** (Elimina). c. Conferma la tua decisione.

Modifica dei report pianificati

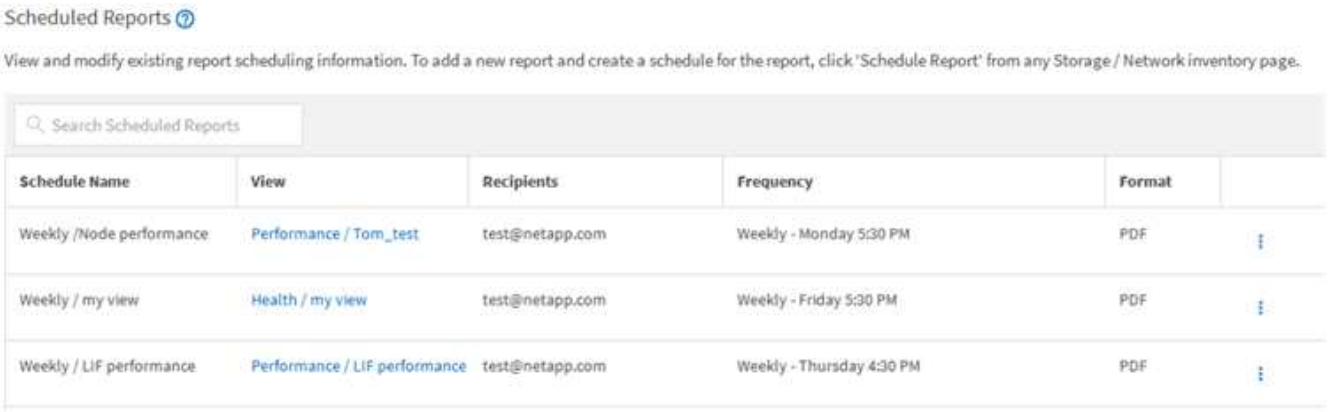
Una volta pianificati i report, è possibile modificarli nella pagina Report Schedules (Pianificazioni report).

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Report Schedules**.



> Se si dispone delle autorizzazioni appropriate, è possibile modificare qualsiasi report e la relativa pianificazione nel sistema.

2. Fare clic sull'icona Altro ⋮ per la pianificazione che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. È possibile modificare l'elenco **Nome pianificazione**, **destinatario**, **frequenza** e **formato** per la pianificazione del report.

5. Al termine, fare clic sul segno di spunta per salvare le modifiche.

Eliminazione dei report pianificati

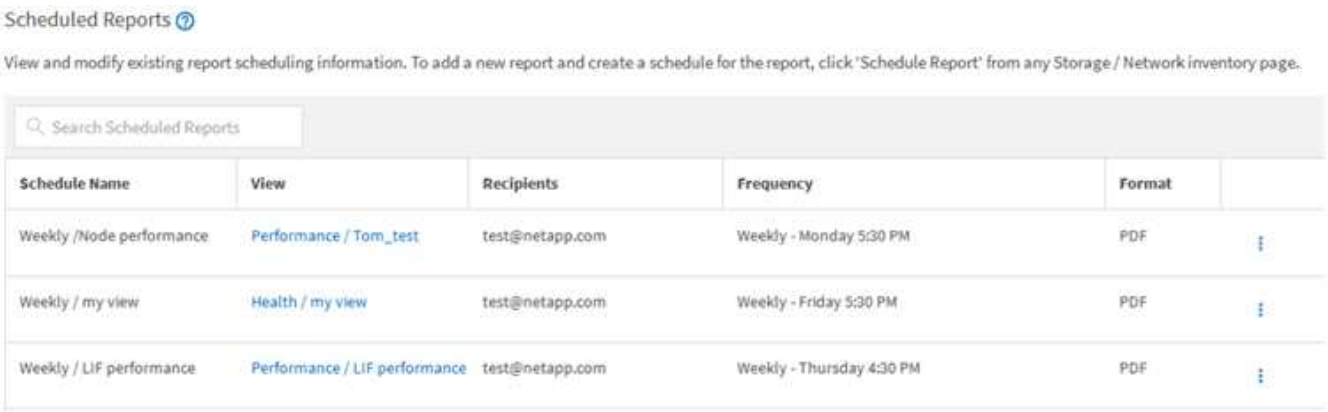
Una volta pianificati i report, è possibile eliminarli dalla pagina Report Schedules (Pianificazioni report).

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Report Schedules**.



Se si dispone delle autorizzazioni appropriate, è possibile rimuovere qualsiasi report e la relativa pianificazione nel sistema.

2. Fare clic sull'icona Altro ⋮ per la pianificazione che si desidera rimuovere.
3. Fare clic su **Delete** (Elimina).
4. Conferma la tua decisione.

   Il report pianificato viene rimosso dall'elenco e non verrà più generato e distribuito secondo la pianificazione impostata.

Se si elimina una vista personalizzata dalla pagina di inventario, vengono eliminati anche i file Excel personalizzati o i report pianificati che utilizzano tale vista.

Report personalizzati di esempio

Questi report personalizzati di esempio vengono comunemente utilizzati per identificare potenziali problemi e per rispondere a potenziali problemi prima che si verifichino.

L'elenco dei report in questa sezione non è esaustivo e crescerà nel tempo. È possibile suggerire report personalizzati da aggiungere a questa sezione fornendo feedback sulla documentazione.

Per gestire i report, è necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Personalizzazione dei report dello storage in cluster

I report di esempio relativi allo storage dei cluster di questa sezione sono solo esempi che consentono di comprendere come creare report sulla capacità dei cluster per monitorare le risorse del sistema di storage.

Creazione di un report per visualizzare la capacità in base al modello di cluster

È possibile creare un report per analizzare la capacità dello storage e l'utilizzo dei cluster in base al modello di sistema storage.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata che visualizzi la capacità in base al modello di cluster, quindi pianificare la creazione di un report per tale vista.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Clusters**.
2. Nel menu Visualizza, selezionare **capacità** > **tutti i cluster**.
3. Selezionare **Mostra/Nascondi** per rimuovere eventuali colonne, ad esempio "Cluster FQDN" e "OS Version", che non si desidera includere nel report.
4. Trascinare "Total Raw Capacity", "odel/Family`" e le tre colonne aggregate vicino alla colonna "Cluster `M".
5. Fare clic sulla parte superiore della colonna "Model/Family" per ordinare i risultati in base al tipo di cluster.
6. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "Capacity by Cluster Model" (capacità per modello cluster).
7. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
8. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina **Report Schedule** (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
9. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile aggiungere maggiore capacità a determinati cluster o aggiornare modelli di cluster meno recenti.

Creazione di un report per identificare i cluster con la capacità LUN più non allocata

È possibile creare un report per trovare i cluster con la capacità LUN più non allocata, superiore a 0,5 TB, per identificare dove è possibile aggiungere ulteriori carichi di lavoro.

Cosa serve * è necessario avere il ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata che visualizzi i cluster con la capacità LUN non allocata più, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Clusters**.
2. Nel menu Visualizza, selezionare **capacità** > **tutti i cluster**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Trascinare la colonna "Unallocated LUN Capacity" (capacità LUN non allocata) vicino alla colonna "ha Pair" (coppia ha).
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro, quindi fare clic su **Applica filtro**:
   - Capacità LUN non allocata superiore a 0.5 TB
6. Fare clic nella parte superiore della colonna "Unallocated LUN Capacity" (capacità LUN non allocata) per ordinare i risultati in base alla quantità massima di capacità LUN non allocata.
7. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "MOST unallocated LUN Capacity" (capacità LUN non allocata OST) e fare clic sul segno di spunta (✓).
8. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
9. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report Schedule (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
10. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile utilizzare la capacità LUN non allocata del cluster.

Creazione di un report per visualizzare le coppie ha con la capacità più disponibile

È possibile creare un report per trovare le coppie ad alta disponibilità (ha) con la maggiore capacità per il provisioning di nuovi volumi e LUN.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Utilizzare i seguenti passaggi per creare una vista personalizzata che visualizzi le coppie ha ordinate in base alla capacità più disponibile per il provisioning di nuovi volumi e LUN, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Clusters**.
2. Nel menu Visualizza, selezionare **capacità** > **tutti i cluster**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Trascinare la colonna "aggregate Unused Capacity" vicino alla colonna "ha Pair".

5. Fare clic sull'icona del filtro, aggiungere il seguente filtro, quindi fare clic su **Applica filtro**:
   - Capacità aggregata inutilizzata superiore a 0.5 TB
6. Fare clic nella parte superiore della colonna "aggregate Unused Capacity" (capacità non utilizzata aggregata) per ordinare i risultati in base alla quantità massima di capacità aggregata non utilizzata.
7. Salvare la vista con un nome specifico che rifletta ciò che la vista mostra, ad esempio "Least used aggregate Capacity", quindi fare clic sul segno di spunta (✓).
8. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
9. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report Schedule (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
10. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile bilanciare le coppie ha in base alla capacità aggregata.

Creazione di un report per visualizzare i nodi che eseguono versioni precedenti di ONTAP

È possibile creare un report per visualizzare la versione del software ONTAP installata su tutti i nodi del cluster in modo da visualizzare i nodi da aggiornare.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata che visualizzi i nodi che eseguono versioni precedenti di ONTAP, quindi pianificare la creazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Nodes**.
2. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
3. Trascinare la colonna "versione sistema operativo" vicino alla colonna "nodo".
4. Fare clic nella parte superiore della colonna "versione del sistema operativo" per ordinare i risultati in base alla versione meno recente di ONTAP.
5. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "Nodes by ONTAP version".
6. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
7. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report Schedule (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
8. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere necessario aggiornare i nodi che eseguono versioni precedenti di ONTAP.

Personalizzazione dei report sulla capacità aggregata

Questi report personalizzati di esempio vengono utilizzati per identificare e rispondere a potenziali problemi relativi alla capacità dello storage aggregato.

I report di questa sezione sono solo esempi per aiutarti a comprendere come creare report sulla capacità aggregata per monitorare le risorse del sistema di storage.

Creazione di un report per visualizzare gli aggregati che raggiungono la piena capacità

È possibile creare un report per individuare gli aggregati che stanno raggiungendo la capacità completa in modo da poter aggiungere più capacità o spostare i carichi di lavoro in altri aggregati.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata che visualizzi aggregati che raggiungono la capacità completa, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates**.
2. Nel menu Visualizza, selezionare **capacità** > **tutti gli aggregati**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Fare clic sull'icona del filtro, aggiungere il seguente filtro, quindi fare clic su **Applica filtro**:
   - Giorni per il pieno meno di 45 giorni
5. Fare clic sulla parte superiore della colonna "Days to Full" per ordinare i risultati in base al numero minimo di giorni rimanenti per raggiungere la piena capacità.
6. Salvare la vista con un nome specifico che rifletta ciò che la vista mostra, ad esempio "Days to full aggregate Capacity", quindi fare clic sul segno di spunta (✓).
7. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
8. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina **Report Schedule** (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
9. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere necessario aumentare lo storage su aggregati che raggiungono la capacità completa. Inoltre, potrebbe essere necessario aumentare la soglia dei giorni fino alla capacità massima a oltre i 7 giorni predefiniti, in modo da ricevere eventi che consentono di ridurre il tempo necessario per reagire allo spazio degli aggregati.

Creazione di un report per visualizzare aggregati che sono pieni al 80% o più

È possibile creare un report per evidenziare gli aggregati che sono pieni al 80% o più.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla procedura riportata di seguito per creare una vista personalizzata che visualizzi aggregati con un livello di riempimento pari o superiore al 80%, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates**.
2. Nel menu Visualizza, selezionare **capacità** > **tutti gli aggregati**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Trascina le colonne "dati disponibili %" e "dati utilizzati %" vicino alla colonna "aggregato".
5. Fare clic sull'icona del filtro, aggiungere i seguenti filtri, quindi fare clic su **Applica filtro**:
   - La percentuale dei dati utilizzati è superiore al 80%
6. Fare clic sulla parte superiore della colonna "dati utilizzati %" per ordinare i risultati in base alla percentuale di capacità.
7. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "aggregati quasi pieni", quindi fare clic sul segno di spunta (✓) .
8. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
9. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report Schedule (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
10. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile spostare alcuni dati da determinati aggregati.

Creazione di un report per visualizzare gli aggregati in eccesso

È possibile creare un report per analizzare la capacità dello storage e l'utilizzo degli aggregati e per visualizzare gli aggregati in eccesso.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata che visualizzi aggregati che superano la soglia di overcommit, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates**.

2. Nel menu Visualizza, selezionare **capacità** > **tutti gli aggregati**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Trascina la colonna “capacità di overcommit %” vicino alla colonna “aggregate”.
5. Fare clic sull’icona del filtro, aggiungere i seguenti filtri, quindi fare clic su **Applica filtro**:
   - La percentuale di capacità con overcommit è superiore al 100%
6. Fare clic nella parte superiore della colonna “capacità in eccesso %” per ordinare i risultati in base alla percentuale di capacità.
7. Salvare la vista con un nome specifico che rifletta ciò che la vista mostra, ad esempio “aggregates overcommit”, quindi fare clic sul segno di spunta (✓).
8. Fare clic sul pulsante **Report pianificati** nella pagina dell’inventario.
9. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report Schedule (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
10. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere necessario aggiungere ulteriore capacità agli aggregati o spostare alcuni dati da determinati aggregati.

Personalizzazione dei report sulla capacità dei volumi

Questi report personalizzati di esempio vengono utilizzati per identificare e rispondere a potenziali problemi legati alla capacità e alle performance dei volumi.

Creazione di un report per identificare i volumi in via di capacità totale per i quali è stata disattivata la funzione di eliminazione automatica di Snapshot

È possibile creare un report contenente l’elenco dei volumi che si stanno avvicinando alla capacità massima con la funzione di eliminazione automatica di Snapshot disattivata. I risultati consentono di identificare i volumi in cui si desidera configurare l’eliminazione automatica di Snapshot.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell’applicazione o di amministratore dello storage.

Seguire i passaggi riportati di seguito per creare una vista personalizzata che visualizzi le colonne richieste nell’ordine corretto, quindi pianificare la creazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu View (Visualizza), selezionare **Capacity** > **All Volumes** (capacità* > **tutti i volumi**).
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Trascinare le colonne “Snapshot Autodelete” e “Days to Full” vicino alla colonna “Available Data Capacity”.

5. Fare clic sull'icona del filtro, aggiungere i seguenti due filtri, quindi fare clic su **Apply Filter** (Applica filtro):
   - Da giorni a pieno meno di 30 giorni
   - L'eliminazione automatica di Snapshot è disattivata
6. Fare clic nella parte superiore della colonna **giorni da completare** in modo che i volumi con il minor numero di giorni rimanenti vengano visualizzati nella parte superiore dell'elenco.
7. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "VOL near Capacity".
8. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
9. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile attivare l'eliminazione automatica Snapshot sui volumi o trovare un modo per aumentare lo spazio disponibile.

Creazione di un report per identificare lo spazio utilizzato dai volumi con il thin provisioning disattivato

Quando un volume non viene sottoposto a thin provisioning, occupa l'intera quantità di spazio sul disco, come definito al momento della creazione del volume. L'identificazione dei volumi con thin provisioning disattivato consente di decidere se attivare il thin provisioning su determinati volumi.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Seguire i passaggi riportati di seguito per creare una vista personalizzata che visualizzi le colonne richieste nell'ordine corretto, quindi pianificare la creazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu View (Visualizza), selezionare **Capacity** > **All Volumes** (capacità* > **tutti i volumi**).
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Trascinare le colonne "dati utilizzati %" e "thin provisioning" vicino alla colonna "capacità dati disponibili".
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro, **thin provisioning** è **No**, quindi fare clic su **Apply Filter** (Applica filtro).
6. Fare clic sulla parte superiore della colonna "dati utilizzati %" per ordinare i risultati in modo che i volumi con la percentuale più alta vengano visualizzati nella parte superiore dell'elenco.
7. Salvare la vista con un nome per riflettere ciò che viene visualizzato, ad esempio "VOL no thin provisioning".
8. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
9. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina **Report Schedule** (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.

10. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile attivare il thin provisioning su determinati volumi.

Creazione di un report per identificare i volumi sugli aggregati FabricPool che devono spostare i dati nel Tier cloud

È possibile creare un report contenente l'elenco dei volumi che attualmente risiedono negli aggregati FabricPool, che hanno una raccomandazione cloud di livello e che hanno una grande quantità di dati cold. Questo report può aiutarti a decidere se modificare la policy di tiering per determinati volumi in "auto" o "all" per trasferire più dati cold (inattivi) al livello cloud.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario aver configurato gli aggregati FabricPool e avere volumi su tali aggregati.

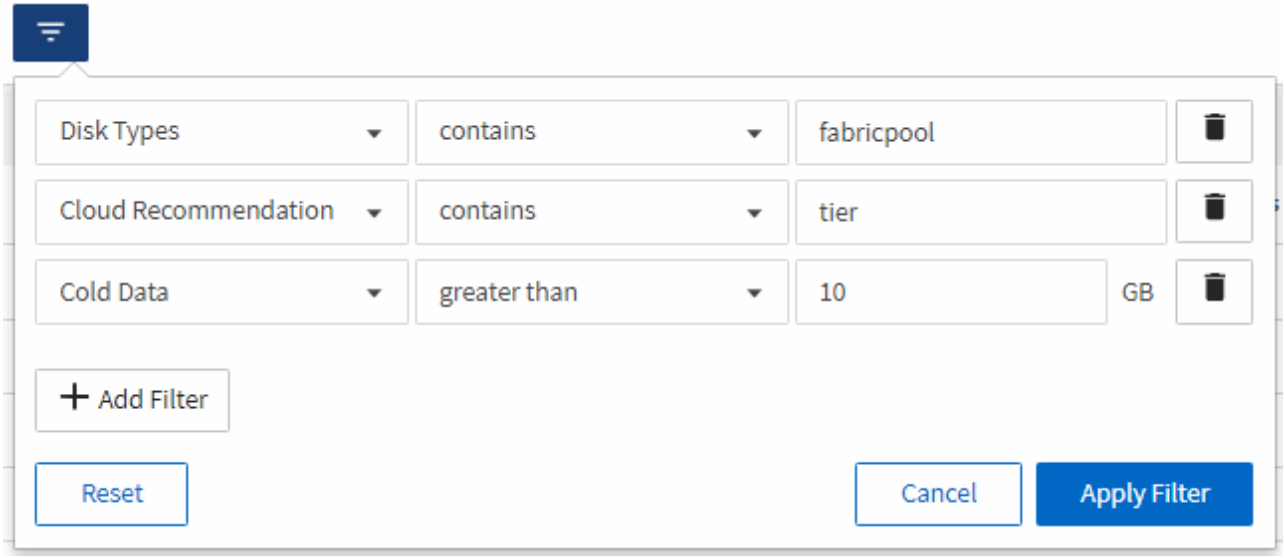
Seguire i passaggi riportati di seguito per creare una vista personalizzata che visualizzi le colonne richieste nell'ordine corretto, quindi pianificare la creazione di un report per tale vista.

Fasi

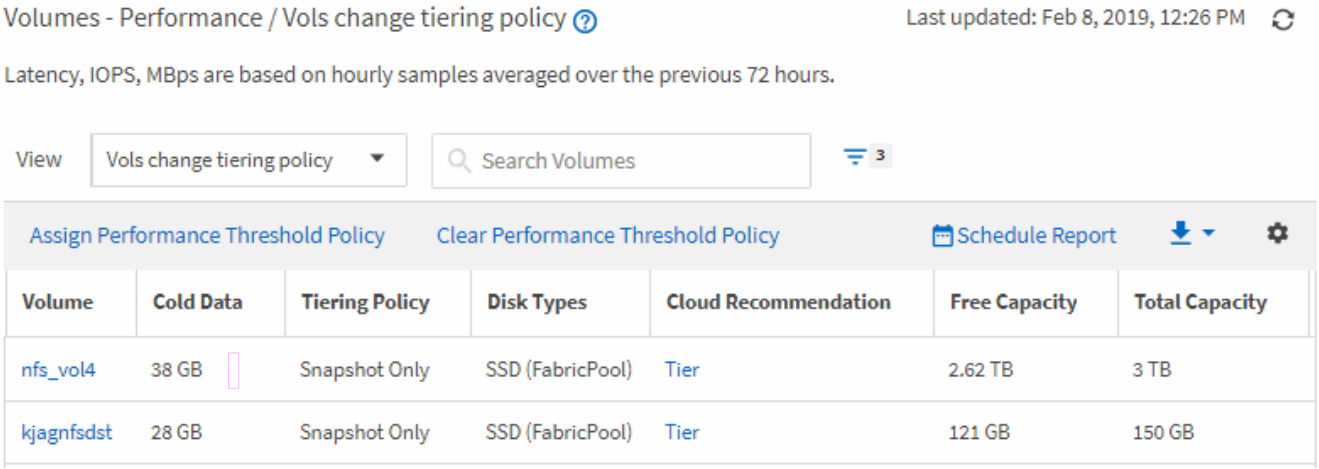
1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu View (Visualizza), selezionare **Performance** (prestazioni) > **All Volumes** (tutti i volumi).
3. Nel selettore di colonna, assicurarsi che la colonna "Disk Type" (tipo di disco) venga visualizzata nella vista.

   Aggiungere o rimuovere altre colonne per creare una vista importante per il report.

4. Trascinare la colonna "Disk Type" (tipo di disco) vicino alla colonna "Cloud Recommendation" (Raccomandazione cloud).
5. Fare clic sull'icona del filtro, aggiungere i tre filtri seguenti, quindi fare clic su **Apply Filter** (Applica filtro):
   - Il tipo di disco contiene FabricPool
   - Cloud Recommendation contiene Tier
   - Cold Data superiore a 10 GB



6. Fare clic sulla parte superiore della colonna Cold Data (dati a freddo) in modo che i volumi con il maggior numero di dati a freddo vengano visualizzati nella parte superiore della vista.
7. Salvare la vista con un nome per riflettere ciò che viene visualizzato, ad esempio “VOL change Tiering policy”.



8. Fare clic sul pulsante **Report pianificati** nella pagina dell’inventario.
9. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report Schedule (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
10. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile utilizzare Gestione sistema o l’interfaccia CLI di ONTAP per modificare la policy di tiering in “auto” o “all” per alcuni volumi per trasferire più dati cold al livello cloud.

Personalizzazione dei report di capacità di Qtree

Questi report personalizzati di esempio vengono utilizzati per identificare e rispondere a potenziali problemi relativi alla capacità di Qtree.

Creazione di un report per visualizzare i qtree quasi pieni

È possibile creare un report per analizzare la capacità dello storage e l'utilizzo dei qtree e visualizzare i qtree quasi pieni.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata che visualizzi qtree quasi pieni, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Storage** > **Qtree**.
2. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
3. Trascina la colonna "Disk used %" vicino alla colonna "Qtree".
4. Fare clic sull'icona del filtro, aggiungere i seguenti filtri, quindi fare clic su **Applica filtro**:
   - La percentuale di dischi utilizzati è superiore al 75%
5. Fare clic sulla parte superiore della colonna "Disk used %" per ordinare i risultati in base alla percentuale di capacità.
6. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "Qtree quasi pieni", quindi fare clic sul segno di spunta (✓).
7. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
8. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina **Report Schedule** (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
9. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere necessario regolare i limiti hard e soft del disco (se impostati) o bilanciare i dati tra i qtree.

Personalizzazione dei report di condivisione NFS

Puoi personalizzare i report di condivisione NFS per analizzare le informazioni sulle policy di esportazione NFS e le regole per i volumi nei tuoi sistemi storage. Ad esempio, è possibile personalizzare i report per visualizzare volumi con percorsi di montaggio e volumi inaccessibili con il criterio di esportazione predefinito.

Creazione di un report per visualizzare i volumi con un percorso di montaggio inaccessibile

È possibile creare un report per trovare i volumi con un percorso di montaggio inaccessibile.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata per i volumi con un percorso di montaggio inaccessibile, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **NFS shares**.
2. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
3. Fare clic sull'icona del filtro, aggiungere il seguente filtro, quindi fare clic su **Applica filtro**:
   - Il percorso di montaggio attivo è No
4. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "Volumes with a inaccessible mount path" (volumi con un percorso di montaggio inaccessibile) e fare clic sul segno di spunta (✓).
5. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
6. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report Schedule (Pianificazioni report) in modo da definire le caratteristiche di pianificazione per il nuovo report.
7. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere necessario correggere i percorsi di montaggio inaccessibili.

Creazione di un report per visualizzare i volumi che utilizzano il criterio di esportazione predefinito

È possibile creare un report per trovare i volumi che utilizzano il criterio di esportazione predefinito.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata per i volumi che utilizzano il criterio di esportazione predefinito, quindi pianificare la creazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **NFS shares**.
2. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
3. Trascinare la colonna "Export Policy" vicino alla colonna "Volume".
4. Fare clic sull'icona del filtro, aggiungere il seguente filtro, quindi fare clic su **Applica filtro**:
   - Il criterio di esportazione contiene i valori predefiniti
5. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "volumi con una policy di esportazione predefinita" e fare clic sul segno di spunta (✓).
6. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
7. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report

Schedule (Pianificazioni report) in modo da definire le caratteristiche di pianificazione per il nuovo report.

8. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati visualizzati nel report, è possibile configurare un criterio di esportazione personalizzato.

Personalizzazione dei report delle macchine virtuali di storage

È possibile creare report sulle macchine virtuali dello storage per analizzare le informazioni sui volumi e visualizzare lo stato generale e la disponibilità dello storage. Ad esempio, è possibile creare report per visualizzare le SVM che raggiungono il numero massimo di volumi e analizzare le SVM interrotte.

Creazione di un report per visualizzare le VM di storage che raggiungono il limite massimo di volume

È possibile creare un report per individuare le SVM che stanno raggiungendo il limite massimo di volume.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata che visualizzi le VM di storage che stanno raggiungendo il limite massimo di volume, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Storage VMS**.
2. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
3. Trascinare le colonne "Volume Count" e "MAXimum Allowed Volumes" vicino alla colonna "Storage VM".
4. Fare clic sulla parte superiore della colonna "MAXimum Allowed Volumes" (volumi massimi consentiti) per ordinare i risultati in base al numero massimo di volumi.
5. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "Smacchine virtuali che raggiungono volumi massimi" e fare clic sul segno di spunta (✓).
6. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
7. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina **Report Schedule** (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
8. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile bilanciare i volumi assegnati alle macchine virtuali storage o, se possibile, utilizzare Gestione di sistema di ONTAP per modificare i volumi massimi consentiti.

Creazione di un report per visualizzare le VM di storage interrotte

È possibile creare un report per visualizzare un elenco di tutte le SVM interrotte.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata che visualizzi le macchine virtuali di storage interrotte, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Storage VMS**.
2. Nel menu View (Visualizza), selezionare **Health** > **All Storage VMS**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Trascinare la colonna "State" vicino alla colonna "Storage VM".
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro, quindi fare clic su **Applica filtro**:
   - Lo stato è interrotto
6. Salvare la vista con un nome specifico che rifletta la vista visualizzata, ad esempio "SSVM in alto" e fare clic sul segno di spunta (✓).
7. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
8. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina **Report Schedule** (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
9. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere necessario esaminare il motivo dell'arresto di SVM per verificare se è necessario riavviare le SVM interrotte.

Personalizzazione dei report delle relazioni dei volumi

Il report Volume Relanes Inventory consente di analizzare i dettagli dell'inventario dello storage in un cluster, comprendere il grado di protezione richiesto per i volumi e filtrare i dettagli del volume in base all'origine del guasto, al modello e alle pianificazioni.

Creazione di un report per raggruppare le relazioni dei volumi in base all'origine dell'errore

È possibile creare un report che raggruppa i volumi in base al motivo per cui la relazione si trova in uno stato non integro.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata che raggruppa i volumi in base

all'origine dell'errore, quindi pianificare la creazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu Visualizza, selezionare **relazione** > **tutte le relazioni**.
3. Selezionare **Mostra/Nascondi** per assicurarsi che le colonne "Relationship Health" e "UnHealthy Reason" siano visualizzate nella vista.

   Aggiungere o rimuovere altre colonne per creare una vista importante per il report.
4. Trascinare le colonne "Relationship Health" e "Unhealthy reason" vicino alla colonna "State".
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro, quindi fare clic su **Applica filtro**:
   - Rapporto salute è male
6. Fare clic sulla parte superiore della colonna "Unhealthy reason" (motivo non integro) per raggruppare le relazioni del volume in base all'origine del guasto.
7. Salvare la vista con un nome specifico che rifletta ciò che la vista mostra, ad esempio "Vol Relaces by failure".
8. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
9. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile analizzare l'origine e l'impatto di ciascun tipo di guasto.

Creazione di un report per raggruppare le relazioni dei volumi in base al problema

È possibile creare un report che raggruppa le relazioni dei volumi in base al problema.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata che raggruppa le relazioni dei volumi in base al problema, quindi pianificare la creazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu Visualizza, selezionare **relazione** > **tutte le relazioni**.
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Trascinare la colonna "unhealthy reason" vicino alla colonna "State".
5. Fare clic sulla parte superiore della colonna "Unhealthy reason" (motivo non integro) per raggruppare i volumi in base al problema.
6. Salvare la vista con un nome specifico che rifletta ciò che la vista mostra, ad esempio "Vol Relaces by Issue".
7. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.

8. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile analizzare l'origine e l'impatto di ciascun tipo di problema.

Creazione di un report per visualizzare i trend di trasferimento dei volumi a intervalli di tempo specifici

È possibile creare un report che visualizzi i trend di trasferimento dei volumi a intervalli di tempo specifici.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata per i volumi a intervalli di tempo specifici, quindi pianificare la creazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu View (Visualizza), selezionare **Relationship** (relazione) > **Last 1 Month Transfer Status** (Stato trasferimento ultimo 1 mese).
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Trascinare la colonna Transfer Duration (durata trasferimento) vicino alla colonna "Operational Result" (risultato operativo).
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro, quindi fare clic su **Applica filtro**:
   - Ora di fine del trasferimento negli ultimi 7 giorni
6. Fare clic nella parte superiore della colonna "Transfer Duration" (durata trasferimento) per ordinare i volumi in base all'intervallo di tempo.
7. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "Volumes by Duration".
8. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
9. Inserire un nome per la pianificazione del report, impostare la frequenza su **settimanale** e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile esaminare gli intervalli di tempo di trasferimento.

Creazione di un report per la visualizzazione di un trasferimento di volume non riuscito o riuscito

È possibile creare un report che visualizzi lo stato dei trasferimenti di volume. In questo report è possibile visualizzare i trasferimenti di volume non riusciti e quelli riusciti.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla procedura riportata di seguito per creare una vista personalizzata che mostri quali trasferimenti non sono riusciti e quali sono stati effettuati correttamente, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu View (Visualizza), selezionare **Relationship** (relazione) > **Last 1 Month Transfer Status** (Stato trasferimento ultimo 1 mese).
3. Selezionare **Mostra/Nascondi** per rimuovere le colonne non desiderate nel report.
4. Trascinare la colonna "risultato dell'operazione" vicino alla colonna "State".
5. Fare clic sulla parte superiore della colonna "risultato operazione" per ordinare i volumi in base allo stato.
6. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "volumi per stato di trasferimento".
7. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
8. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile esaminare lo stato del trasferimento.

Creazione di un report per visualizzare i trasferimenti di volume in base alle dimensioni del trasferimento

È possibile creare un report per visualizzare i trasferimenti di volume in base alle dimensioni del trasferimento.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata per i trasferimenti di volume in base alle dimensioni di trasferimento, quindi pianificare la creazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu View (Visualizza), selezionare **Relationship** (relazione) > **Last 1 Month Transfer Rate** (tasso di trasferimento ultimo 1 mese).
3. Fare clic sulla parte superiore della colonna "Total Transfer Size" per ordinare i trasferimenti di volume in base alle dimensioni.
4. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "Volumes by transfer size" (volumi per dimensione trasferimento).
5. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
6. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile analizzare le relazioni dei volumi in base alle dimensioni del trasferimento.

Creazione di un report per visualizzare i trasferimenti di volume raggruppati per giorno

È possibile creare un report per visualizzare i trasferimenti di volume raggruppati per giorno.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata per i trasferimenti di volume raggruppati per giorno, quindi pianificare la creazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu View (Visualizza), selezionare **Relationship** (relazione) > **Last 1 Month Transfer Rate** (tasso di trasferimento ultimo 1 mese).
3. Fare clic sulla parte superiore della colonna "DAy" per ordinare i trasferimenti di volume per giorno.
4. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "Volume Transfer by day".
5. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
6. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile analizzare i trasferimenti di volume di giorno in giorno.

Personalizzazione dei report sulle performance dei volumi

Questi report personalizzati di esempio vengono utilizzati per identificare e rispondere a potenziali problemi relativi alle performance dei volumi.

Creazione di un report per visualizzare volumi con un'elevata quantità di dati cold su un aggregato non abilitato a FabricPool

È possibile creare un report per visualizzare volumi con un'elevata quantità di dati cold su un aggregato non FabricPool. In questo modo è possibile identificare i volumi che devono essere spostati in un aggregato FabricPool.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Attenersi alla seguente procedura per creare una vista personalizzata per i volumi con un'elevata quantità di dati cold su un aggregato non abilitato a FabricPool, quindi pianificare la generazione di un report per tale vista.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Nel menu View (Visualizza), selezionare **Performance** (prestazioni) > **All Volumes** (tutti i volumi).
3. Selezionare **Mostra/Nascondi** per assicurarsi che nella vista venga visualizzata la colonna "Dtipo di disco".

   Aggiungere o rimuovere altre colonne per creare una vista importante per il report.
4. Trascinare la colonna "Disk Type" vicino alla colonna "Cold Data".
5. Fare clic sull'icona del filtro, aggiungere il seguente filtro, quindi fare clic su **Applica filtro**:
   - Cold Data superiore a 100 GB
   - Il tipo di disco contiene SSD
6. Fare clic sulla parte superiore della colonna "Dtipo di disco" per ordinare i volumi in base al tipo di disco, in modo che il tipo di disco SSD (FabricPool) si trovi nella parte inferiore.
7. Salvare la vista con un nome specifico che rifletta ciò che viene visualizzato, ad esempio "Cold data vols Not FabricPool" (volumi dati a freddo non).
8. Fare clic sul pulsante **Report pianificati** nella pagina dell'inventario.
9. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

   Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile trovare volumi che sono buoni candidati per essere spostati negli aggregati FabricPool.

Report Microsoft Excel di esempio

Questi report di esempio di Microsoft Excel hanno lo scopo di introdurre le opzioni di reporting disponibili utilizzando le funzionalità avanzate di Excel.

Le funzionalità avanzate di Excel consentono di creare un'ampia gamma di report specifici per le tue esigenze. Per informazioni complete sull'utilizzo di Excel, consultare la documentazione del prodotto.

> Per gestire i report, è necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Creazione di un report per visualizzare una tabella e un grafico della capacità aggregata

È possibile creare un report per analizzare la capacità in un file Excel utilizzando i totali sommati e il formato del grafico a colonne in cluster.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Per aprire una vista Health: All aggregates (Salute: Tutti gli aggregati), scaricare la vista in Excel, creare un grafico della capacità disponibile, caricare il file Excel personalizzato e pianificare il report finale.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates**.
2. Selezionare **Report** > **Download Excel**.

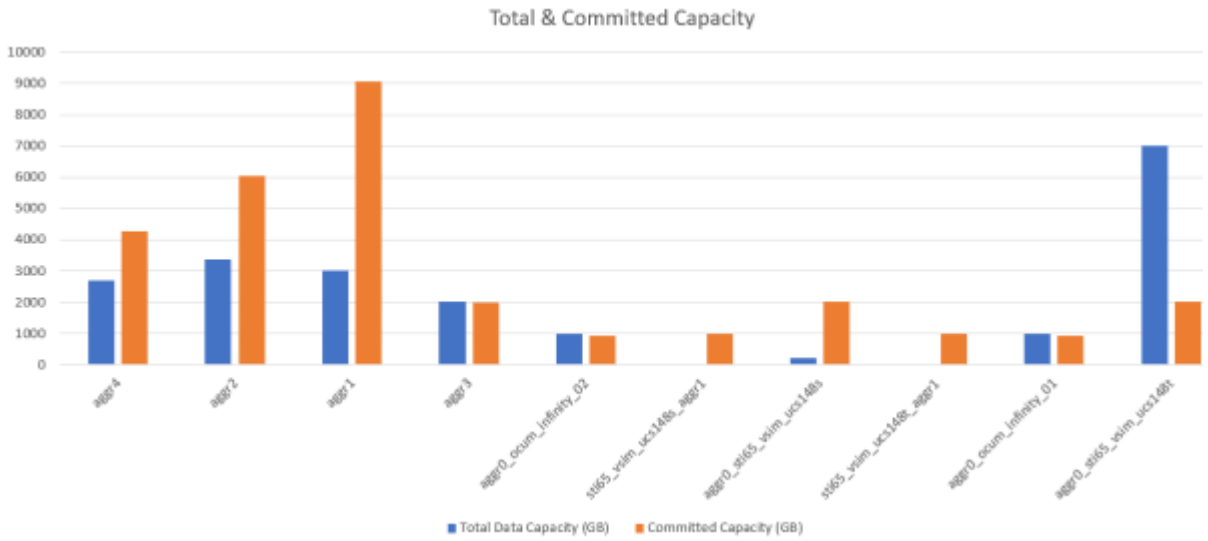
   A seconda del browser in uso, potrebbe essere necessario fare clic su **OK** per salvare il file.

3. Se necessario, fare clic su **Enable editing** (attiva modifica).
4. In Excel, aprire il file scaricato.
5. Creare un nuovo foglio (⊕) dopo `data` Foglio e nome **capacità totale dei dati**.
6. Aggiungere le seguenti colonne nella nuova scheda capacità dati totale:
   a. Capacità totale dei dati (GB)
   b. Capacità impegnata (GB)
   c. Capacità dei dati utilizzati (GB)
   d. Capacità dati disponibile (GB)
7. Nella prima riga di ciascuna colonna, immettere la formula seguente, assicurandosi che faccia riferimento alla scheda dati (dati!) e faccia riferimento agli specificatori di colonna e riga corretti per i dati acquisiti (capacità dati totale estrae i dati dalla colonna e, righe da 2 a 20).
   a. =SOMMA(dati!2:dati!20 USD)
   b. =SOMMA(dati!€2:dati!€50)
   c. =SOMMA(data!GUSD 2:dati!GUSD 50)
   d. =SOMMA(dati!2:dati!50 dollari USA)

   La formula totalizza ogni colonna in base ai dati correnti.

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. Nella scheda informativa, selezionare le colonne **capacità totale dei dati (GB)** e **capacità impegnata (GB)**.
2. Selezionare **Recommended Charts** (grafici consigliati) dal menu **Insert** (Inserisci) e selezionare il grafico **Clustered Column** (colonna in cluster).
3. Fare clic con il pulsante destro del mouse sul grafico e selezionare **Sposta grafico** per spostarlo in `Total Data Capacity` foglio.
4. Utilizzando i menu **Design** e **Format**, disponibili quando viene selezionato il grafico, è possibile personalizzare l'aspetto del grafico.
5. Quando è soddisfatto, salvare il file con le modifiche. Non modificare il nome o la posizione del file.

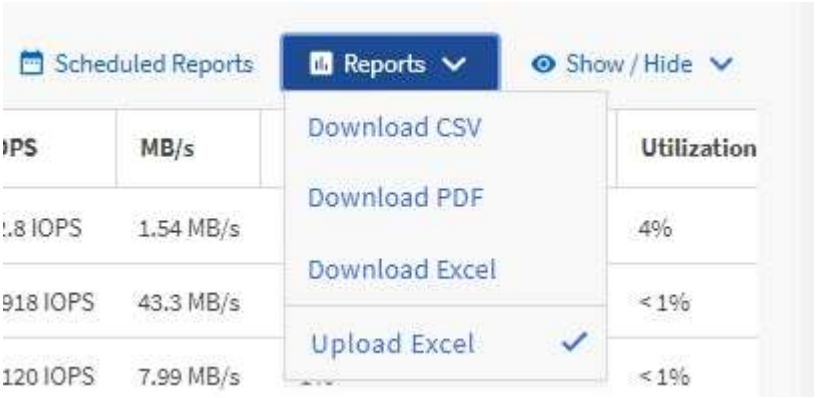


6. In Unified Manager, selezionare **Report** > **carica Excel**.

   Assicurarsi di essere nella stessa vista in cui è stato scaricato il file Excel.

7. Selezionare il file Excel modificato.
8. Fare clic su **Apri**.
9. Fare clic su **Invia**.

   Viene visualizzato un segno di spunta accanto alla voce di menu **Report** > **carica Excel**.



10. Fare clic su **Report pianificati**.

11. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report Schedule (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.

    Selezionare il formato **XLSX** per il report.

12. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere necessario analizzare come utilizzare al meglio la capacità disponibile nella rete.

Creazione di un report per visualizzare i grafici di capacità totale aggregato rispetto a quelli disponibili

È possibile creare un report per analizzare la capacità totale e impegnata dello storage in un formato grafico Excel.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Per aprire una vista Health: All aggregates (Salute: Tutti gli aggregati), scaricare la vista in Excel, creare un grafico della capacità totale e impegnata, caricare il file Excel personalizzato e pianificare il report finale.

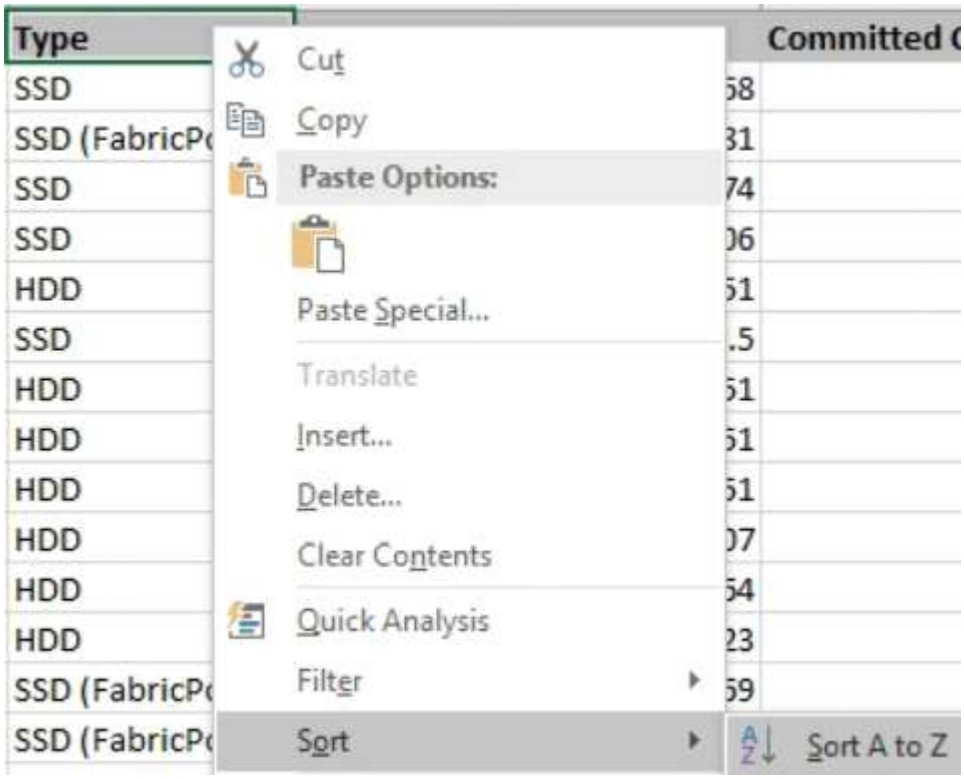
Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates**.
2. Selezionare **Report** > **Download Excel**.

   A seconda del browser in uso, potrebbe essere necessario fare clic su **OK** per salvare il file.

3. In Excel, aprire il file scaricato.
4. Se necessario, fare clic su **Enable editing** (attiva modifica).
5. Nella scheda tecnica, fare clic con il pulsante destro del mouse sulla colonna Type (tipo) e selezionare

Sort (Ordina) > **Sort A to Z** (Ordina Da A a Z).

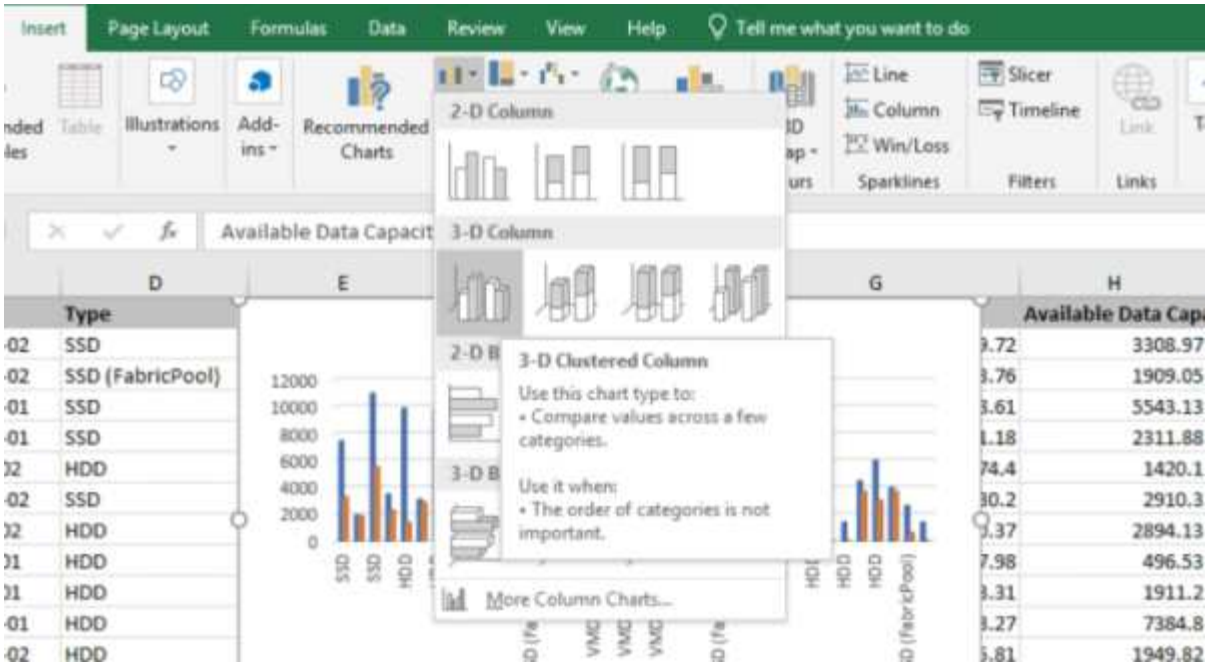


In questo modo i dati verranno sistemati in base al tipo di storage, ad esempio:

- DISCO RIGIDO
- Ibrido
- SSD
- SSD (FabricPool)

6. Selezionare `Type, Total Data Capacity,` e. `Available Data Capacity` colonne.
7. Nel menu **Inserisci**, selezionare A. `3-D column` grafico.

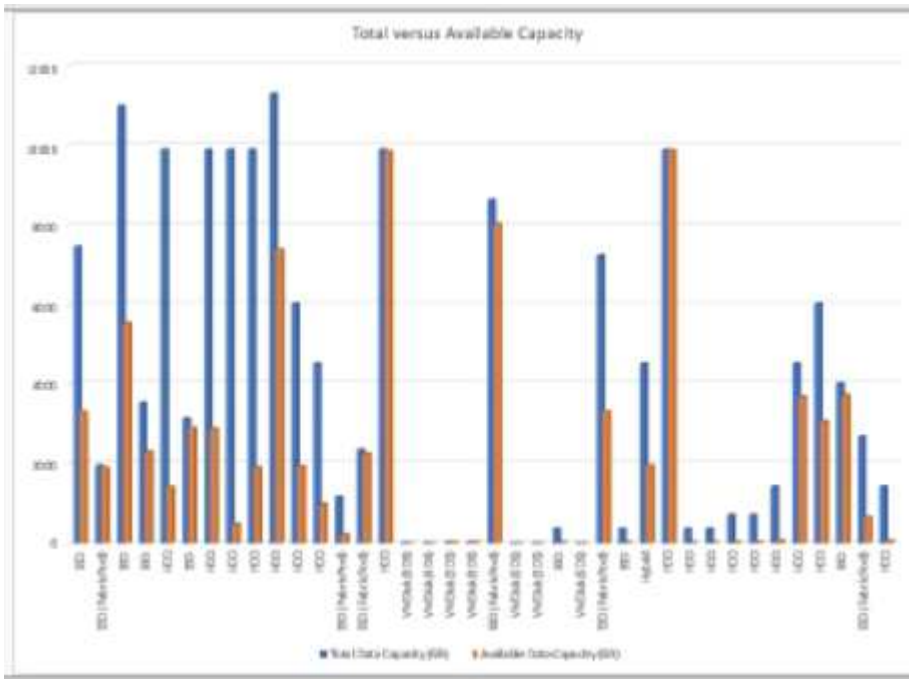
   Il grafico viene visualizzato sulla scheda tecnica.



8. Fare clic con il pulsante destro del mouse sul grafico e selezionare **Sposta grafico**.
9. Selezionare **New sheet** (nuovo foglio) e assegnare un nome al foglio **Total Storage Chart** (grafici di storage totali).

> Assicurarsi che il nuovo foglio venga visualizzato dopo le schede informative e dati.

10. Indicare il titolo del grafico **capacità totale e capacità disponibile**.
11. Utilizzando i menu **Design** e **Format**, disponibili quando si seleziona il grafico, è possibile personalizzare l'aspetto del grafico.
12. Quando è soddisfatto, salvare il file con le modifiche. Non modificare il nome o la posizione del file.

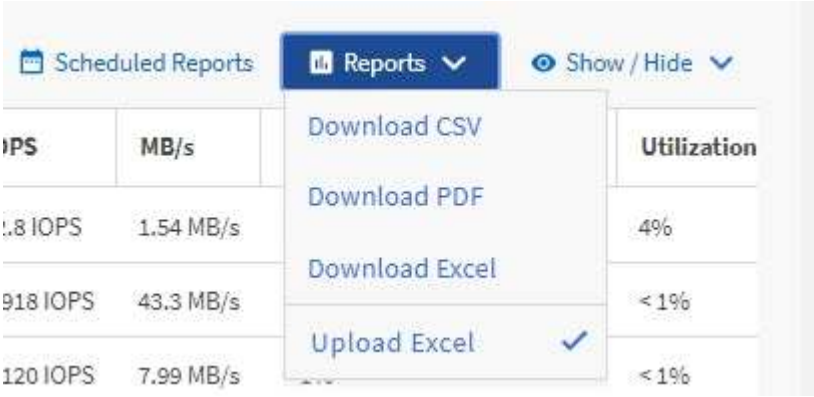


13. In Unified Manager, selezionare **Report** > **carica Excel**.

Assicurarsi di essere nella stessa vista in cui è stato scaricato il file Excel.

14. Selezionare il file Excel modificato.
15. Fare clic su **Apri**.
16. Fare clic su **Invia**.

    Viene visualizzato un segno di spunta accanto alla voce di menu **Report** > **carica Excel**.



17. Fare clic su **Report pianificati**.
18. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina **Report Schedule** (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.

    Selezionare il formato **XLSX** per il report.

19. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile bilanciare il carico sugli aggregati.

Creazione di un report per visualizzare i grafici della capacità dei volumi disponibili

È possibile creare un report per analizzare la capacità di volume disponibile in un grafico Excel.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Per aprire la vista Health: All Volumes (Salute: Tutti i volumi), scaricare la vista in Excel, creare un grafico della capacità disponibile, caricare il file Excel personalizzato e pianificare il report finale.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Volumes**.
2. Selezionare **Report** > **Download Excel**.

A seconda del browser in uso, potrebbe essere necessario fare clic su **OK** per salvare il file.

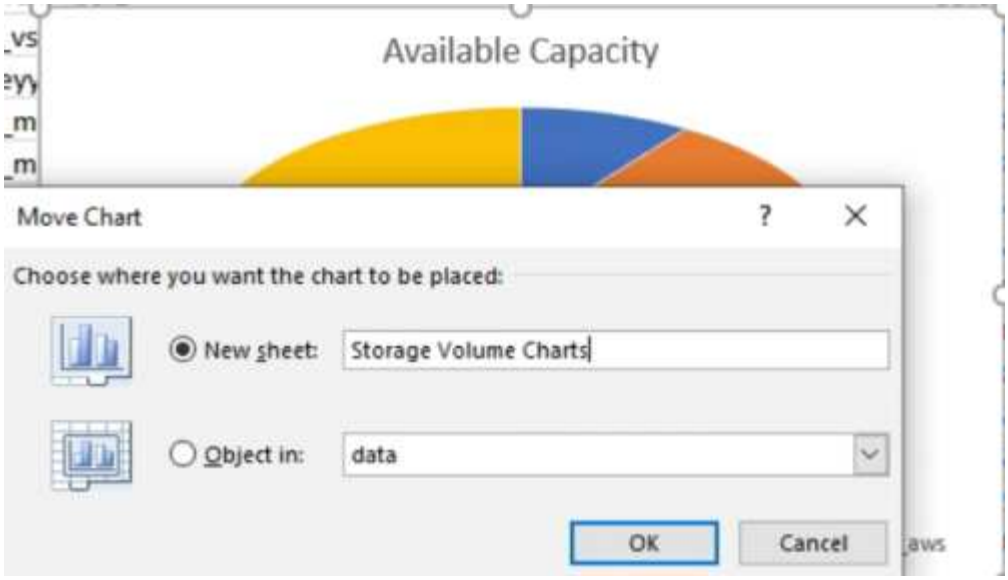
3. Se necessario, fare clic su **Enable editing** (attiva modifica).
4. In Excel, aprire il file scaricato.
5. Su `data` selezionare i dati che si desidera utilizzare in `Volume` e. `Available Data` colonne %.
6. Nel menu **Inserisci**, selezionare A. `3-D piechart.`

   Il grafico mostra quali volumi hanno lo spazio disponibile più grande. Il grafico viene visualizzato sulla scheda tecnica.

   A seconda della configurazione di rete, la selezione di intere colonne o di troppe righe di dati potrebbe rendere il grafico a torta illeggibile. Questo esempio utilizza il grafico a torta 3D, ma è possibile utilizzare qualsiasi tipo di grafico. Utilizza il grafico che mostra al meglio i dati che desideri acquisire.

7. Assegnare un nome al grafico **capacità disponibile**.
8. Fare clic con il pulsante destro del mouse sul grafico e selezionare **Sposta grafico**.
9. Selezionare **nuovo foglio** e assegnare un nome al foglio **Storage Volume Chart**.

   Assicurarsi che il nuovo foglio venga visualizzato dopo le schede informative e dati.

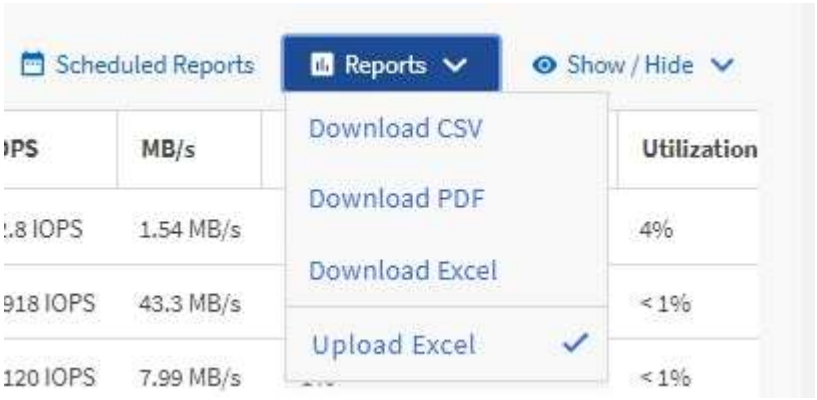


10. Utilizzando i menu **Design** e **Format**, disponibili quando si seleziona il grafico, è possibile personalizzare l'aspetto del grafico.
11. Quando è soddisfatto, salvare il file con le modifiche.
12. In Unified Manager, selezionare **Report** > **carica Excel**.

    Assicurarsi di essere nella stessa vista in cui è stato scaricato il file Excel.

13. Selezionare il file Excel modificato.
14. Fare clic su **Apri**.
15. Fare clic su **Invia**.

    Viene visualizzato un segno di spunta accanto alla voce di menu **Report** > **carica Excel**.



16. Fare clic su **Report pianificati**.
17. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina **Report Schedule** (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
18. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Selezionare il formato **XLSX** per il report.

Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, potrebbe essere necessario bilanciare il carico sui volumi.

Creazione di un report per visualizzare gli aggregati con IOPS più disponibili

Questo report mostra quali aggregati dispongono degli IOPS più disponibili per tipo di aggregato su cui è possibile eseguire il provisioning di nuovi workload.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Per aprire la vista Health: All Volumes (Salute: Tutti i volumi), scaricare la vista in Excel, creare un grafico della capacità disponibile, caricare il file Excel personalizzato e pianificare il report finale.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage** > **Aggregates**.
2. Selezionare **Performance: All aggregates** (prestazioni: Tutti gli aggregati) dal menu a discesa **View** (Visualizza).
3. Selezionare **Mostra/Nascondi** per visualizzare `Available IOPS` e nascondere `Cluster FQDN`, `Inactive Data Reporting`, e. `Threshold Policy` colonne.
4. Trascinare il `Available IOPS` e. `Free Capacity` colonne accanto a. `Type` colonna.
5. Assegnare un nome e salvare la vista personalizzata `Available IOPS Per Aggr.`
6. Selezionare **Report** > **Download Excel**.

   A seconda del browser in uso, potrebbe essere necessario fare clic su **OK** per salvare il file.

7. Se necessario, fare clic su **Enable editing** (attiva modifica).
8. In Excel, aprire il file scaricato.
9. Sulla scheda tecnica, fare clic sul piccolo triangolo in alto a sinistra del foglio per selezionare l'intero foglio.
10. Sulla barra multifunzione **Data**, selezionare **Sort** dal `Sort & Filter area.`
11. Impostare i seguenti livelli di ordinamento:

a. Specificare **Ordina per** come `Available IOPS` (IOPS), il comando **Sort on** As `Cell Values`, E l'ordine * come `Largest to Smallest`.

b. Fare clic su **Aggiungi livello**.

c. Specificare **Ordina per** come `Type`, Il campo **Sort on** As `Cell Values`, E l'ordine * come `Z to A`.

d. Fare clic su **Aggiungi livello**.

e. Specificare **Ordina per** come `Free Capacity (GB)`, Il campo **Ordina** come `Cell Values`, E l'ordine * come `Largest to Smallest`.

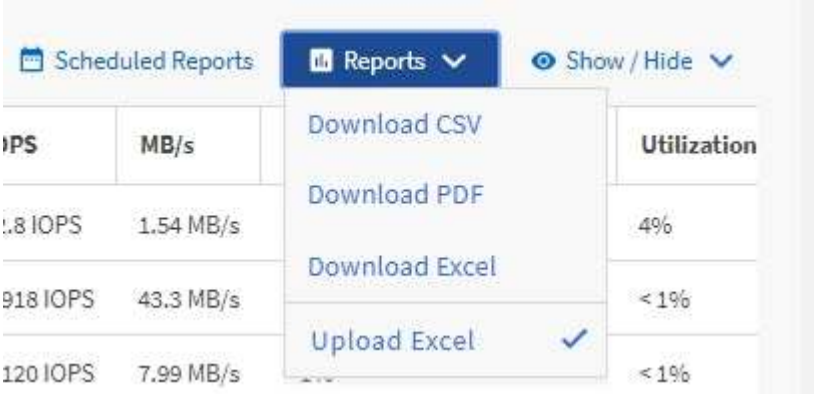
f. Fare clic su **OK**.

12. Salvare e chiudere il file Excel.
13. In Unified Manager, selezionare **Report** > **carica Excel**.

    Assicurarsi di essere nella stessa vista in cui è stato scaricato il file Excel.

14. In questo caso, selezionare il file Excel modificato `performance-aggregates-<date>.xlsx`.
15. Fare clic su **Apri**.
16. Fare clic su **Invia**.

    Viene visualizzato un segno di spunta accanto alla voce di menu **Report** > **carica Excel**.



17. Fare clic su **Report pianificati**.
18. Fare clic su **Add Schedule** (Aggiungi pianificazione) per aggiungere una nuova riga alla pagina Report Schedule (Pianificazioni report) in modo da poter definire le caratteristiche di pianificazione per il nuovo report.
19. Immettere un nome per la pianificazione del report e completare gli altri campi del report, quindi fare clic sul segno di spunta (✓) alla fine della riga.

    Selezionare il formato **XLSX** per il report.

    Il report viene inviato immediatamente come test. Successivamente, il report viene generato e inviato via email ai destinatari elencati utilizzando la frequenza specificata.

In base ai risultati mostrati nel report, è possibile eseguire il provisioning di nuovi workload sugli aggregati che hanno il massimo IOPS disponibile.

Gestire lo storage utilizzando API REST

Introduzione alle API REST di Active IQ Unified Manager

Active IQ Unified Manager offre un set di API per gestire le risorse di storage sui sistemi di storage supportati attraverso un'interfaccia di servizio Web RESTful per qualsiasi integrazione di terze parti.

In questi argomenti, troverai informazioni sulle API di Unified Manager, flussi di lavoro di esempio per risolvere problemi specifici e alcuni codici di esempio. Utilizzando queste informazioni, è possibile creare client RESTful delle soluzioni software di gestione NetApp per la gestione dei sistemi NetApp. Le API sono basate sullo stile architettonico REST (Representational state Transfer). Sono supportate tutte e quattro le operazioni REST Create, Read, Update ed Delete (note anche come CRUD).

Destinatari di questo contenuto

Gli argomenti riportati di seguito sono destinati agli sviluppatori che creano applicazioni che si interfacciano con il software Active IQ Unified Manager tramite API REST.

Gli amministratori e gli architetti dello storage possono fare riferimento a queste informazioni per ottenere una comprensione di base di come le API REST di Unified Manager possono essere utilizzate per creare applicazioni client per gestire e monitorare i sistemi storage NetApp.

Utilizzare queste informazioni se si desidera utilizzare il provider di storage, il cluster ONTAP e le API di amministrazione della gestione per la gestione dello storage.

È necessario disporre di uno dei seguenti ruoli: Operatore, Amministratore dello storage o Amministratore dell'applicazione. È necessario conoscere l'indirizzo IP o il nome di dominio completo del server Unified Manager su cui si desidera eseguire le API REST.

Accesso e categorie API Active IQ Unified Manager

Le API di Active IQ Unified Manager consentono di gestire ed eseguire il provisioning degli oggetti di storage nel proprio ambiente. È inoltre possibile accedere all'interfaccia utente Web di Unified Manager per eseguire alcune di queste funzioni.

Creazione di un URL per accedere direttamente alle API REST

È possibile accedere alle API REST direttamente tramite un linguaggio di programmazione, ad esempio Python, n. C, C++, JavaScript, e così via. Immettere il nome host o l'indirizzo IP e l'URL per accedere alle API REST nel formato

https://<hostname>/api

La porta predefinita è 443. È possibile configurare la porta in base alle esigenze del proprio ambiente.

Accesso alla pagina della documentazione API online

È possibile accedere alla pagina del contenuto di riferimento di *documentazione API* fornita insieme al prodotto per visualizzare la documentazione API e per eseguire manualmente una chiamata API (sull'interfaccia, ad esempio, Swagger). Per accedere a questa documentazione, fare clic su **barra dei menu** > **pulsante Guida** > **documentazione API**

In alternativa, inserire il nome host o l'indirizzo IP e l'URL per accedere alla pagina API REST nel formato

https://<hostname>/docs/api/

Categorie

Le chiamate API sono organizzate in base alle aree o alle categorie. Per individuare un'API specifica, fare clic sulla categoria API applicabile.

Le API REST fornite con Unified Manager consentono di eseguire funzioni amministrative, di monitoraggio e di provisioning. Le API sono raggruppate nelle seguenti categorie.

- **datacenter**

  Questa categoria contiene le API che ti aiutano nella gestione dello storage del data center e nell'analisi utilizzando strumenti come Work Flow Automation e Ansible. Le API REST di questa categoria forniscono informazioni su cluster, nodi, aggregati, volumi, LUN, condivisioni di file, spazi dei nomi e altri elementi del data center.

- **server di gestione**

  Le API nella categoria **server di gestione** contengono `jobs`, `system`, e. `events` API. I job sono operazioni pianificate per l'esecuzione asincrona relativa alla gestione di oggetti di storage o carichi di lavoro su Unified Manager. Il `events` API restituisce gli eventi nel data center e in `system` API restituisce i dettagli dell'istanza di Unified Manager.

- **provider di storage**

  Questa categoria contiene tutte le API di provisioning necessarie per la gestione e il provisioning di condivisioni di file, LUN, livelli di servizio delle performance e policy di efficienza dello storage. Le API consentono inoltre di configurare endpoint di accesso, Active Directory e assegnare livelli di servizio delle performance e policy di efficienza dello storage sui carichi di lavoro dello storage.

- **amministrazione**

  Questa categoria contiene le API utilizzate per l'esecuzione delle attività amministrative, come la manutenzione delle impostazioni di backup, la visualizzazione dei certificati dell'archivio trust per le origini dati di Unified Manager e la gestione dei cluster ONTAP come origini dati per Unified Manager.

- **gateway**

  Unified Manager consente di richiamare le API REST di ONTAP attraverso le API nella categoria gateway e gestire gli oggetti di storage nel data center.

- **sicurezza**

  Questa categoria contiene API per la gestione degli utenti di Unified Manager.

Servizi REST offerti in Active IQ Unified Manager

Prima di iniziare a utilizzare le API Active IQ Unified Manager, è necessario conoscere i servizi REST e le operazioni offerte.

Le API di provisioning e amministrazione utilizzate per configurare il server API supportano le operazioni di lettura (GET) o scrittura (POST, PATCH, ELIMINAZIONE). Di seguito sono riportati alcuni esempi delle operazioni GET, PATCH, POST ed ELIMINAZIONE supportate dalle API:

- Esempio per GET: `GET /datacenter/cluster/clusters` recupera i dettagli del cluster nel data center. Il numero massimo di record restituiti da `GET` il funzionamento è 1000.

  Le API consentono di filtrare, ordinare e ordinare i record in base agli attributi supportati.

- Esempio di POST: `POST /datacenter/svm/svms` Crea una Storage Virtual Machine (SVM) personalizzata.
- Esempio di PATCH: `PATCH /datacenter/svm/svms/{key}` Modifica le proprietà di una SVM, utilizzando la relativa chiave univoca.
- Esempio di ELIMINAZIONE: `DELETE /storage-provider/access-endpoints/{key}` Elimina un endpoint di accesso da una LUN, SVM o condivisione di file utilizzando la relativa chiave univoca.

Le operazioni RIMANENTI che possono essere eseguite utilizzando le API dipendono dal ruolo dell'utente Operator, Storage Administrator o Application Administrator.

Ruolo dell'utente	Metodo DI RIPOSO supportato
Operatore	Accesso in sola lettura ai dati. Gli utenti con questo ruolo possono eseguire tutte le richieste GET.
Amministratore dello storage	Accesso in lettura a tutti i dati. Gli utenti con questo ruolo possono eseguire tutte le richieste GET. Inoltre, dispongono dell'accesso in scrittura (per eseguire RICHIESTE DI PATCH, POST ed ELIMINAZIONE) per eseguire attività specifiche, come la gestione, gli oggetti del servizio di storage e le opzioni di gestione dello storage.
Amministratore dell'applicazione	Accesso in lettura e scrittura a tutti i dati. Gli utenti con questo ruolo possono eseguire RICHIESTE GET, PATCH, POST ed ELIMINAZIONE per tutte le funzioni.

Per ulteriori informazioni su tutte LE operazioni RIMANENTI, consultare la *documentazione API online*.

Versione API in Active IQ Unified Manager

Gli URI API REST in Active IQ Unified Manager specificano un numero di versione. Ad esempio, `/v2/datacenter/svm/svms`. Il numero di versione `v2` poll `/v2/datacenter/svm/svms` Indica la versione API utilizzata in una release specifica.

Il numero di versione riduce al minimo l'impatto delle modifiche API sul software client inviando una risposta che il client può elaborare.

La parte numerica di questo numero di versione è incrementale rispetto alle release. Gli URI con un numero di versione forniscono un'interfaccia coerente che mantiene la compatibilità con le versioni precedenti nelle release future. Ad esempio, è possibile trovare le stesse API senza una versione `/datacenter/svm/svms`, Che indicano le API di base senza una versione. Le API di base sono sempre la versione più recente delle API.

> Nell'angolo in alto a destra dell'interfaccia Swagger, è possibile selezionare la versione dell'API da utilizzare. Per impostazione predefinita, viene selezionata la versione più alta. Si consiglia di utilizzare la versione più alta di una specifica API (rispetto al numero intero incrementale) disponibile nell'istanza di Unified Manager.

Per tutte le richieste, è necessario richiedere esplicitamente la versione dell'API che si desidera utilizzare. Quando viene specificato il numero di versione, il servizio non restituisce elementi di risposta che l'applicazione non è progettata per gestire. Nelle richieste REST, è necessario includere il parametro version. Le versioni precedenti delle API vengono deprecate dopo alcune release. In questa versione, il `v1` La versione delle API è obsoleta.

Risorse di storage in ONTAP

Le risorse di storage in ONTAP possono essere classificate in generale in *risorse di storage fisiche* e *risorse di storage logico.* per gestire in modo efficace i sistemi ONTAP utilizzando le API fornite in Active IQ Unified Manager, è necessario comprendere il modello di risorse di storage e la relazione tra le varie risorse di storage.

- **Risorse di storage fisico**

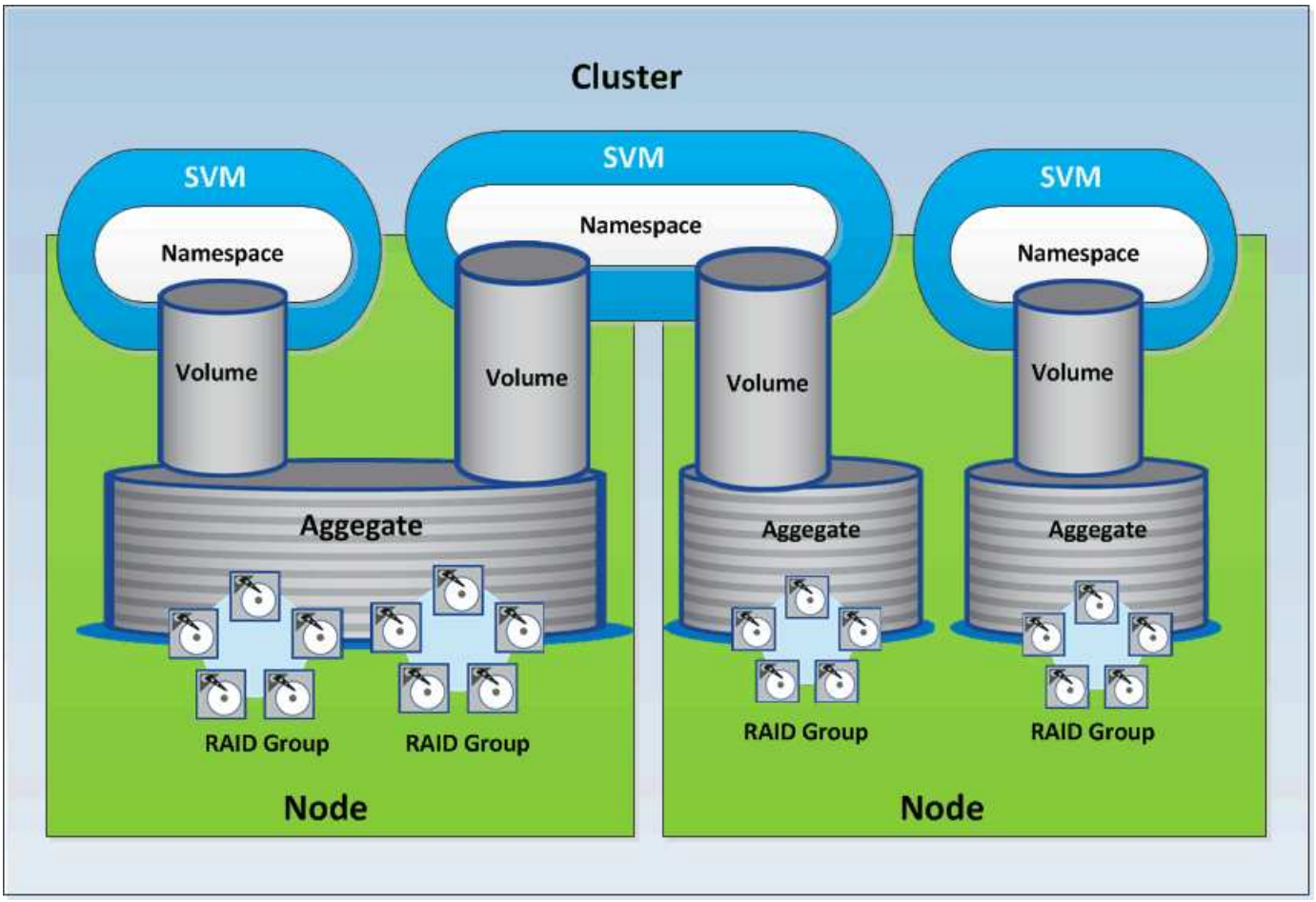
  Si riferisce agli oggetti di storage fisico forniti da ONTAP. Le risorse di storage fisico includono dischi, cluster, storage controller, nodi e aggregati.

- **Risorse di storage logico**

  Si riferisce alle risorse di storage fornite da ONTAP che non sono legate a una risorsa fisica. Queste risorse sono associate a una macchina virtuale per lo storage (SVM, in precedenza nota come Vserver) ed esistono indipendentemente da qualsiasi risorsa fisica di storage specifica, come un disco, un LUN di array o un aggregato.

  Le risorse di storage logico includono volumi di tutti i tipi e qtree, oltre alle funzionalità e alle configurazioni che è possibile utilizzare con queste risorse, come le copie Snapshot, la deduplica, la compressione e le quote.

La seguente illustrazione mostra le risorse di storage in un cluster a 2 nodi:



Autenticazione e accesso API REST in Active IQ Unified Manager

L'API REST di Active IQ Unified Manager è accessibile utilizzando qualsiasi client REST o piattaforma di programmazione in grado di emettere richieste HTTP con un meccanismo di autenticazione HTTP di base.

Una richiesta e una risposta di esempio:

- **Richiesta**

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

- **Risposta**

```
{
  "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* È l'indirizzo IP o il nome di dominio completo (FQDN) del server API.
- Porta 443

  443 è la porta HTTPS predefinita. Se necessario, è possibile personalizzare la porta HTTPS.

Per inviare richieste HTTP da un browser Web, è necessario utilizzare i plug-in del browser REST API. È inoltre possibile accedere all'API REST utilizzando piattaforme di scripting come CURL e Perl.

Autenticazione

Unified Manager supporta lo schema di autenticazione HTTP di base per le API. Per un flusso di informazioni sicuro (richiesta e risposta), le API REST sono accessibili solo tramite HTTPS. Il server API fornisce un certificato SSL autofirmato a tutti i client per la verifica del server. Questo certificato può essere sostituito da un certificato personalizzato (o certificato CA).

È necessario configurare l'accesso dell'utente al server API per richiamare le API REST. Gli utenti possono essere utenti locali (profili utente memorizzati nel database locale) o utenti LDAP (se il server API è stato configurato per l'autenticazione su LDAP). È possibile gestire l'accesso degli utenti accedendo all'interfaccia utente di Unified Manager Administration Console.

Codici di stato HTTP utilizzati in Active IQ Unified Manager

Durante l'esecuzione delle API o la risoluzione dei problemi, è necessario conoscere i vari codici di stato HTTP e i codici di errore utilizzati dalle API Active IQ Unified Manager.

La seguente tabella elenca i codici di errore relativi all'autenticazione:

Codice di stato HTTP	Titolo del codice di stato	Descrizione
200	OK	Restituito in caso di esecuzione riuscita di chiamate API sincrone.
201	Creato	Creazione di nuove risorse mediante chiamate sincrone, ad esempio la configurazione di Active Directory.
202	Accettato	Restituito in caso di esecuzione corretta di chiamate asincrone per funzioni di provisioning, come la creazione di LUN e condivisioni di file.
400	Richiesta non valida	Indica un errore di convalida dell'input. L'utente deve correggere gli input, ad esempio chiavi valide in un corpo di richiesta.
401	Richiesta non autorizzata	Non sei autorizzato a visualizzare la risorsa/non autorizzato.
403	Richiesta non consentita	L'accesso alla risorsa che si stava tentando di raggiungere è vietato.
404	Risorsa non trovata	La risorsa che stavi cercando di raggiungere non è stata trovata.
405	Metodo non consentito	Metodo non consentito.
429	Troppe richieste	Viene restituito quando l'utente invia troppe richieste entro un tempo specifico.

Codice di stato HTTP	Titolo del codice di stato	Descrizione
500	Errore interno del server	Errore interno del server. Impossibile ottenere la risposta dal server. Questo errore interno del server potrebbe essere permanente o meno. Ad esempio, se si esegue un `GET` oppure `GET ALL` operazione e si riceve questo errore, si consiglia di ripetere questa operazione per almeno cinque tentativi. Se si tratta di un errore permanente, il codice di stato restituito continua a essere 500. Se l'operazione ha esito positivo, il codice di stato restituito è 200.

Raccomandazioni per l'utilizzo delle API per Active IQ Unified Manager

Quando si utilizzano le API in Active IQ Unified Manager, è necessario seguire alcune procedure consigliate.

- Per un'esecuzione valida, tutti i tipi di contenuto della risposta devono essere nel seguente formato:

```
application/json
```

- Il numero di versione dell'API non è correlato al numero di versione del prodotto. Utilizzare la versione più recente dell'API disponibile per l'istanza di Unified Manager. Per ulteriori informazioni sulle versioni delle API di Unified Manager, vedere la sezione "reversione delle API ST in Active IQ Unified Manager".
- Durante l'aggiornamento dei valori degli array mediante un'API di Unified Manager, è necessario aggiornare l'intera stringa di valori. Non è possibile aggiungere valori a un array. È possibile sostituire solo un array esistente.
- È possibile utilizzare gli operatori di filtro, come pipe (|) e wild card (*) per tutti i parametri di query, ad eccezione dei valori doppi, ad esempio IOPS e performance nelle API delle metriche.
- Evitare di eseguire query sugli oggetti utilizzando una combinazione di wild card (*) e pipe (|) degli operatori di filtro. Potrebbe recuperare un numero di oggetti non corretto.
- Quando si utilizzano i valori per il filtro, assicurarsi che il valore non contenga alcun valore `?` carattere. In questo modo si riducono i rischi di SQL injection.
- Tenere presente che il `GET` (All) la richiesta per qualsiasi API restituisce un massimo di 1000 record. Anche se si esegue la query impostando `max_records` parametro con un valore superiore a 1000, vengono restituiti solo 1000 record.
- Per eseguire le funzioni amministrative, si consiglia di utilizzare l'interfaccia utente di Unified Manager.

Registri per la risoluzione dei problemi

I registri di sistema consentono di analizzare le cause dei guasti e di risolvere i problemi

che possono verificarsi durante l'esecuzione delle API.

Recuperare i registri dalla seguente posizione per la risoluzione dei problemi relativi alle chiamate API.

Percorso del log	Utilizzare
`/var/log/ocie/access_log.log`	Contiene tutti i dettagli delle chiamate API, ad esempio il nome utente dell'utente che richiama l'API, l'ora di inizio, l'ora di esecuzione, lo stato e l'URL. È possibile utilizzare questo file di log per controllare le API utilizzate di frequente o per risolvere i problemi di qualsiasi flusso di lavoro GUI. È inoltre possibile utilizzarlo per scalare l'analisi in base al tempo di esecuzione.
`/var/log/ocum/ocumserver.log`	Contiene tutti i log di esecuzione API. È possibile utilizzare questo file di log per risolvere i problemi e eseguire il debug delle chiamate API.
`/var/log/ocie/server.log`	Contiene tutte le implementazioni del server Wildfly e i log relativi al servizio start/stop. È possibile utilizzare questo file di log per individuare la causa principale di eventuali problemi che si verificano durante l'avvio, l'arresto o la distribuzione del server Wildfly.
`/var/log/ocie/au.log`	Contiene i log relativi all'unità di acquisizione. È possibile utilizzare questo file di log quando si creano, modificano o eliminano oggetti in ONTAP, ma non vengono riflessi per le API REST di Active IQ Unified Manager.

Processi asincroni degli oggetti di lavoro

Active IQ Unified Manager offre `jobs` API che recupera informazioni sui lavori eseguiti durante l'esecuzione di altre API. È necessario conoscere il funzionamento dell'elaborazione asincrona utilizzando l'oggetto Job.

Alcune delle chiamate API, in particolare quelle utilizzate per l'aggiunta o la modifica delle risorse, possono richiedere più tempo per il completamento rispetto ad altre chiamate. Unified Manager elabora queste richieste a esecuzione prolungata in modo asincrono.

Richieste asincrone descritte utilizzando l'oggetto Job

Dopo aver effettuato una chiamata API eseguita in modo asincrono, il codice di risposta HTTP 202 indica che la richiesta è stata convalidata e accettata correttamente, ma non ancora completata. La richiesta viene elaborata come attività in background che continua a essere eseguita dopo la risposta HTTP iniziale al client. La risposta include l'oggetto Job che ancora la richiesta, incluso il relativo identificatore univoco.

Esecuzione di query sull'oggetto Job associato a una richiesta API

L'oggetto Job restituito nella risposta HTTP contiene diverse proprietà. È possibile eseguire una query sulla proprietà state per determinare se la richiesta è stata completata correttamente. Un oggetto Job può trovarsi in uno dei seguenti stati:

- `NORMAL`
- `WARNING`
- `PARTIAL_FAILURES`
- `ERROR`

Esistono due tecniche che è possibile utilizzare quando si esegue il polling di un oggetto Job per rilevare lo stato di un terminale per l'attività, ovvero riuscito o non riuscito:

- Richiesta di polling standard: Lo stato corrente del processo viene restituito immediatamente.
- Richiesta di polling lunga: Quando lo stato del processo passa a. `NORMAL, ERROR,` oppure `PARTIAL_FAILURES.`

Passaggi in una richiesta asincrona

È possibile utilizzare la seguente procedura di alto livello per completare una chiamata API asincrona:

1. Eseguire la chiamata API asincrona.
2. Ricevere una risposta HTTP 202 che indichi la corretta accettazione della richiesta.
3. Estrarre l'identificatore per l'oggetto Job dal corpo della risposta.
4. All'interno di un loop, attendere che l'oggetto Job raggiunga lo stato terminale `NORMAL, ERROR,` oppure `PARTIAL_FAILURES.`
5. Verificare lo stato terminale del lavoro e recuperare il risultato del lavoro.

Ciao API server

Il *Hello API server* è un programma di esempio che dimostra come richiamare un'API REST in Active IQ Unified Manager utilizzando un semplice client REST. Il programma di esempio fornisce informazioni di base sul server API nel formato JSON (il server supporta solo tale funzione) `application/json` formato).

L'URI utilizzato è: `https://<hostname>/api/datacenter/svm/svms`. Questo codice di esempio utilizza i seguenti parametri di input:

- L'indirizzo IP o FQDN del server API
- Opzionale: Numero di porta (impostazione predefinita: 443)
- Nome utente
- Password
- Formato di risposta (`application/json`)

Per richiamare le API REST, è anche possibile utilizzare altri script come Jersey e RESTEasy per scrivere un client REST Java per Active IQ Unified Manager. Tenere presente le seguenti considerazioni relative al codice

di esempio:

- Utilizza una connessione HTTPS a Active IQ Unified Manager per richiamare l'URI REST specificato
- Ignora il certificato fornito da Active IQ Unified Manager
- Ignora la verifica del nome host durante l'handshake
- Utilizzi `javax.net.ssl.HttpsURLConnection` Per una connessione URI
- Utilizza una libreria di terze parti (`org.apache.commons.codec.binary.Base64`) Per la costruzione della stringa codificata Base64 utilizzata nell'autenticazione di base HTTP

Per compilare ed eseguire il codice di esempio, è necessario utilizzare il compilatore Java 1.8 o versione successiva.

```
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;
    }

}
```

API REST di Unified Manager

Le API REST per Active IQ Unified Manager sono elencate in questa sezione, in base alle relative categorie.

È possibile visualizzare la pagina della documentazione online dall'istanza di Unified Manager che include i dettagli di ogni chiamata API REST. Questo documento non ripete i dettagli della documentazione online. Ogni chiamata API elencata o descritta in questo documento include solo le informazioni necessarie per individuare la chiamata nella pagina della documentazione. Dopo aver individuato una chiamata API specifica, è possibile esaminare i dettagli completi della chiamata, inclusi i parametri di input, i formati di output, i codici di stato HTTP e il tipo di elaborazione della richiesta.

Le seguenti informazioni sono incluse per ogni chiamata API all'interno di un flusso di lavoro per facilitare l'individuazione della chiamata nella pagina della documentazione:

- Categoria

  Le chiamate API sono organizzate nella pagina della documentazione in aree o categorie correlate alla funzionalità. Per individuare una chiamata API specifica, scorrere verso il basso fino alla fine della pagina, quindi fare clic sulla categoria API applicabile.

- Verbo HTTP (chiamata)

Il verbo HTTP identifica l'azione eseguita su una risorsa. Ogni chiamata API viene eseguita tramite un singolo verbo HTTP.

- Percorso

  Il percorso determina la risorsa specifica a cui l'azione utilizza come parte dell'esecuzione di una chiamata. La stringa del percorso viene aggiunta all'URL principale per formare l'URL completo che identifica la risorsa.

Gestione degli oggetti storage in un data center mediante API

Le API REST in `datacenter` La categoria consente di gestire gli oggetti storage nel data center, ad esempio cluster, nodi, aggregati, macchine virtuali storage, Volumi, LUN, condivisioni di file e spazi dei nomi. Queste API sono disponibili per eseguire query sulla configurazione degli oggetti, mentre alcune consentono di eseguire operazioni di aggiunta, eliminazione o modifica di tali oggetti.

La maggior parte di queste API è CHIAMATA GET che fornisce l'aggregazione tra cluster con il supporto di filtraggio, ordinamento e impaginazione. Eseguendo queste API, restituiscono i dati dal database. Pertanto, gli oggetti appena creati devono essere rilevati dal ciclo di acquisizione successivo per essere visualizzati nella risposta.

Se si desidera eseguire una query sui dettagli di un oggetto specifico, è necessario immettere l'ID univoco di tale oggetto per visualizzarne i dettagli. Ad esempio, per le metriche e le informazioni di analisi degli oggetti storage, vedere "Visualizzazione delle metriche delle performance".

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-
2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

I comandi, gli esempi, le richieste e le risposte ALLE API SONO disponibili sull'interfaccia API di Swagger. È possibile filtrare e ordinare i risultati in base a parametri specifici, come indicato in Swagger. Queste API consentono di filtrare i risultati per oggetti storage specifici, come cluster, volumi o macchine virtuali di storage.

API per gli oggetti storage nel data center

Verbo HTTP	Percorso	Descrizione

`GET`	`/datacenter/cluster/clusters`
	
	`/datacenter/cluster/clusters/{key}`
		È possibile utilizzare questo metodo per visualizzare i dettagli dei cluster ONTAP nel data center. L'API restituisce informazioni, ad esempio l'indirizzo IPv4 o IPv6 del cluster, informazioni sul nodo, ad esempio lo stato del nodo, la capacità delle performance e la coppia ha (High Availability) e indica se il cluster è All SAN Array.

Verbo HTTP	Percorso	Descrizione
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	Restituisce i dettagli delle licenze installate sui cluster del data center. È possibile filtrare i risultati in base ai criteri richiesti. Vengono restituite informazioni quali la chiave di licenza, la chiave del cluster, la data di scadenza e l'ambito della licenza. È possibile inserire una chiave di licenza per recuperare i dettagli di una licenza specifica.
GET	/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}	È possibile utilizzare questo metodo per visualizzare i dettagli dei nodi nel data center. È possibile visualizzare informazioni sul cluster, sullo stato del nodo, sulla capacità delle performance e sulla coppia ha (High Availability) per il nodo.
GET	/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}	È possibile utilizzare questo metodo per visualizzare i dettagli delle condivisioni CIFS nel data center. Oltre ai dettagli di cluster, SVM e volume, vengono restituite anche informazioni sull'elenco di controllo di accesso (ACL).
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	È possibile utilizzare questo metodo per visualizzare i dettagli dei criteri di esportazione per i servizi NFS supportati. È possibile eseguire query sui criteri di esportazione per una VM di cluster o storage e riutilizzare la chiave dei criteri di esportazione per il provisioning delle condivisioni file NFS. Per ulteriori informazioni sull'assegnazione e il riutilizzo delle policy di esportazione sui carichi di lavoro, consulta "Provisioning CIFS e condivisioni file NFS".

Verbo HTTP	Percorso	Descrizione
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	Puoi utilizzare questo metodo per visualizzare la raccolta di aggregati nel data center o un aggregato specifico per il provisioning o il monitoraggio dei carichi di lavoro su di essi. Vengono restituite informazioni quali dettagli su cluster e nodi, capacità di performance utilizzata, spazio disponibile e utilizzato ed efficienza dello storage.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	È possibile utilizzare questo metodo per visualizzare l'insieme di LUN nell'intero data center. È possibile visualizzare informazioni sul LUN, ad esempio dettagli su cluster e SVM, policy QoS e igroups.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	È possibile utilizzare questo metodo per visualizzare i dettagli di tutte le policy QoS applicabili agli oggetti di storage nel data center. Vengono restituite informazioni quali i dettagli del cluster e della SVM, i dettagli delle policy fisse o adattive e il numero di oggetti applicabili a tale policy.
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	È possibile utilizzare questo metodo per visualizzare i dettagli del qtree nel data center per tutti i volumi FlexVol o FlexGroup. Vengono restituite informazioni quali cluster e dettagli SVM, volume FlexVol e policy di esportazione.

Verbo HTTP	Percorso	Descrizione
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	È possibile utilizzare questo metodo per visualizzare la raccolta di volumi nel data center. Vengono restituite informazioni sui volumi, come SVM e dettagli del cluster, QoS e policy di esportazione, sia che il volume sia di tipo Read-write, data-Protection o load-sharing. Per i volumi FlexVol e FlexClone, è possibile visualizzare le informazioni sui rispettivi aggregati. Per un volume FlexGroup, la query restituisce l'elenco degli aggregati costituenti.

Verbo HTTP	Percorso	Descrizione

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/protocols/san/igroups`
	
	`/datacenter/protocols/san/igroups/{key}`
		È possibile assegnare gruppi iniziatori (igroups) autorizzati ad accedere a specifiche destinazioni LUN. Se esiste già un igroup, è possibile assegnarlo. È inoltre possibile creare igroups e assegnarli ai LUN.
		
		È possibile utilizzare questi metodi per eseguire query, creare, eliminare e modificare igroups rispettivamente.
		
		Punti da notare:
		
		• `POST`: Durante la creazione di un igroup, è possibile designare la VM di storage su cui si desidera assegnare l'accesso.
		• `DELETE`: È necessario fornire la chiave igroup come parametro di input per eliminare un igroup particolare. Se è già stato assegnato un igroup a un LUN, non è possibile eliminare tale igroup.
		• `PATCH`: È necessario fornire la chiave igroup come parametro di input per modificare un igroup particolare. È inoltre necessario immettere la proprietà che si desidera aggiornare, insieme al relativo valore.

Verbo HTTP	Percorso	Descrizione

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/svm/svms`
	
	`/datacenter/svm/svms/{key}`
		È possibile utilizzare questi metodi per visualizzare, creare, eliminare e modificare le macchine virtuali di storage (VM di storage).
		
		• `POST`: Inserire l'oggetto VM di storage che si desidera creare come parametro di input. È possibile creare una VM di storage personalizzata e assegnarvi le proprietà richieste.
		• `DELETE`: Per eliminare una particolare VM di storage, è necessario fornire la chiave della VM di storage.
		• `PATCH`: Per modificare una particolare VM di storage, è necessario fornire la chiave della VM di storage. È inoltre necessario immettere le proprietà da aggiornare, insieme ai relativi valori.

Punti da notare:

Se è stato abilitato il provisioning del carico di lavoro basato su SLO nell'ambiente, durante la creazione della VM di storage, assicurarsi che supporti tutti i protocolli richiesti per il provisioning delle LUN e delle condivisioni di file su di essi, ad esempio CIFS o SMB, NFS, FCP, E iSCSI. I flussi di lavoro di provisioning potrebbero non riuscire se la VM di storage non supporta i servizi richiesti. Si consiglia di abilitare anche i servizi per i rispettivi tipi di carichi di lavoro sulla VM di storage.

Se è stato abilitato il provisioning del carico di lavoro basato su SLO nell'ambiente, non è possibile eliminare la VM di storage su cui sono stati forniti i carichi di lavoro dello storage. Quando si elimina una VM di storage su cui è stato configurato un server CIFS o SMB, questa API elimina anche il server CIFS o SMB, insieme alla configurazione locale di Active Directory. Tuttavia, il nome del server CIFS o SMB continua ad essere nella configurazione di Active Directory che è necessario eliminare manualmente dal server Active Directory.

API per gli elementi di rete nel data center

Le seguenti API nella categoria del data center recuperano informazioni sulle porte e sulle interfacce di rete dell'ambiente, in particolare le porte FC, le interfacce FC, le porte ethernet e le interfacce IP.

Verbo HTTP	Percorso	Descrizione
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	Recupera informazioni su tutte le porte ethernet nell'ambiente del data center. Con una chiave di porta come parametro di input, è possibile visualizzare le informazioni di quella specifica porta. Informazioni, come dettagli del cluster, dominio di trasmissione, dettagli delle porte, come stato, velocità, e digitare, e se la porta è attivata, viene recuperato.
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	È possibile utilizzare questo metodo per visualizzare i dettagli delle interfacce FC nell'ambiente del data center. Con un tasto di interfaccia come parametro di input, è possibile visualizzare le informazioni di quella specifica interfaccia. Vengono recuperate informazioni quali dettagli del cluster, dettagli del nodo principale e dettagli della porta principale.
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	Recupera informazioni su tutte le porte FC utilizzate nei nodi dell'ambiente del data center. Con una chiave di porta come parametro di input, è possibile visualizzare le informazioni di quella specifica porta. Vengono recuperate informazioni quali dettagli del cluster, descrizione della porta, protocollo supportato e stato della porta.
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	È possibile utilizzare questo metodo per visualizzare i dettagli delle interfacce IP nell'ambiente del data center. Con un tasto di interfaccia come parametro di input, è possibile visualizzare le informazioni di quella specifica interfaccia. Vengono recuperate informazioni quali dettagli del cluster, dettagli IPSpace, dettagli del nodo principale, se il failover è attivato.

Accesso alle API ONTAP tramite accesso proxy

Le API del gateway offrono il vantaggio di utilizzare le credenziali Active IQ Unified Manager per eseguire le API REST ONTAP e gestire gli oggetti di storage. Queste API sono disponibili quando la funzione API Gateway è attivata dall'interfaccia utente Web di Unified Manager.

Le API REST di Unified Manager supportano solo un set selezionato di azioni da eseguire sulle origini dati di Unified Manager, ovvero i cluster ONTAP. È possibile utilizzare le altre funzionalità tramite le API di ONTAP. Le API del gateway consentono a Unified Manager di essere un'interfaccia pass-through per il tunneling di tutte le richieste API da eseguire sui cluster ONTAP gestiti, senza accedere a ciascun cluster del data center singolarmente. Funziona come un singolo punto di gestione per l'esecuzione delle API nei cluster ONTAP gestiti dall'istanza di Unified Manager. La funzione gateway API consente a Unified Manager di essere un singolo piano di controllo da cui è possibile gestire più cluster ONTAP, senza effettuare l'accesso singolarmente. Le API del gateway consentono di rimanere connessi a Unified Manager e gestire i cluster ONTAP eseguendo le operazioni delle API REST di ONTAP.

Tutti gli utenti possono eseguire una query utilizzando l'operazione GET. Gli amministratori delle applicazioni possono eseguire tutte le operazioni REST di ONTAP.

Il gateway funge da proxy per il tunneling delle richieste API mantenendo le richieste di intestazione e corpo nello stesso formato delle API ONTAP. È possibile utilizzare le credenziali di Unified Manager ed eseguire le operazioni specifiche per accedere e gestire i cluster ONTAP senza passare le credenziali dei singoli cluster. Continua a gestire l'autenticazione del cluster e la gestione del cluster, ma reindirizza le richieste API in modo che vengano eseguite direttamente sul cluster specifico. La risposta restituita dalle API è la stessa della risposta restituita dalle rispettive API REST ONTAP eseguite direttamente da ONTAP.

Verbo HTTP	Percorso (URL)	Descrizione
`GET`	`/gateways`	Questo metodo GET recupera l'elenco di tutti i cluster gestiti da Unified Manager che supportano le chiamate A RIPOSO ONTAP. È possibile verificare i dettagli del cluster e scegliere di eseguire altri metodi in base all'UUID del cluster o all'UUID (Universal Unique Identifier). Le API del gateway recuperano solo i cluster supportati da ONTAP 9.5 o versione successiva e vengono aggiunte a Unified Manager su HTTPS.

Verbo HTTP	Percorso (URL)	Descrizione

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
 	
`OPTIONS` (Non disponibile su Swagger)
 	
`HEAD` (Non disponibile su Swagger)
	`/gateways/{uuid}/{path}`
	
	Il valore di{uuid} deve essere sostituito con l'UUID del cluster su cui deve essere eseguita l'operazione REST. Inoltre, assicurarsi che l'UUID sia del cluster supportato da ONTAP 9.5 o versione successiva e aggiunto a Unified Manager su HTTPS. Il{path} deve essere sostituito dall'URL REST ONTAP. È necessario rimuovere `/api/` Dall'URL.
		Si tratta di un'API proxy a punto singolo che supporta OPERAZIONI POST, DELETE, PATCH e GET per tutte le API REST di ONTAP. Non sono previste restrizioni per nessuna API, purché supportata da ONTAP. La funzionalità di tunneling o proxy non può essere disattivata.
		
		Il `OPTIONS` Method restituisce tutte le operazioni supportate da un'API REST ONTAP. Ad esempio, se un'API ONTAP supporta solo l' `GET` funzionamento, esecuzione di `OPTIONS` Metodo utilizzando questo gateway API restituisce `GET` come risposta. Questo metodo non è supportato da Swagger, ma può essere eseguito su altri strumenti API.
		
		Il `OPTIONS` method (metodo) determina se una risorsa è disponibile. Questa operazione può essere utilizzata per visualizzare i metadati relativi a una risorsa nelle intestazioni delle risposte HTTP. Questo metodo non è supportato da Swagger, ma può essere eseguito su altri strumenti API.

Informazioni sul tunneling del gateway API

Le API del gateway consentono di gestire gli oggetti ONTAP tramite Unified Manager. Unified Manager gestisce i cluster e i dettagli di autenticazione e reindirizza le richieste all'endpoint REST di ONTAP. L'API del gateway trasforma URL e Hypermedia come collegamenti HATEOAS (Engine of Application state) nell'intestazione e nel corpo di risposta con l'URL di base del gateway API. L'API del gateway funge da URL di base del proxy a cui si aggiunge l'URL REST ONTAP ed esegue l'endpoint REST ONTAP richiesto.

Affinché un'API ONTAP possa essere eseguita correttamente attraverso il gateway API, l'API deve essere supportata dalla versione del cluster ONTAP su cui viene eseguita. L'esecuzione di un'API non supportata sul cluster ONTAP non restituisce alcun risultato.

In questo esempio, l'API del gateway (URL di base del proxy) è: `/gateways/{uuid}/`

L'API ONTAP utilizzata è: `/storage/volumes`. È necessario aggiungere l'URL REST API ONTAP come valore per il parametro path.

Durante l'aggiunta del percorso, assicurarsi di aver rimosso "/" symbol at the beginning of the URL. For the API `/storage/volumes`, aggiungi `storage/volumes`.

L'URL aggiunto è: `/gateways/{uuid}/storage/volumes`

Durante l'esecuzione di `GET` Operazione, l'URL generato è il seguente: `GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes`

Il `/api` Il tag dell'URL REST ONTAP viene rimosso nell'URL allegato e quello dell'API del gateway viene conservato.

Comando CURL campione

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes" -H "accept: application/hal+json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

L'API restituisce l'elenco dei volumi di storage in quel cluster. Il formato di risposta corrisponde a quello ricevuto quando si esegue la stessa API da ONTAP. I codici di stato restituiti sono i codici di stato ONTAP REST.

Impostazione dell'ambito API

Tutte le API hanno un contesto impostato all'interno dell'ambito del cluster. Le API che operano sulla base delle VM di storage hanno anche il cluster come scopo, ovvero le operazioni API vengono eseguite su una particolare VM di storage all'interno di un cluster gestito. Quando si esegue `/gateways/{uuid}/{path}` API, assicurarsi di immettere l'UUID del cluster (UUID origine dati di Unified Manager) per il cluster su cui si esegue l'operazione. Per impostare il contesto su una specifica VM di storage all'interno di quel cluster, inserire la chiave della VM di storage come parametro X-Dot-SVM-UID o il nome della VM di storage come parametro X-Dot-SVM-Name. Il parametro viene aggiunto come filtro nell'intestazione della stringa e l'operazione viene eseguita nell'ambito della VM di storage all'interno del cluster.

Comando CURL campione

```
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>"
```

Per ulteriori informazioni sull'utilizzo delle API REST di ONTAP, vederehttps://docs.netapp.com/us-en/ontap-automation/index.html["Automazione delle API REST di ONTAP"]

Esecuzione di attività amministrative utilizzando le API

È possibile utilizzare le API in `administration` Categoria per modificare le impostazioni di backup, verificare le informazioni del file di backup e i certificati del cluster e gestire i cluster ONTAP come origini dati Active IQ Unified Manager.

Per eseguire queste operazioni, è necessario disporre del ruolo di amministratore dell'applicazione. È inoltre possibile utilizzare l'interfaccia utente Web di Unified Manager per configurare queste impostazioni.

Verbo HTTP	Percorso	Descrizione
GET PATCH	/admin/backup-settings /admin/backup-settings	È possibile utilizzare GET Metodo per visualizzare le impostazioni della pianificazione di backup configurata in Unified Manager per impostazione predefinita. È possibile verificare quanto segue: • Se la pianificazione è attivata o disattivata • Frequenza del backup pianificato (giornaliero o settimanale) • Ora del backup • Numero massimo di file di backup da conservare nell'applicazione L'ora del backup si trova nel fuso orario del server. Le impostazioni di backup del database sono disponibili su Unified Manager per impostazione predefinita e non è possibile creare una pianificazione di backup. Tuttavia, è possibile utilizzare PATCH metodo per modificare le impostazioni predefinite.
GET	/admin/backup-file-info	Ogni volta che viene modificata la pianificazione di backup per Unified Manager, viene generato un file dump di backup. È possibile utilizzare questo metodo per verificare se il file di backup viene generato in base alle impostazioni di backup modificate e se le informazioni sul file corrispondono alle impostazioni modificate.
GET	/admin/datasource-certificate	È possibile utilizzare questo metodo per visualizzare il certificato dell'origine dati (cluster) dall'archivio trust. La convalida del certificato è necessaria prima di aggiungere un cluster ONTAP come origine dati di Unified Manager.

Verbo HTTP	Percorso	Descrizione

`GET`
 	
`POST`
 	
`PATCH`
 	
`DELETE`
	`/admin/datasources/clusters`
	
	`/admin/datasources/clusters/{key}`
		È possibile utilizzare `GET` Metodo per recuperare i dettagli delle origini dati (cluster ONTAP) gestite da Unified Manager.
		
		È inoltre possibile aggiungere un nuovo cluster a Unified Manager come origine dati. Per aggiungere un cluster, è necessario conoscerne il nome host, il nome utente e la password.
		
		Per modificare ed eliminare un cluster gestito come origine dati da Unified Manager, utilizzare la chiave cluster ONTAP.

Gestione degli utenti mediante API

È possibile utilizzare le API in `security` Categoria per controllare l'accesso degli utenti agli oggetti cluster selezionati in Active IQ Unified Manager. È possibile aggiungere utenti locali o utenti di database. È inoltre possibile aggiungere utenti o gruppi remoti appartenenti a un server di autenticazione. In base ai privilegi dei ruoli assegnati agli utenti, possono gestire gli oggetti storage o visualizzare i dati in Unified Manager.

Per eseguire queste operazioni, è necessario disporre del ruolo di amministratore dell'applicazione. È inoltre possibile utilizzare l'interfaccia utente Web di Unified Manager per configurare queste impostazioni.

Le API in `security` category utilizza il parametro users, ovvero il nome utente, e non il parametro key come identificatore univoco per l'entità utente.

Verbo HTTP	Percorso	Descrizione

`GET`
 	
`POST`
	`/security/users`
	
	`/security/users`
		È possibile utilizzare questi metodi per ottenere i dettagli degli utenti o aggiungere un nuovo utente a Unified Manager.
		
		È possibile aggiungere ruoli specifici agli utenti in base al tipo di utente. Durante l'aggiunta di utenti, è necessario fornire password per l'utente locale, l'utente di manutenzione e l'utente del database.

Verbo HTTP	Percorso	Descrizione

`GET`
 	
`PATCH`
 	
`DELETE`
	`/security/users/{name}`	Il metodo GET consente di recuperare tutti i dettagli di un utente, ad esempio nome, indirizzo e-mail, ruolo e tipo di autorizzazione. Il metodo PATCH consente di aggiornare i dettagli. Il metodo DI ELIMINAZIONE consente di rimuovere l'utente.

Visualizzazione delle metriche delle performance tramite le API

Active IQ Unified Manager fornisce un set di API in `/datacenter` categoria che consente di visualizzare i dati sulle performance dei cluster e degli oggetti storage in un data center. Queste API recuperano i dati delle performance dei diversi oggetti storage come cluster, nodi, LUN, volumi, aggregati, VM di storage, interfacce FC, porte FC, porte Ethernet e interfacce IP.

Il `/metrics` e. `/analytics` Le API offrono diverse viste delle metriche delle performance, utilizzando le quali è possibile eseguire il drill-down a diversi livelli di dettagli per i seguenti oggetti di storage nel data center:

- cluster
- nodi
- VM di storage
- aggregati
- volumi
- LUN
- Interfacce FC
- Porte FC
- Porte Ethernet
- Interfacce IP

La seguente tabella traccia un confronto tra `/metrics` e. `/analytics` API per quanto riguarda i dettagli dei dati delle performance recuperati.

Metriche	Analytics
Dettagli delle performance per un singolo oggetto. Ad esempio, il `/datacenter/cluster/clusters/{key}/metrics` API richiede che la chiave del cluster sia inserita come parametro di percorso per il recupero delle metriche per quel cluster specifico.	Dettagli sulle performance per più oggetti dello stesso tipo in un data center. Ad esempio, il `/datacenter/cluster/clusters/analytics` API recupera le metriche collettive di tutti i cluster di un data center.

Metriche	Analytics
Esempio di metriche di performance per un oggetto storage basato sul parametro dell'intervallo di tempo per il recupero.	Valore aggregato di alto livello delle performance per un determinato tipo di oggetto storage per un determinato periodo (oltre 72 ore).
Vengono recuperati i dettagli di base dell'oggetto, ad esempio i dettagli di un nodo o di un cluster.	Non vengono recuperati dettagli specifici.
I contatori accumulati, ad esempio minimo, massimo, 95° percentile e i valori medi delle prestazioni in un determinato periodo di tempo, vengono recuperati per un singolo oggetto, ad esempio lettura, scrittura, totale e altri contatori.	Viene visualizzato un singolo valore aggregato per tutti gli oggetti dello stesso tipo.

Metriche	Analytics
L’intervallo di tempo e i dati di esempio si basano sulla seguente pianificazione: L’intervallo di tempo per i dati. Ad esempio 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6 m. Si ottengono campioni di 1 ora se l’intervallo è superiore a 3 giorni (72 ore), altrimenti si tratta di campioni di 5 minuti. Il periodo per ciascun intervallo di tempo è il seguente: • 1h: Metriche nell’ora più recente campionate in 5 minuti. • 12h: Metriche nelle ultime 12 ore campionate in 5 minuti. • 1d: Metriche nell’ultimo giorno campionate in 5 minuti. • 2d: Metriche degli ultimi 2 giorni campionate in 5 minuti. • 3d: Metriche degli ultimi 3 giorni campionate in 5 minuti. • 15d: Metriche relative ai 15 giorni più recenti campionati in 1 ora. • 1w: Metriche della settimana più recente campionate in 1 ora. • 1M: Metriche nel mese più recente campionate in 1 ora. • 2 m: Metriche degli ultimi 2 mesi campionate in un’ora. • 3 milioni: Metriche degli ultimi 3 mesi campionate in 1 ora. • 6M: Metriche degli ultimi 6 mesi campionati in 1 ora. Valori disponibili: 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6 m. Valore predefinito: 1h	Oltre 72 ore. La durata del calcolo di questo campione è rappresentata nel formato standard ISO-8601.

Esempio di output per le API di metriche

Ad esempio, il `/datacenter/cluster/nodes/{key}/metrics` API recupera i seguenti dettagli (tra gli altri) per un nodo:

Il 95 percentile nel valore di riepilogo indica che il 95% dei campioni raccolti per il periodo ha un valore di contatore inferiore al valore specificato come 95 percentile.

```
{
```

```
      "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
      }
    },
```

Esempio di output per le API di analisi

Ad esempio, il `/datacenter/cluster/nodes/analytics` API recupera i seguenti valori (tra gli altri) per tutti i nodi:

```
{     "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"
       }
     }
   },
```


Elenco delle API disponibili

La seguente tabella descrive `/metrics` e. `/analytics` API nei dettagli.

> Gli IOPS e le metriche delle performance restituite da queste API sono valori doppi, ad esempio `100.53`. Il filtraggio di questi valori float in base ai caratteri pipe (|) e jolly (*) non è supportato.

Verbo HTTP	Percorso	Descrizione
GET	/datacenter/cluster/clusters/{key}/metrics	Recupera i dati delle performance (campione e riepilogo) per un cluster specificato dal parametro di input della chiave del cluster. Vengono restituite informazioni quali la chiave del cluster e UUID, l'intervallo di tempo, gli IOPS, il throughput e il numero di campioni.
GET	/datacenter/cluster/clusters/analytics	Recupera metriche di performance di alto livello per tutti i cluster di un data center. È possibile filtrare i risultati in base ai criteri richiesti. Vengono restituiti valori come IOPS aggregati, throughput e periodo di raccolta (in ore).
GET	/datacenter/cluster/nodes/{key}/metrics	Recupera i dati delle performance (campione e riepilogo) per un nodo specificato dal parametro di input della chiave del nodo. Vengono restituite informazioni quali UUID del nodo, intervallo di tempo, riepilogo degli IOPS, throughput, latenza e performance, numero di campioni raccolti e percentuale utilizzata.
GET	/datacenter/cluster/nodes/analytics	Recupera metriche di performance di alto livello per tutti i nodi di un data center. È possibile filtrare i risultati in base ai criteri richiesti. Vengono restituite informazioni, come chiavi di nodo e cluster, e valori, come IOPS aggregati, throughput e periodo di raccolta (in ore).
GET	/datacenter/storage/aggregates/{key}/metrics	Recupera i dati delle performance (campione e riepilogo) per un aggregato specificato dal parametro di input della chiave aggregata. Vengono restituite informazioni quali intervallo di tempo, riepilogo degli IOPS, latenza, throughput e capacità delle performance, il numero di campioni raccolti per ciascun contatore e la percentuale utilizzata.

Verbo HTTP	Percorso	Descrizione
GET	/datacenter/storage/aggregates/analytics	Recupera metriche di performance di alto livello per tutti gli aggregati di un data center. È possibile filtrare i risultati in base ai criteri richiesti. Vengono restituite informazioni, come chiavi di aggregato e cluster, e valori, come IOPS aggregati, throughput e periodo di raccolta (in ore).
GET	/datacenter/storage/luns/{key}/metrics /datacenter/storage/volumes/{key}/metrics	Recupera i dati sulle prestazioni (campione e riepilogo) per una LUN o una condivisione di file (volume) specificata dal parametro di input della chiave LUN o volume. Informazioni, come il riepilogo degli IOPS minimi, massimi e medi di lettura, scrittura e totale, latenza e throughput, e il numero di campioni raccolti per ciascun contatore viene restituito.
GET	/datacenter/storage/luns/analytics /datacenter/storage/volumes/analytics	Recupera metriche di performance di alto livello per tutti i LUN o volumi in un data center. È possibile filtrare i risultati in base ai criteri richiesti. Vengono restituite informazioni, come le chiavi di storage VM e cluster, e valori, come IOPS aggregati, throughput e periodo di raccolta (in ore).
GET	/datacenter/svm/svms/{key}/metrics	Recupera i dati sulle performance (campione e riepilogo) per una VM di storage specificata dal parametro di input della chiave della VM di storage. Riepilogo degli IOPS in base a ciascun protocollo supportato, ad esempio `nvmf, fcp, iscsi,` e. `nfs`, throughput, latenza e il numero di campioni raccolti vengono restituiti.

Verbo HTTP	Percorso	Descrizione
GET	/datacenter/svm/svms/analytics	Recupera metriche di performance di alto livello per tutte le VM di storage in un data center. È possibile filtrare i risultati in base ai criteri richiesti. Vengono restituite informazioni come UUID VM storage, IOPS aggregati, latenza, throughput e periodo di raccolta (in ore).
GET	/datacenter/network/ethernet/ports/{key}/metrics	Recupera le metriche delle prestazioni per una porta ethernet specifica specificata dal parametro di input della chiave della porta. Quando viene fornito un intervallo (intervallo di tempo) dall'intervallo supportato, l'API restituisce i contatori accumulati, ad esempio i valori minimi, massimi e medi delle prestazioni nel periodo di tempo.
GET	/datacenter/network/ethernet/ports/analytics	Recupera le metriche di performance di alto livello per tutte le porte ethernet nel tuo ambiente di data center. Vengono restituite informazioni quali la chiave del cluster e del nodo e UUID, il throughput, il periodo di raccolta e la percentuale di utilizzo per le porte. È possibile filtrare il risultato in base ai parametri disponibili, ad esempio la chiave della porta, la percentuale di utilizzo, il nome del cluster e del nodo, l'UUID e così via.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Recupera le metriche delle performance per una specifica interfaccia FC di rete specificata dal parametro di input della chiave di interfaccia. Quando viene fornito un intervallo (intervallo di tempo) dall'intervallo supportato, l'API restituisce i contatori accumulati, ad esempio i valori minimi, massimi e medi delle prestazioni nel periodo di tempo.

Verbo HTTP	Percorso	Descrizione
GET	/datacenter/network/fc/interfaces/analytics	Recupera le metriche di performance di alto livello per tutte le porte ethernet nel tuo ambiente di data center. Vengono restituite informazioni quali cluster e chiave di interfaccia FC e UUID, throughput, IOPS, latenza e VM di storage. È possibile filtrare il risultato in base ai parametri disponibili, ad esempio il nome del cluster e dell'interfaccia FC, UUID, VM di storage, throughput e così via.
GET	/datacenter/network/fc/ports/{key}/metrics	Recupera le metriche delle performance per una porta FC specifica specificata dal parametro di input della chiave della porta. Quando viene fornito un intervallo (intervallo di tempo) dall'intervallo supportato, l'API restituisce i contatori accumulati, ad esempio i valori minimi, massimi e medi delle prestazioni nel periodo di tempo.
GET	/datacenter/network/fc/ports/analytics	Recupera le metriche di performance di alto livello per tutte le porte FC nel tuo ambiente di data center. Vengono restituite informazioni quali la chiave del cluster e del nodo e UUID, il throughput, il periodo di raccolta e la percentuale di utilizzo per le porte. È possibile filtrare il risultato in base ai parametri disponibili, ad esempio la chiave della porta, la percentuale di utilizzo, il nome del cluster e del nodo, l'UUID e così via.

Verbo HTTP	Percorso	Descrizione
GET	/datacenter/network/ip/interfaces/{key}/metrics	Recupera le metriche di performance per un'interfaccia IP di rete come specificato dal parametro di input della chiave di interfaccia. Quando viene fornito un intervallo (intervallo di tempo) dall'intervallo supportato, l'API restituisce informazioni, come il numero di campioni, i contatori accumulati, il throughput e il numero di pacchetti ricevuti e trasmessi.
GET	/datacenter/network/ip/interfaces/analytics	Recupera le metriche di performance di alto livello per tutte le interfacce IP di rete nell'ambiente del data center. Vengono restituite informazioni quali il cluster e la chiave di interfaccia IP, UUID, throughput, IOPS e latenza. È possibile filtrare il risultato in base ai parametri disponibili, ad esempio il nome del cluster e dell'interfaccia IP e UUID, IOPS, latenza, throughput e così via.

Visualizzazione dei processi e dei dettagli di sistema

È possibile utilizzare `jobs` API in `management-server` per visualizzare i dettagli di esecuzione delle operazioni asincrone. Il `system` API in `management-server` Category (Categoria) consente di visualizzare i dettagli dell'istanza nell'ambiente Active IQ Unified Manager.

Visualizzazione dei lavori

In Active IQ Unified Manager, le operazioni, come l'aggiunta e la modifica delle risorse, vengono eseguite mediante invocazioni API sincrone e asincrone. Le invocazioni pianificate per l'esecuzione asincrona possono essere monitorate da un oggetto Job creato per tale invocazione. Ogni oggetto Job dispone di una chiave univoca per l'identificazione. Ogni oggetto Job restituisce l'URI dell'oggetto Job per consentire all'utente di accedere e tenere traccia dell'avanzamento del lavoro. È possibile utilizzare questa API per recuperare i dettagli di ciascuna esecuzione.

Utilizzando questa API, è possibile eseguire query su tutti gli oggetti di lavoro del data center, inclusi i dati storici. L'interrogazione di tutti i lavori, per impostazione predefinita, restituisce i dettagli degli ultimi 20 lavori attivati tramite l'interfaccia API e l'interfaccia utente Web. Utilizzare i filtri integrati per visualizzare lavori specifici. È inoltre possibile utilizzare la chiave Job per eseguire query sui dettagli di un lavoro specifico ed eseguire il successivo set di operazioni sulle risorse.

Categoria	Verbo HTTP	Percorso	Descrizione
server di gestione	OTTIENI	`/management-server/jobs`	Restituisce i dettagli di tutti i lavori. Senza alcun ordinamento, l'ultimo oggetto Job inviato viene restituito in primo piano.
server di gestione	OTTIENI	`/management-server/jobs/{key}` Inserire la chiave del lavoro dell'oggetto Job per visualizzare i dettagli specifici del lavoro.	Restituisce i dettagli dell'oggetto Job specifico.

Visualizzazione dei dettagli del sistema

Utilizzando `/management-server/system` API, è possibile eseguire query sui dettagli specifici dell'istanza dell'ambiente Unified Manager. L'API restituisce informazioni sul prodotto e sui servizi, ad esempio la versione di Unified Manager installata nel sistema, UUID, nome del vendor, sistema operativo host e nome, Descrizione e stato dei servizi in esecuzione sull'istanza di Unified Manager.

Categoria	Verbo HTTP	Percorso	Descrizione
server di gestione	OTTIENI	`/management-server/system`	Non è richiesto alcun parametro di input per l'esecuzione di questa API. Per impostazione predefinita, vengono restituiti i dettagli di sistema dell'istanza corrente di Unified Manager.

Gestione di eventi e avvisi tramite API

Il `events`, `alerts`, e. `scripts` API in `management-server` Category consente di gestire gli eventi, gli avvisi e gli script associati agli avvisi nell'ambiente Active IQ Unified Manager.

Visualizzazione e modifica degli eventi

Unified Manager riceve gli eventi generati su ONTAP per i cluster monitorati e gestiti da Unified Manager. Utilizzando queste API, è possibile visualizzare gli eventi generati per i cluster, risolverli e aggiornarli.

Eseguendo il `GET` metodo per `/management-server/events` API, è possibile eseguire query sugli eventi nel data center, inclusi i dati storici. Utilizzare i filtri integrati, ad esempio nome, livello di impatto, area di impatto, severità, stato, nome della risorsa e tipo di risorsa, per visualizzare eventi specifici. I parametri relativi al tipo di risorsa e all'area restituiscono informazioni sull'oggetto di storage in cui si è verificato l'evento e l'area di impatto restituisce le informazioni relative al problema per cui viene generato l'evento, ad esempio

disponibilità, capacità, configurazione, sicurezza, protezione e performance.

Eseguendo l'operazione DI PATCH per questa API, è possibile attivare il flusso di lavoro di risoluzione per l'evento. È possibile assegnare un evento a se stessi o a un altro utente e confermare la ricezione dell'evento. Quando si eseguono le procedure relative alle risorse per risolvere il problema che ha generato l'evento, è possibile utilizzare questa API per contrassegnare l'evento come risolto.

Per ulteriori informazioni sugli eventi, vedere "Gestione degli eventi".

Categoria	Verbo HTTP	Percorso	Descrizione
server di gestione	OTTIENI	`/management-server/events` `/management-server/events/{key}`	Quando si esegue il metodo Get ALL, il corpo della risposta è costituito dai dettagli degli eventi di tutti gli eventi nel data center. Quando si recuperano i dettagli dell'evento mediante una chiave specifica, è possibile visualizzare i dettagli di un evento specifico ed eseguire il successivo set di operazioni sulle risorse. Il corpo della risposta è costituito dai dettagli dell'evento.
server di gestione	PATCH	`management-server/events/{key}`	Eseguire questa API per assegnare un evento o modificare lo stato in riconosciuto o risolto. È inoltre possibile utilizzare questo metodo per assegnare l'evento a se stessi o a un altro utente. Si tratta di un'operazione sincrona.

Gestione degli avvisi

Gli eventi vengono generati automaticamente e continuamente. Unified Manager genera un avviso solo quando un evento soddisfa determinati criteri di filtro. È possibile selezionare gli eventi per i quali devono essere generati gli avvisi. Utilizzando `/management-server/alerts` API, è possibile configurare gli avvisi per inviare automaticamente le notifiche quando si verificano eventi o eventi specifici di determinati tipi di severità.

Per ulteriori informazioni sugli avvisi, vedere "Gestione degli avvisi".

Categoria	Verbo HTTP	Percorso	Descrizione
server di gestione	OTTIENI	`/management-server/alerts` `/management-server/alerts/{key}`	Eseguire una query su tutti gli avvisi esistenti nel proprio ambiente o su uno specifico avviso utilizzando il tasto alert. È possibile visualizzare le informazioni sugli avvisi generati nell'ambiente, ad esempio la descrizione dell'avviso, l'azione, l'ID e-mail a cui viene inviata la notifica, l'evento e la gravità.
server di gestione	POST	`/management-server/alerts`	Questo metodo consente di aggiungere avvisi per eventi specifici. È necessario aggiungere il nome dell'avviso, la risorsa fisica o logica o l'evento a cui è applicabile l'avviso, se l'avviso è attivato e se si stanno emettendo trap SNMP. È possibile aggiungere ulteriori dettagli per i quali si desidera generare l'avviso, ad esempio l'azione, l'ID e-mail di notifica, i dettagli dello script, nel caso in cui si aggiunga uno script di avviso e così via.
server di gestione	APPLICARE PATCH ed ELIMINARE	`management-server/events/{key}`	È possibile utilizzare questi metodi per modificare ed eliminare avvisi specifici. È possibile modificare diversi attributi, ad esempio descrizione, nome e attivazione e disattivazione dell'avviso. È possibile eliminare un avviso quando non è più necessario.

Durante la selezione di una risorsa per l'aggiunta di un avviso, tenere presente che la selezione di un cluster come risorsa non consente di selezionare automaticamente gli oggetti di storage all'interno di tale cluster. Ad esempio, se si crea un avviso per tutti gli eventi critici per tutti i cluster, si riceveranno avvisi solo per gli eventi critici del cluster. Non riceverai avvisi per eventi critici su nodi, aggregati e così via.

Gestione degli script

Utilizzando `/management-server/scripts` API, è anche possibile associare un avviso a uno script eseguito quando viene attivato un avviso. È possibile utilizzare gli script per modificare o aggiornare automaticamente più oggetti di storage in Unified Manager. Lo script è associato a un avviso. Quando un evento attiva un avviso, lo script viene eseguito. È possibile caricare script personalizzati e testarne l'esecuzione quando viene generato un avviso. È possibile associare un avviso allo script in modo che venga eseguito quando viene generato un avviso per un evento in Unified Manager.

Per ulteriori informazioni sugli script, vedere "Gestione degli script".

Categoria	Verbo HTTP	Percorso	Descrizione
server di gestione	OTTIENI	`/management-server/scripts`	Utilizzare questa API per eseguire query su tutti gli script esistenti nell'ambiente. Utilizzare il filtro standard e le operazioni Ordina per per visualizzare solo script specifici.
server di gestione	POST	`/management-server/scripts`	Utilizzare questa API per aggiungere una descrizione dello script e caricare il file di script associato a un avviso.

Gestione dei carichi di lavoro tramite API

Le API descritte in questa sezione coprono varie funzioni di amministrazione dello storage, come la visualizzazione dei carichi di lavoro dello storage, la creazione di LUN e condivisioni di file, la gestione dei livelli di servizio delle performance e delle policy di efficienza dello storage e l'assegnazione delle policy sui carichi di lavoro dello storage.

Visualizzazione dei carichi di lavoro dello storage mediante API

Le API elencate di seguito consentono di visualizzare un elenco consolidato di carichi di lavoro dello storage per tutti i cluster ONTAP nel data center. Le API forniscono inoltre una vista riepilogativa del numero di carichi di lavoro dello storage forniti nell'ambiente Active IQ Unified Manager e delle relative statistiche di capacità e performance (IOPS).

Visualizza i carichi di lavoro dello storage

Puoi utilizzare il seguente metodo per visualizzare tutti i carichi di lavoro dello storage in tutti i cluster del tuo data center. Per informazioni sul filtraggio della risposta in base a colonne specifiche, consultare la documentazione di riferimento API disponibile nell'istanza di Unified Manager.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/workloads`

Visualizza il riepilogo dei carichi di lavoro dello storage

È possibile utilizzare il seguente metodo per valutare la capacità utilizzata, la capacità disponibile, gli IOPS utilizzati, gli IOPS disponibili e il numero di carichi di lavoro dello storage gestiti da ciascun livello di servizio delle performance. I carichi di lavoro dello storage visualizzati possono essere per qualsiasi condivisione LUN, file share NFS o CIFS. L'API offre una panoramica dei carichi di lavoro dello storage, una panoramica dei carichi di lavoro dello storage forniti da Unified Manager, una panoramica del data center, una panoramica dello spazio totale, utilizzato e disponibile e degli IOPS nel data center, in termini di livelli di Performance Service assegnati. Le informazioni ricevute in risposta a questa API vengono utilizzate per popolare la dashboard nell'interfaccia utente di Unified Manager.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/workloads-summary`

Gestione degli endpoint di accesso tramite API

È necessario creare endpoint di accesso o interfacce logiche (LIFF), necessari per il provisioning di Storage Virtual Machine (SVM), LUN e condivisioni di file. È possibile visualizzare, creare, modificare ed eliminare gli endpoint di accesso per le SVM, le LUN o le condivisioni di file nell'ambiente Active IQ Unified Manager.

Visualizzare gli endpoint di accesso

È possibile visualizzare un elenco degli endpoint di accesso nell'ambiente Unified Manager utilizzando il seguente metodo. Per eseguire una query su un elenco di endpoint di accesso di una specifica SVM, LUN o condivisione file, è necessario inserire l'identificatore univoco per SVM, LUN o condivisione file. È inoltre possibile inserire la chiave univoca dell'endpoint di accesso per recuperare i dettagli dell'endpoint di accesso specifico.

Categoria	Verbo HTTP	Percorso

provider di storage	OTTIENI	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

Aggiungere endpoint di accesso

È possibile creare endpoint di accesso personalizzati e assegnarvi le proprietà richieste. Immettere i dettagli dell'endpoint di accesso che si desidera creare come parametri di input. È possibile utilizzare questa API, il Gestore di sistema o l'interfaccia utente di ONTAP per creare un endpoint di accesso su ciascun nodo. Gli indirizzi IPv4 e IPv6 sono supportati per la creazione degli endpoint di accesso.

> È necessario configurare la SVM con un numero minimo di endpoint di accesso per nodo per il corretto provisioning delle LUN e delle condivisioni file. È necessario configurare la SVM con almeno due endpoint di accesso per nodo, uno che supporti il protocollo CIFS e/o NFS e un altro che supporti il protocollo iSCSI o FCP.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/access-endpoints`

Eliminare gli endpoint di accesso

È possibile eliminare un endpoint di accesso specifico utilizzando il seguente metodo. È necessario fornire la chiave dell'endpoint di accesso come parametro di input per eliminare un particolare endpoint di accesso.

Categoria	Verbo HTTP	Percorso
provider di storage	ELIMINARE	`/storage-provider/access-endpoints/{key}`

Modificare gli endpoint di accesso

È possibile modificare un endpoint di accesso e aggiornarne le proprietà utilizzando il seguente metodo. Per modificare un particolare endpoint di accesso, è necessario fornire la chiave dell'endpoint di accesso. È inoltre necessario immettere la proprietà che si desidera aggiornare, insieme al relativo valore.

Categoria	Verbo HTTP	Percorso
provider di storage	PATCH	`/storage-provider/access-endpoints/{key}`

Gestione del mapping di Active Directory tramite API

È possibile utilizzare le API elencate di seguito per gestire le mappature di Active Directory sulla SVM necessarie per il provisioning delle condivisioni CIFS sulle SVM. È necessario configurare le mappature di Active Directory per il mapping delle SVM con ONTAP.

Visualizzare le mappature di Active Directory

È possibile visualizzare i dettagli di configurazione delle mappature di Active Directory per una SVM utilizzando il seguente metodo. Per visualizzare le mappature di Active Directory su una SVM, è necessario inserire la chiave SVM. Per eseguire query sui dettagli di una mappatura specifica, è necessario inserire la chiave di

mappatura.

Categoria	Verbo HTTP	Percorso

provider di storage	OTTIENI	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

Aggiungi mappatura Active Directory

È possibile creare mappature di Active Directory su una SVM utilizzando il seguente metodo. Inserire i dettagli della mappatura come parametri di input.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/active-directories-mappings`

Gestione delle condivisioni di file mediante API

È possibile utilizzare `/storage-provider/file-shares` API per visualizzare, aggiungere, modificare ed eliminare i volumi di condivisione file CIFS e NFS nell'ambiente del data center.

Prima di eseguire il provisioning dei volumi di condivisione file, assicurarsi che la SVM sia stata creata e fornita con i protocolli supportati. Se si assegnano livelli di servizio delle performance (PSL) o criteri di efficienza dello storage (SEPS) durante il provisioning, è necessario creare PSL o SEPS prima di creare le condivisioni di file.

Visualizzare le condivisioni di file

È possibile utilizzare il seguente metodo per visualizzare i volumi di condivisione file disponibili nell'ambiente Unified Manager. Una volta aggiunto un cluster ONTAP come origine dati su Active IQ Unified Manager, i carichi di lavoro dello storage per tali cluster vengono aggiunti automaticamente all'istanza di Unified Manager. Questa API recupera automaticamente le condivisioni file e le aggiunge manualmente all'istanza di Unified Manager. È possibile visualizzare i dettagli di una condivisione file specifica eseguendo questa API con la chiave di condivisione file.

Categoria	Verbo HTTP	Percorso

provider di storage	OTTIENI	`/storage-provider/file-shares`
		
		`/storage-provider/file-shares/{key}`

Aggiungere condivisioni di file

È possibile utilizzare il seguente metodo per aggiungere condivisioni di file CIFS e NFS nella SVM. Immettere i dettagli della condivisione file che si desidera creare, come parametri di input. Non è possibile utilizzare questa

API per aggiungere volumi FlexGroup.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/file-shares`

A seconda che siano forniti i parametri dell'elenco di controllo di accesso (ACL) o i parametri dei criteri di esportazione, vengono create condivisioni CIFS o condivisioni file NFS. Se non si forniscono i valori per i parametri ACL, le condivisioni CIFS non vengono create e le condivisioni NFS vengono create per impostazione predefinita, fornendo l'accesso a tutti.

Creazione di volumi di protezione dei dati: Quando si aggiungono condivisioni di file a SVM, il tipo di volume montato, per impostazione predefinita, è `rw` (lettura/scrittura). Per creare volumi di protezione dei dati (DP), specificare `dp` come valore per `type` parametro.

Eliminare le condivisioni di file

Per eliminare una condivisione file specifica, è possibile utilizzare il metodo seguente. Per eliminare una determinata condivisione file, è necessario inserire la chiave di condivisione file come parametro di input.

Categoria	Verbo HTTP	Percorso
provider di storage	ELIMINARE	`/storage-provider/file-shares/{key}`

Modificare le condivisioni di file

È possibile utilizzare il seguente metodo per modificare una condivisione file e aggiornarne le proprietà.

È necessario fornire la chiave di condivisione file per modificare una determinata condivisione file. Inoltre, è necessario immettere la proprietà che si desidera aggiornare, insieme al relativo valore.

Tenere presente che è possibile aggiornare solo una proprietà a una singola chiamata di questa API. Per gli aggiornamenti multipli, è necessario eseguire questa API tante volte.

Categoria	Verbo HTTP	Percorso
provider di storage	PATCH	`/storage-provider/file-shares/{key}`

Gestione delle LUN tramite API

È possibile utilizzare `/storage-provider/luns` API per visualizzare, aggiungere, modificare ed eliminare le LUN nell'ambiente del data center.

Prima di eseguire il provisioning dei LUN, assicurarsi che la SVM sia stata creata e fornita con i protocolli supportati. Se si assegnano livelli di servizio delle performance (PSL) o criteri di efficienza dello storage (SEPS) durante il provisioning, è necessario creare PSL o SEPS prima di creare il LUN.

Visualizza LUN

È possibile utilizzare il seguente metodo per visualizzare le LUN nell'ambiente Unified Manager. Una volta aggiunto un cluster ONTAP come origine dati su Active IQ Unified Manager, i carichi di lavoro dello storage per tali cluster vengono aggiunti automaticamente all'istanza di Unified Manager. Questa API recupera tutte le LUN automaticamente e aggiunte manualmente all'istanza di Unified Manager. È possibile visualizzare i dettagli di un LUN specifico eseguendo questa API con la chiave LUN.

Categoria	Verbo HTTP	Percorso

provider di storage	OTTIENI	`/storage-provider/luns`
		
		`/storage-provider/luns/{key}`

Aggiungere LUN

È possibile utilizzare il seguente metodo per aggiungere LUN alle SVM.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/luns`

Nella richiesta curl, se si fornisce un valore per il parametro opzionale volume_name_tag nell'input, tale valore viene utilizzato durante la creazione del LUN. Questo tag consente di eseguire ricerche nel volume in modo semplice. Se si specifica il tasto volume nella richiesta, il tagging viene ignorato.

Elimina LUN

Per eliminare una LUN specifica, utilizzare il metodo seguente. Per eliminare una determinata LUN, è necessario fornire la chiave LUN.

Se è stato creato un volume in ONTAP e poi eseguito il provisioning delle LUN tramite Unified Manager su tale volume, quando si eliminano tutte le LUN utilizzando questa API, il volume viene eliminato anche dal cluster ONTAP.

Categoria	Verbo HTTP	Percorso
provider di storage	ELIMINARE	`/storage-provider/luns/{key}`

Modificare i LUN

È possibile utilizzare il seguente metodo per modificare un LUN e aggiornarne le proprietà. Per modificare una determinata LUN, è necessario fornire la chiave LUN. È inoltre necessario immettere la proprietà LUN che si desidera aggiornare, insieme al relativo valore. Per aggiornare gli array LUN utilizzando questa API, consultare le raccomandazioni in "Recommendations for Using the API".

È possibile aggiornare solo una proprietà a una singola chiamata di questa API. Per gli aggiornamenti multipli, è necessario eseguire questa API tante volte.

Categoria	Verbo HTTP	Percorso
provider di storage	PATCH	`/storage-provider/luns/{key}`

Gestione dei livelli di servizio delle performance tramite le API

È possibile visualizzare, creare, modificare ed eliminare i livelli dei servizi di performance utilizzando le API del provider di storage per sul proprio Active IQ Unified Manager.

Visualizza i livelli di Performance Service

È possibile utilizzare il seguente metodo per visualizzare i livelli di Performance Service per assegnarli ai carichi di lavoro dello storage. L'API elenca tutti i livelli di Performance Service definiti dal sistema e creati dall'utente e recupera gli attributi di tutti i livelli di Performance Service. Se si desidera eseguire una query su uno specifico livello di servizio delle prestazioni, è necessario inserire l'ID univoco del livello di servizio delle prestazioni per recuperarne i dettagli.

Categoria	Verbo HTTP	Percorso

provider di storage	OTTIENI	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

Aggiungere livelli di servizio delle performance

È possibile utilizzare il seguente metodo per creare livelli di Performance Service personalizzati e assegnarli ai carichi di lavoro dello storage se i livelli di Performance Service definiti dal sistema non soddisfano gli obiettivi del livello di servizio (SLO) richiesti per i carichi di lavoro dello storage. Inserire i dettagli del livello di servizio Performance che si desidera creare. Per le proprietà IOPS, assicurarsi di immettere un intervallo di valori valido.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/performance-service-levels`

Eliminare i livelli di Performance Service

È possibile utilizzare il seguente metodo per eliminare uno specifico livello di servizio delle prestazioni. Non è possibile eliminare un livello di servizio delle performance se è assegnato a un carico di lavoro o se è l'unico livello di servizio delle performance disponibile. È necessario fornire l'ID univoco del livello di servizio

Performance come parametro di input per eliminare un determinato livello di servizio Performance.

Categoria	Verbo HTTP	Percorso
provider di storage	ELIMINARE	`/storage-provider/performance-service-levels/{key}`

Modificare i livelli di Performance Service

È possibile utilizzare il seguente metodo per modificare un livello di servizio delle prestazioni e aggiornarne le proprietà. Non è possibile modificare un livello di servizio delle prestazioni definito dal sistema o assegnato a un carico di lavoro. Per modificare un determinato livello di servizio delle prestazioni, è necessario fornire l'ID univoco di. È inoltre necessario immettere la proprietà IOPS che si desidera aggiornare, insieme a un valore valido.

Categoria	Verbo HTTP	Percorso
provider di storage	PATCH	`/storage-provider/performance-service-levels/{key}`

Visualizzazione delle funzionalità aggregate in base ai livelli di Performance Service

È possibile utilizzare il seguente metodo per eseguire query sulle funzionalità aggregate in base ai livelli di Performance Service. Questa API restituisce l'elenco degli aggregati disponibili nel data center e indica le funzionalità in termini di livelli di servizio delle performance che possono essere supportati in tali aggregati. Durante il provisioning dei carichi di lavoro su un volume, è possibile visualizzare la capacità di un aggregato di supportare un determinato livello di servizio delle performance e di eseguire il provisioning dei carichi di lavoro in base a tale funzionalità. La possibilità di specificare l'aggregato è disponibile solo quando si esegue il provisioning di un carico di lavoro utilizzando le API. Questa funzionalità non è disponibile nell'interfaccia utente Web di Unified Manager.

Categoria	Verbo HTTP	Percorso

provider di storage	OTTIENI	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

Gestione delle policy di efficienza dello storage tramite API

È possibile visualizzare, creare, modificare ed eliminare le policy di efficienza dello storage utilizzando le API del provider di storage.

Prendere nota dei seguenti punti:

- Non è obbligatorio assegnare una policy di efficienza dello storage durante la creazione di un carico di lavoro su Unified Manager.
- Non è possibile annullare l'assegnazione di una policy di efficienza dello storage a un workload dopo l'assegnazione di una policy.
- Se un carico di lavoro ha alcune impostazioni di storage specificate sui volumi ONTAP, come deduplica e compressione, tali impostazioni possono essere sovrascritte dalle impostazioni specificate nella policy di efficienza dello storage applicata quando si aggiungono i carichi di lavoro dello storage su Unified Manager.

Visualizza le policy di efficienza dello storage

È possibile utilizzare il seguente metodo per visualizzare le policy di efficienza dello storage prima di assegnarle ai carichi di lavoro dello storage. Questa API elenca tutte le policy di efficienza dello storage definite dal sistema e create dall'utente e recupera gli attributi di tutte le policy di efficienza dello storage. Se si desidera eseguire una query su una policy di efficienza dello storage specifica, è necessario inserire l'ID univoco della policy per recuperarne i dettagli.

Categoria	Verbo HTTP	Percorso

provider di storage	OTTIENI	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

Aggiungi policy di efficienza dello storage

È possibile utilizzare il seguente metodo per creare policy di efficienza dello storage personalizzate e assegnarle ai carichi di lavoro dello storage se le policy definite dal sistema non soddisfano i requisiti di provisioning per i carichi di lavoro dello storage. Inserire i dettagli della Storage Efficiency Policy che si desidera creare, come parametri di input.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/storage-efficiency-policies`

Eliminare le policy di efficienza dello storage

È possibile utilizzare il seguente metodo per eliminare una policy di efficienza dello storage specifica. Non è possibile eliminare una policy di efficienza dello storage se assegnata a un workload o se è l'unica policy di efficienza dello storage disponibile. È necessario fornire l'ID univoco della Storage Efficiency Policy come parametro di input per eliminare una particolare Storage Efficiency Policy.

Categoria	Verbo HTTP	Percorso
provider di storage	ELIMINARE	`/storage-provider/storage-efficiency-policies/{key}`

Modificare le policy di efficienza dello storage

È possibile utilizzare il seguente metodo per modificare un criterio di efficienza dello storage e aggiornarne le proprietà. Non è possibile modificare una policy di efficienza dello storage definita dal sistema o assegnata a un carico di lavoro. Per modificare una particolare policy di efficienza dello storage, è necessario fornire l'ID univoco della policy di efficienza dello storage. Inoltre, è necessario fornire la proprietà che si desidera aggiornare, insieme al relativo valore.

Categoria	Verbo HTTP	Percorso
provider di storage	PATCH	`/storage-provider/storage-efficiency-policies/{key}`

Flussi di lavoro API comuni per la gestione dello storage

I flussi di lavoro comuni forniscono agli sviluppatori di applicazioni client esempi di come le API Active IQ Unified Manager possono essere chiamate da un'applicazione client per eseguire funzioni comuni di gestione dello storage. Questa sezione contiene alcuni di questi flussi di lavoro di esempio.

I flussi di lavoro descrivono alcuni dei casi di utilizzo più comuni per la gestione dello storage e i codici di esempio da utilizzare. Ciascuna delle attività viene descritta utilizzando un processo di workflow costituito da una o più chiamate API.

Informazioni sulle chiamate API utilizzate nei flussi di lavoro

È possibile visualizzare la pagina della documentazione online dall'istanza di Unified Manager che include i dettagli di ogni chiamata API REST. Questo documento non ripete i dettagli della documentazione online. Ogni chiamata API utilizzata negli esempi del flusso di lavoro in questo documento include solo le informazioni necessarie per individuare la chiamata nella pagina della documentazione. Dopo aver individuato una chiamata API specifica, è possibile esaminare i dettagli completi della chiamata, inclusi i parametri di input, i formati di output, i codici di stato HTTP e il tipo di elaborazione della richiesta.

Le seguenti informazioni sono incluse per ogni chiamata API all'interno di un flusso di lavoro per facilitare l'individuazione della chiamata nella pagina della documentazione:

- Category (Categoria): Le chiamate API sono organizzate nella pagina della documentazione in aree o categorie correlate alle funzioni. Per individuare una chiamata API specifica, scorrere fino alla fine della pagina e fare clic sulla categoria API appropriata.
- Verbo HTTP (chiamata): Il verbo HTTP identifica l'azione eseguita su una risorsa. Ogni chiamata API viene eseguita tramite un singolo verbo HTTP.
- Percorso: Il percorso determina la risorsa specifica a cui si applica l'azione durante l'esecuzione di una chiamata. La stringa del percorso viene aggiunta all'URL principale per formare l'URL completo che identifica la risorsa.

Determinare i problemi di spazio negli aggregati utilizzando le API

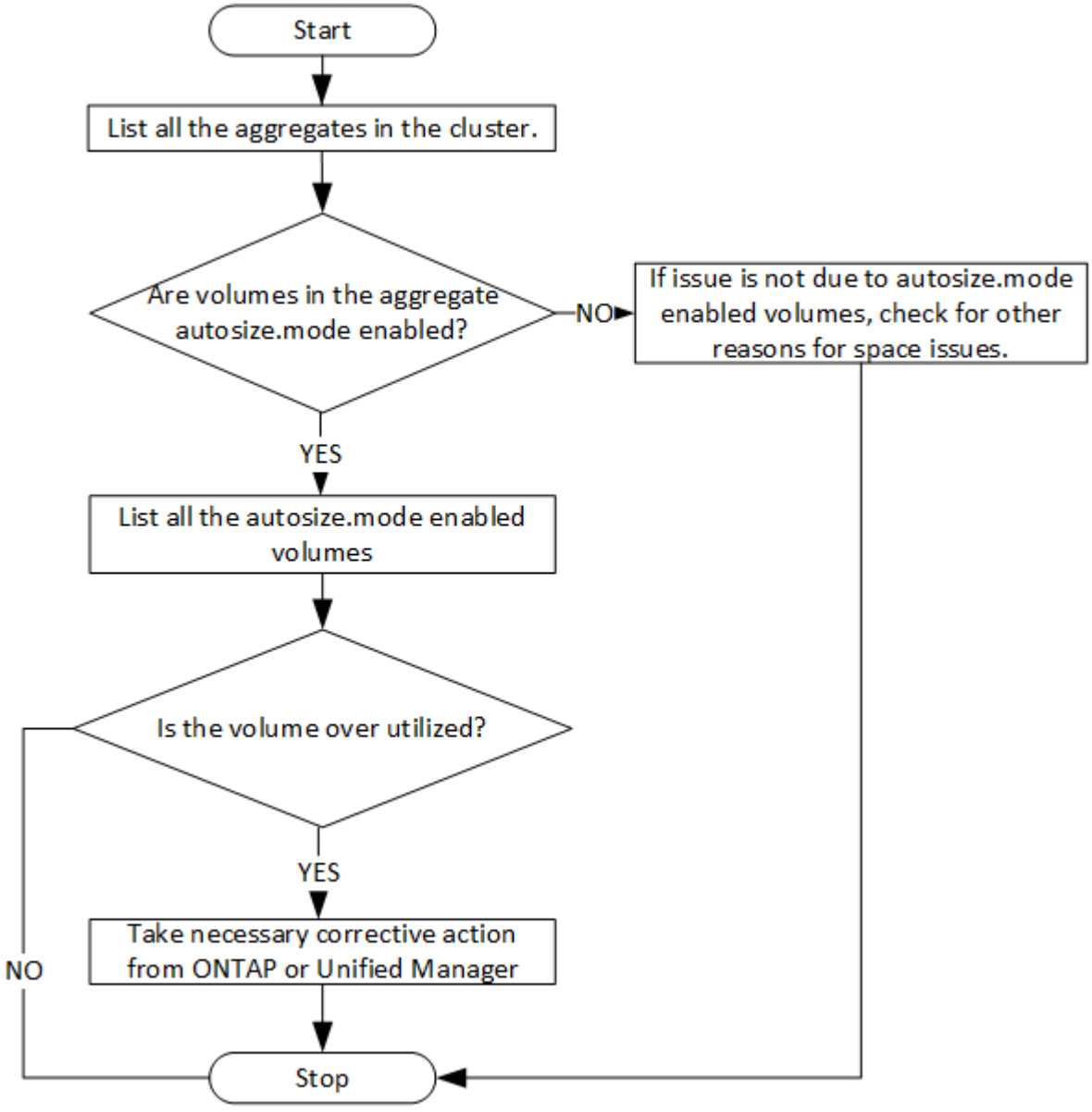
È possibile utilizzare le API del data center in Active IQ Unified Manager per monitorare la disponibilità e l'utilizzo dello spazio nei volumi. È possibile determinare i problemi di spazio nel volume e identificare le risorse di storage che sono sovrautilizzate o

sottoutilizzate.

Le API del data center per gli aggregati recuperano le informazioni rilevanti sullo spazio disponibile e utilizzato e le impostazioni di efficienza per il risparmio di spazio. È inoltre possibile filtrare le informazioni recuperate in base agli attributi specificati.

Un metodo per determinare l'eventuale mancanza di spazio negli aggregati consiste nel verificare la presenza di volumi nell'ambiente con la modalità di dimensionamento automatico attivata. È quindi necessario identificare i volumi che vengono utilizzati in eccesso ed eseguire eventuali azioni correttive.

Il seguente diagramma di flusso illustra il processo di recupero delle informazioni sui volumi con la modalità di dimensionamento automatico attivata:



Questo flusso presuppone che i cluster siano già stati creati in ONTAP e aggiunti a Unified Manager.

1. Ottenere la chiave del cluster, a meno che non si conosca il valore:

Categoria	Verbo HTTP	Percorso
data center	OTTIENI	`/datacenter/cluster/clusters`

2. Utilizzando la chiave del cluster come parametro di filtro, eseguire una query sugli aggregati di quel cluster.

Categoria	Verbo HTTP	Percorso
data center	OTTIENI	`/datacenter/storage/aggregates`

3. Dalla risposta, analizza l'utilizzo dello spazio degli aggregati e determina quali aggregati presentano problemi di spazio. Per ogni aggregato con problemi di spazio, ottenere la chiave aggregata dallo stesso output JSON.
4. Utilizzando ciascuna chiave aggregata, filtrare tutti i volumi con il valore del parametro autodize.mode come `grow`.

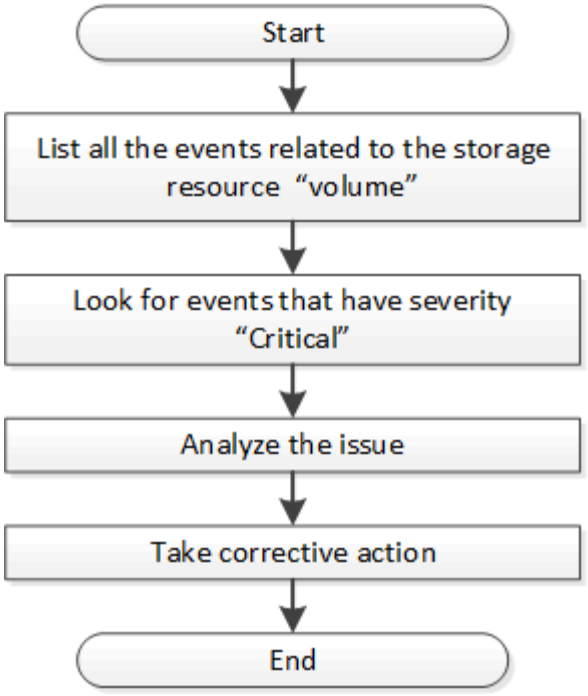
Categoria	Verbo HTTP	Percorso
data center	OTTIENI	`/datacenter/storage/volumes`

5. Analizzare quali volumi vengono utilizzati in eccesso.
6. Eseguire qualsiasi azione correttiva necessaria, ad esempio lo spostamento del volume tra aggregati, per risolvere i problemi di spazio nel volume. È possibile eseguire queste azioni dall'interfaccia utente Web di ONTAP o Unified Manager.

Determinazione dei problemi negli oggetti di storage utilizzando le API degli eventi

Quando un oggetto di storage nel data center supera una soglia, viene inviata una notifica relativa a tale evento. Utilizzando questa notifica, è possibile analizzare il problema e intraprendere azioni correttive utilizzando `events` API.

Questo flusso di lavoro prende l'esempio di un volume come oggetto risorsa. È possibile utilizzare `events` API per recuperare l'elenco degli eventi correlati a un volume, analizzare i problemi critici per quel volume e intraprendere azioni correttive per risolvere il problema.



Prima di intraprendere le azioni correttive, attenersi alla procedura descritta di seguito per determinare i problemi del volume.

Fasi

1. Analizza le notifiche degli eventi critici di Active IQ Unified Manager per i volumi nel tuo data center.
2. Eseguire una query su tutti gli eventi dei volumi utilizzando i seguenti parametri nell’API /management-server/events:
   `"resource_type": "volume"`
   `"severity": "critical"`

Categoria	Verbo HTTP	Percorso
server di gestione	OTTIENI	/server-gestione/eventi

3. Visualizzare l’output e analizzare i problemi nei volumi specifici.
4. Eseguire le azioni necessarie utilizzando le API REST di Unified Manager o l’interfaccia utente Web per risolvere i problemi.

Risoluzione dei problemi relativi ai volumi ONTAP utilizzando le API del gateway

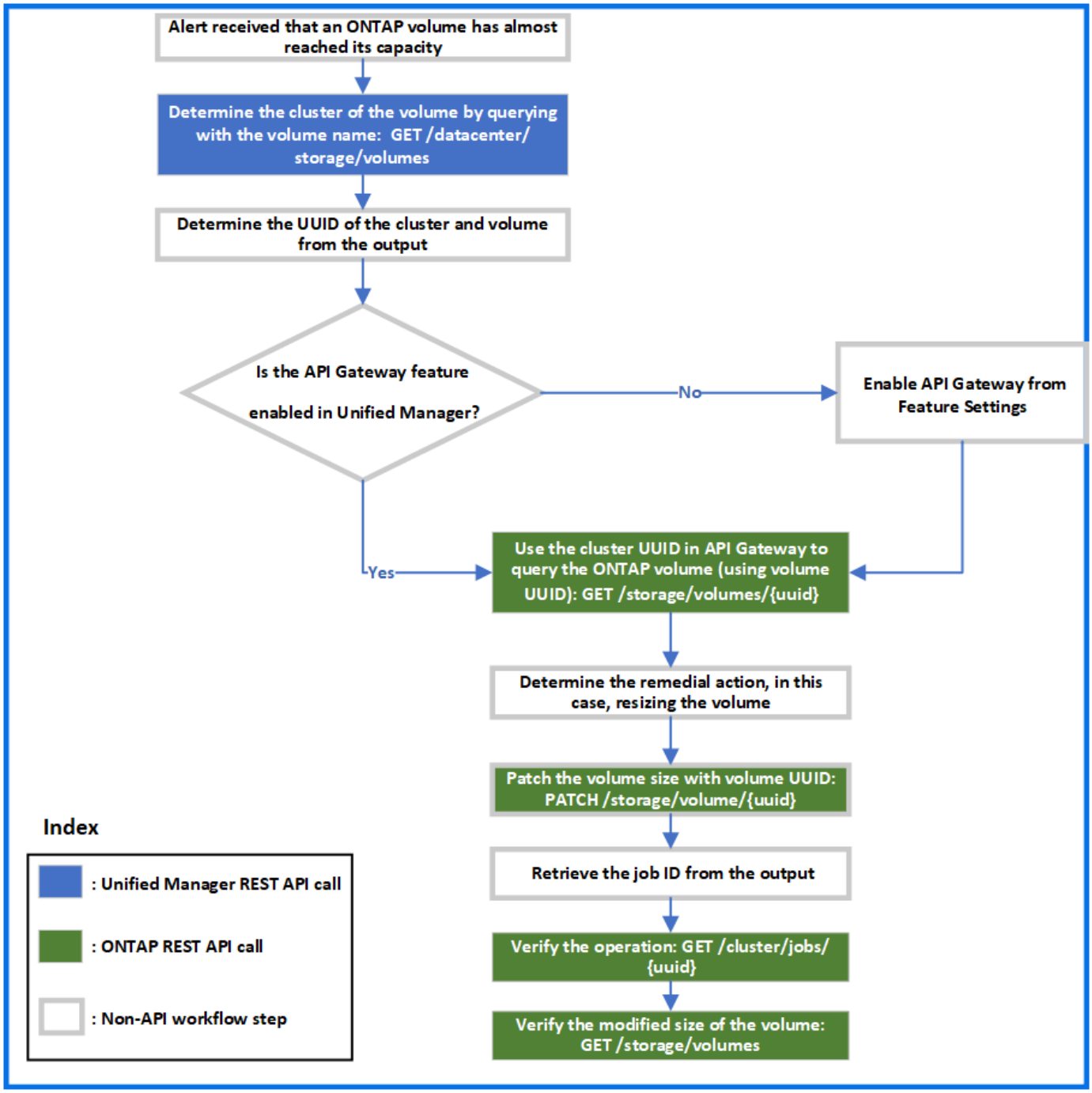
Le API del gateway fungono da gateway per richiamare le API ONTAP per eseguire query sulle informazioni relative agli oggetti di storage ONTAP e adottare misure correttive per risolvere i problemi segnalati.

Questo flusso di lavoro prende in esame un caso di utilizzo di esempio in cui un evento viene generato quando un volume ONTAP raggiunge quasi la sua capacità. Il flusso di lavoro dimostra anche come risolvere questo problema richiamando una combinazione di API REST Active IQ Unified Manager e ONTAP.

Prima di eseguire le fasi del flusso di lavoro, assicurarsi che:

- Conosci le API del gateway e il loro utilizzo. Per ulteriori informazioni, vedere "Accesso alle API ONTAP tramite accesso proxy".
- Sei a conoscenza dell'utilizzo delle API REST di ONTAP. Per informazioni sull'utilizzo delle API REST di ONTAP, vederehttps://docs.netapp.com/us-en/ontap-automation/index.html["Documentazione sull'automazione ONTAP"].
- Sei un amministratore dell'applicazione.
- Il cluster su cui si desidera eseguire le operazioni API REST è supportato da ONTAP 9.5 o versione successiva e il cluster viene aggiunto a Unified Manager su HTTPS.

Il seguente diagramma illustra ogni fase del flusso di lavoro per la risoluzione dei problemi relativi all'utilizzo della capacità del volume ONTAP.



Il flusso di lavoro copre i punti di richiamo delle API REST di Unified Manager e ONTAP.

1. Annotare il nome del volume dell'evento che notifica l'utilizzo della capacità del volume.
2. Utilizzando il nome del volume come valore nel parametro name, eseguire una query sul volume eseguendo la seguente API di Unified Manager.

Categoria	Verbo HTTP	Percorso
data center	OTTIENI	`/datacenter/storage/volumes`

3. Recuperare l'UUID del cluster e l'UUID del volume dall'output.

4. Nell'interfaccia utente Web di Unified Manager, accedere a **Generale** > **Impostazioni delle funzioni** > **Gateway API** per verificare se la funzione gateway API è attivata. A meno che non sia attivato, le API della categoria gateway non sono disponibili per l'utente. Attivare la funzione se è disattivata.
5. Utilizzare l'UUID del cluster per eseguire l'API ONTAP `/storage/volumes/{uuid}` Tramite gateway API. La query restituisce i dettagli del volume quando l'UUID del volume viene passato come parametro API.

   Per l'esecuzione delle API ONTAP attraverso il gateway API, le credenziali di Unified Manager vengono passate internamente per l'autenticazione e non è necessario eseguire un'ulteriore fase di autenticazione per l'accesso al singolo cluster.

Categoria	Verbo HTTP	Percorso

Unified Manager: Gateway
 	
ONTAP: Storage
	OTTIENI	API gateway:
		`/gateways/{uuid}/{path}`
		
		API ONTAP:
		`/storage/volumes/{uuid}`

   > In /gateway/{uuid}/{percorso}, il valore di{uuid} deve essere sostituito con l'UUID del cluster su cui deve essere eseguita l'operazione REST. Il{percorso} deve essere sostituito dall'URL REST ONTAP /storage/Volumes/{uuid}.

   L'URL aggiunto è: `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

   All'esecuzione dell'operazione GET, l'URL generato è:
   `GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes/{volume_uuid}`

   Comando CURL campione

```
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. Dall'output, determinare le dimensioni, l'utilizzo e le misure correttive da adottare. In questo flusso di lavoro, la misura correttiva adottata consiste nel ridimensionare il volume.
7. Utilizzare l'UUID del cluster ed eseguire la seguente API ONTAP attraverso il gateway API per ridimensionare il volume. Per informazioni sui parametri di input per il gateway e le API ONTAP, vedere il passaggio 5.

Categoria	Verbo HTTP	Percorso

Unified Manager: Gateway
 	
ONTAP: Storage
	PATCH	API gateway:
		`/gateways/{uuid}/{path}`
		
		API ONTAP:
		`/storage/volumes/{uuid}`

Insieme all'UUID del cluster e all'UUID del volume, è necessario immettere un valore per il parametro size per il ridimensionamento del volume. Assicurarsi di immettere il valore *in byte*. Ad esempio, se si desidera aumentare la dimensione di un volume da 100 GB a 120 GB, inserire il valore per la dimensione del parametro alla fine della query: `-d {\"size\": 128849018880}"`

Comando CURL campione

```
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}"
```

L'output JSON restituisce un UUID del job.

8. Verificare se il processo è stato eseguito correttamente utilizzando l'UUID del processo. Utilizzare l'UUID del cluster e l'UUID del job per eseguire la seguente API ONTAP attraverso il gateway API. Per informazioni sui parametri di input per il gateway e le API ONTAP, vedere il passaggio 5.

Categoria	Verbo HTTP	Percorso

Unified Manager: Gateway
 	
ONTAP: Cluster
	OTTIENI	API gateway:
		`/gateways/{uuid}/{path}`
		
		API ONTAP:
		`/cluster/jobs/{uuid}`

I codici HTTP restituiti sono gli stessi dei codici di stato HTTP dell'API REST di ONTAP.

9. Eseguire la seguente API ONTAP per eseguire query sui dettagli del volume ridimensionato. Per informazioni sui parametri di input per il gateway e le API ONTAP, vedere il passaggio 5.

Categoria	Verbo HTTP	Percorso

Unified Manager: Gateway
 	
ONTAP: Storage
	OTTIENI	API gateway:
		`/gateways/{uuid}/{path}`
		
		API ONTAP:
		`/storage/volumes/{uuid}`

L'output visualizza un volume maggiore di 120 GB.

Flussi di lavoro API per la gestione dei carichi di lavoro

Con Active IQ Unified Manager, è possibile eseguire il provisioning e modificare i carichi di lavoro dello storage (LUN, condivisioni di file NFS e condivisioni CIFS). Il provisioning è costituito da più fasi, dalla creazione della Storage Virtual Machine (SVM) all'applicazione delle policy di performance service level e di efficienza dello storage sui carichi di lavoro dello storage. La modifica dei carichi di lavoro consiste nella procedura per modificare parametri specifici e abilitare funzionalità aggiuntive su di essi.

Vengono descritti i seguenti flussi di lavoro:

- Workflow per il provisioning di Storage Virtual Machine (SVM) su Unified Manager.

  Questo flusso di lavoro deve essere eseguito prima del provisioning di LUN o condivisioni di file su Unified Manager.

- Provisioning delle condivisioni di file.
- Provisioning dei LUN.
- Modifica di LUN e condivisioni di file (utilizzando l'esempio per aggiornare il parametro Performance Service Level per i carichi di lavoro dello storage).
- Modifica di una condivisione file NFS per supportare il protocollo CIFS
- Modifica dei carichi di lavoro per aggiornare QoS ad AQoS

Per ogni flusso di lavoro di provisioning (LUN e condivisioni di file), assicurarsi di aver completato il flusso di lavoro per la verifica delle SVM sui cluster.

È inoltre necessario leggere i consigli e le limitazioni prima di utilizzare ogni API nei flussi di lavoro. I dettagli relativi alle API sono disponibili nelle singole sezioni elencate nei relativi concetti e riferimenti.

Verifica delle SVM sui cluster utilizzando le API

Prima di eseguire il provisioning di condivisioni di file o LUN, è necessario verificare se nei cluster sono state create macchine virtuali di storage (SVM).

Il flusso di lavoro presuppone che i cluster ONTAP siano stati aggiunti a Unified Manager e che sia stata ottenuta la chiave del cluster. I cluster devono disporre delle licenze necessarie per il provisioning delle LUN e delle condivisioni di file.

1. Verificare se nel cluster è stata creata una SVM.

Categoria	Verbo HTTP	Percorso
data center	OTTIENI	`/datacenter/svm/svms` `/datacenter/svm/svms/{key}`

CURL campione

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Se la chiave SVM non viene restituita, creare la SVM. Per la creazione delle SVM, è necessaria la chiave del cluster su cui eseguire il provisioning della SVM. È inoltre necessario specificare il nome SVM. Seguire questa procedura.

Categoria	Verbo HTTP	Percorso
data center	OTTIENI	`/datacenter/cluster/clusters` `/datacenter/cluster/clusters/{key}`

Ottieni la chiave del cluster.

CURL campione

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

3. Dall'output, ottenere la chiave del cluster e utilizzarla come input per la creazione della SVM.

Durante la creazione di SVM, assicurarsi che supporti tutti i protocolli richiesti per il provisioning di LUN e condivisioni di file, ad esempio CIFS, NFS, FCP, E iSCSI. I flussi di lavoro di provisioning potrebbero non riuscire se SVM non supporta i servizi richiesti. Si consiglia di abilitare anche i servizi per i rispettivi tipi di carichi di lavoro sulla SVM.

Categoria	Verbo HTTP	Percorso
data center	POST	`/datacenter/svm/svms`

CURL campione

Inserire i dettagli dell'oggetto SVM come parametri di input.

```
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\"}"
```

L'output JSON visualizza una chiave oggetto lavoro che è possibile utilizzare per verificare la SVM creata.

4. Verificare la creazione di SVM utilizzando la chiave oggetto lavoro per la query. Se la SVM viene creata correttamente, la chiave SVM viene restituita nella risposta.

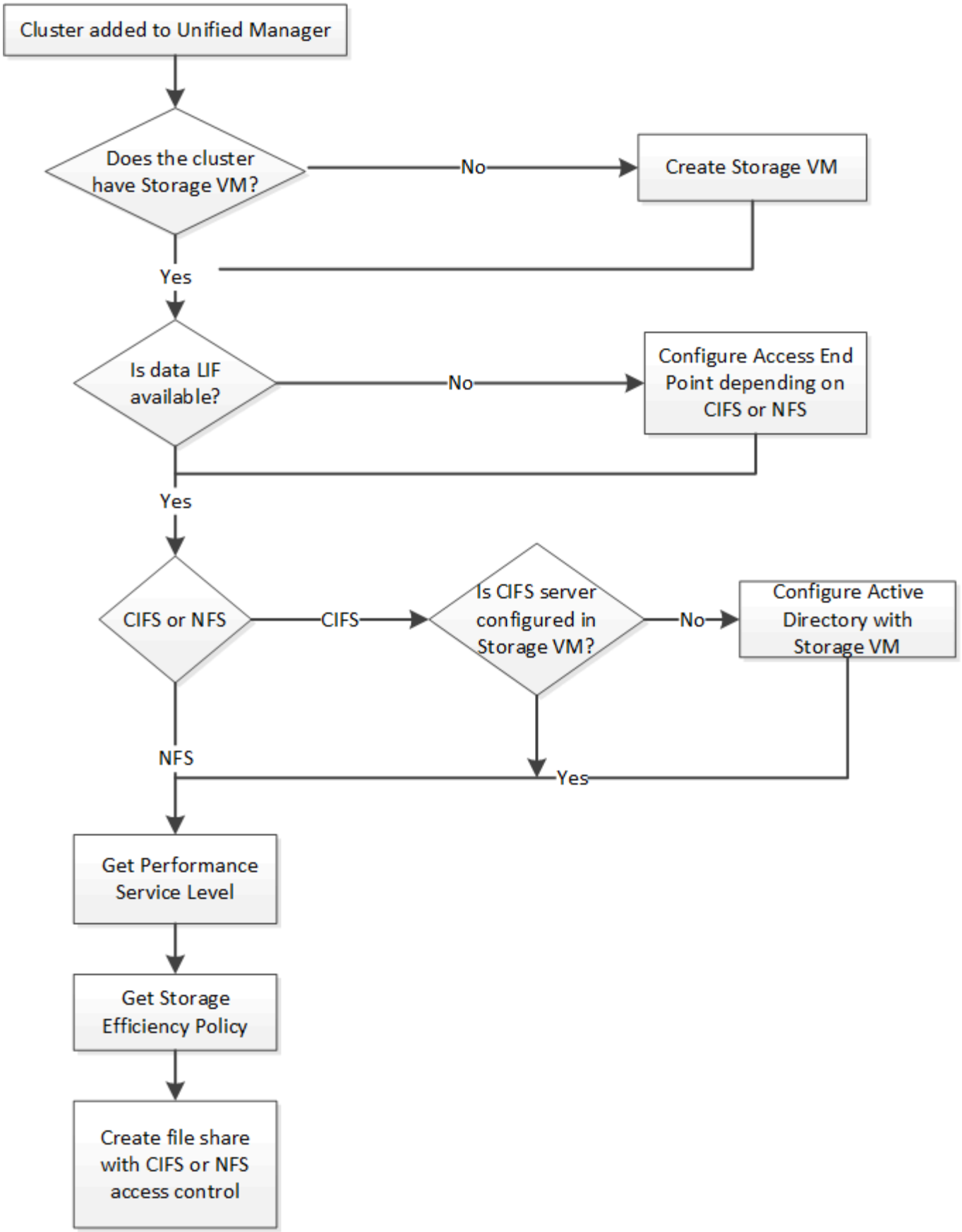
Categoria	Verbo HTTP	Percorso
server di gestione	OTTIENI	`/management-server/jobs/{key}`

Provisioning delle condivisioni di file CIFS e NFS tramite API

È possibile eseguire il provisioning delle condivisioni CIFS e delle condivisioni file NFS sulle macchine virtuali di storage (SVM) utilizzando le API di provisioning fornite come

parte di Active IQ Unified Manager. Questo flusso di lavoro di provisioning descrive in dettaglio i passaggi per il recupero delle chiavi delle SVM, dei livelli di servizio delle performance e delle policy di efficienza dello storage prima di creare le condivisioni di file.

Il seguente diagramma illustra ogni fase di un flusso di lavoro di provisioning della condivisione file. Include il provisioning di condivisioni CIFS e file share NFS.


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

Verificare quanto segue:

- I cluster ONTAP sono stati aggiunti a Unified Manager ed è stata ottenuta la chiave del cluster.
- Le SVM sono state create sui cluster.
- Le SVM supportano i servizi CIFS e NFS. Il provisioning delle condivisioni di file potrebbe non riuscire se le SVM non supportano i servizi richiesti.
- La porta FCP è online per il provisioning delle porte.

1. Determinare se le LIF dei dati o gli endpoint di accesso sono disponibili sulla SVM su cui si desidera creare la condivisione CIFS. Ottieni l'elenco degli endpoint di accesso disponibili su SVM:

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/access-endpoints` `/storage-provider/access-endpoints/{key}`

CURL campione

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Se l'endpoint di accesso è disponibile nell'elenco, ottenere la chiave dell'endpoint di accesso, altrimenti creare l'endpoint di accesso.

Assicurarsi di creare endpoint di accesso con il protocollo CIFS attivato. Il provisioning delle condivisioni CIFS non riesce a meno che non sia stato creato un endpoint di accesso con il protocollo CIFS attivato.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/access-endpoints`

CURL campione

Immettere i dettagli dell'endpoint di accesso che si desidera creare, come parametri di input.

```
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}"
```

L'output JSON visualizza una chiave Job Object che è possibile utilizzare per verificare l'endpoint di accesso creato.

3. Verificare l'endpoint di accesso:

Categoria	Verbo HTTP	Percorso
server di gestione	OTTIENI	`/management-server/jobs/{key}`

4. Determinare se è necessario creare una condivisione CIFS o una condivisione file NFS. Per la creazione di condivisioni CIFS, seguire questi passaggi secondari:

   a. Determinare se il server CIFS è configurato sulla SVM, in modo da determinare se viene creata una mappatura Active Directory sulla SVM.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/active-directories-mappings`

   b. Se viene creata la mappatura di Active Directory, prendere la chiave, altrimenti creare la mappatura di Active Directory sulla SVM.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/active-directories-mappings`

CURL campione

È necessario inserire i dettagli per la creazione del mapping di Active Directory, come parametri di input.

```
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\"}"
```

+
Si tratta di una chiamata sincrona ed è possibile verificare la creazione del mapping Active Directory nell'output. In caso di errore, viene visualizzato il messaggio di errore per risolvere il problema ed eseguire nuovamente la richiesta.

5. Ottenere la chiave SVM per la SVM su cui si desidera creare la condivisione CIFS o la condivisione file NFS, come descritto nell'argomento *Verifying SVM on Clusters* workflow (verifica delle SVM sui cluster).
6. Ottenere la chiave per il livello di servizio Performance eseguendo la seguente API e recuperando la chiave dalla risposta.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/performance-service-levels`

È possibile recuperare i dettagli dei livelli di Performance Service definiti dal sistema impostando `system_defined` inserire il parametro in `true`. Dall'output, ottenere la chiave del Performance Service Level che si desidera applicare alla condivisione file.

7. Facoltativamente, ottenere la chiave Storage Efficiency Policy per la Storage Efficiency Policy che si desidera applicare alla condivisione file eseguendo la seguente API e recuperando la chiave dalla risposta.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/storage-efficiency-policies`

8. Creare la condivisione file. È possibile creare una condivisione file che supporti CIFS e NFS specificando l'elenco di controllo degli accessi e la policy di esportazione. Le seguenti istruzioni forniscono informazioni se si desidera creare una condivisione file per il supporto di uno solo dei protocolli sul volume. È inoltre

possibile aggiornare una condivisione file NFS per includere l'elenco di controllo degli accessi dopo aver creato la condivisione NFS. Per informazioni, consulta l'argomento *Modifica dei carichi di lavoro dello storage*.

a. Per creare solo una condivisione CIFS, raccogliere le informazioni sull'elenco di controllo di accesso (ACL). Per creare la condivisione CIFS, fornire valori validi per i seguenti parametri di input. Per ogni gruppo di utenti assegnato, viene creato un ACL quando viene eseguita la condivisione CIFS/SMB. In base ai valori immessi per il mapping ACL e Active Directory, il controllo dell'accesso e il mapping vengono determinati per la condivisione CIFS al momento della creazione.

   Un comando curl con valori di esempio

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    },
```

b. Per creare solo una condivisione file NFS, raccogliere le informazioni relative alla policy di esportazione. Per creare la condivisione file NFS, fornire valori validi per i seguenti parametri di input. In base ai valori, la policy di esportazione viene allegata alla condivisione file NFS al momento della creazione.

   Durante il provisioning della condivisione NFS, è possibile creare una policy di esportazione fornendo tutti i valori richiesti oppure fornire la chiave della policy di esportazione e riutilizzare una policy di esportazione esistente. Se si desidera riutilizzare un criterio di esportazione per la VM di storage, è necessario aggiungere la chiave del criterio di esportazione. A meno che non si conosca la chiave, è possibile recuperare la chiave del criterio di esportazione utilizzando `/datacenter/protocols/nfs/export-policies` API. Per creare un nuovo criterio, è necessario immettere le regole come mostrato nell'esempio seguente. Per le regole inserite, l'API tenta di cercare un criterio di esportazione esistente in base all'host, alla VM di storage e alle regole corrispondenti. Se esiste già una policy di esportazione, viene utilizzata. In caso contrario, viene creata una nuova policy di esportazione.

   Un comando curl con valori di esempio

```
"export_policy": {
      "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
      "name_tag": "ExportPolicyNameTag",
      "rules": [
        {
          "clients": [
            {
              "match": "0.0.0.0/0"
            }
```

Dopo aver configurato l'elenco di controllo degli accessi e la policy di esportazione, fornire i valori validi per i parametri di input obbligatori per le condivisioni di file CIFS e NFS:

La Storage Efficiency Policy è un parametro facoltativo per la creazione di condivisioni di file.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/file-shares`

L'output JSON visualizza una chiave oggetto lavoro che è possibile utilizzare per verificare la condivisione file creata. . Verificare la creazione della condivisione del file utilizzando la chiave oggetto lavoro restituita durante l'interrogazione del lavoro:

Categoria	Verbo HTTP	Percorso
server di gestione	OTTIENI	`/management-server/jobs/{key}`

Al termine della risposta, viene visualizzata la chiave della condivisione file creata.

```
    ],
    "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. Verificare la creazione della condivisione file eseguendo la seguente API con la chiave restituita:

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/file-shares/{key}`

Esempio di output JSON

Si può vedere che il metodo POST di `/storage-provider/file-shares` Richiama internamente tutte le API richieste per ciascuna delle funzioni e crea l'oggetto. Ad esempio, richiama `/storage-provider/performance-service-levels/` API per l'assegnazione del livello di servizio delle prestazioni nella condivisione file.

```
{
    "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",
```

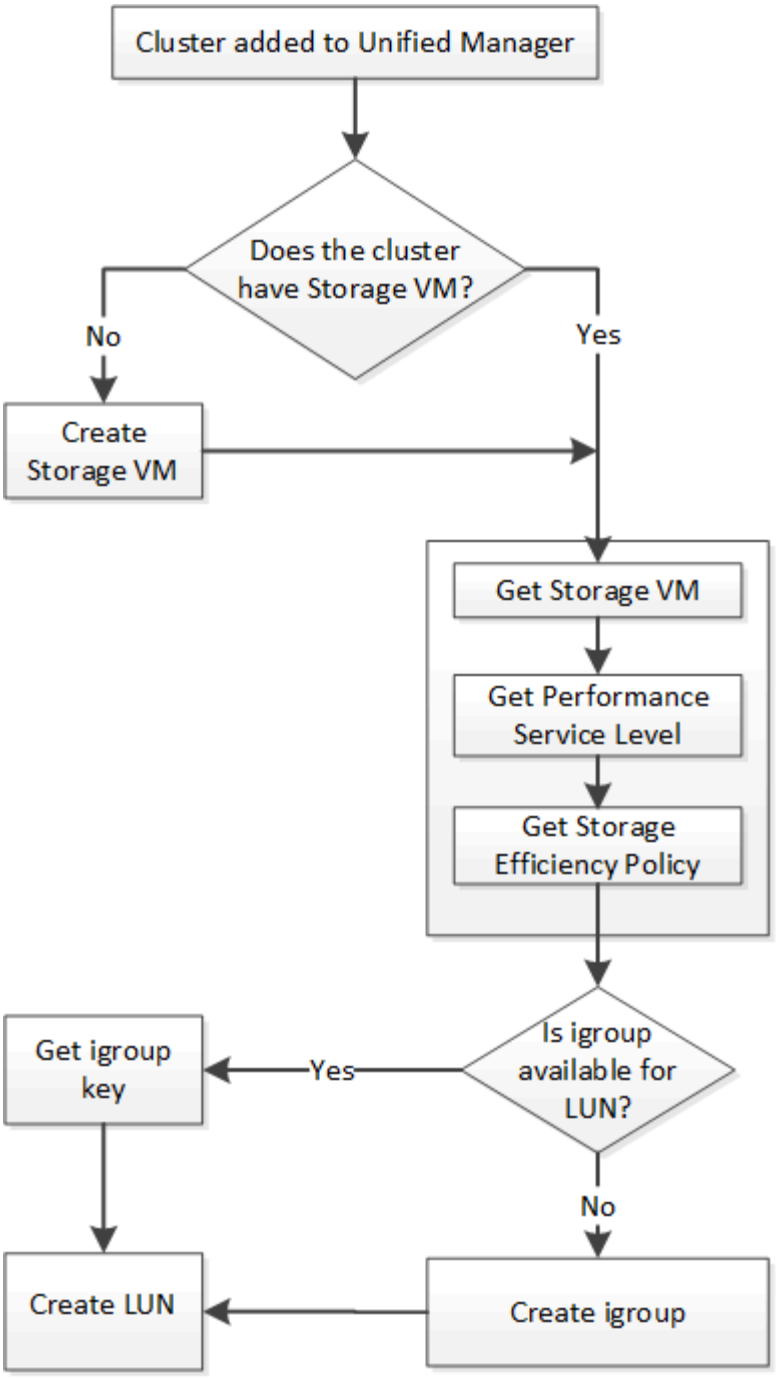
```
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "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"
        }
    }
}
```


Provisioning delle LUN tramite API

È possibile eseguire il provisioning delle LUN sulle macchine virtuali di storage (SVM) utilizzando le API di provisioning fornite come parte di Active IQ Unified Manager. Questo flusso di lavoro di provisioning descrive in dettaglio i passaggi per il recupero delle chiavi delle SVM, dei livelli di servizio delle performance e delle policy di efficienza dello storage prima della creazione del LUN.

Il seguente diagramma illustra i passaggi di un flusso di lavoro di provisioning del LUN.



Questo flusso di lavoro presuppone che i cluster ONTAP siano stati aggiunti a Unified Manager e che sia stata ottenuta la chiave del cluster. Il flusso di lavoro presuppone inoltre che le SVM siano già state create sui cluster.

1. Ottenere la chiave SVM per la SVM su cui si desidera creare la LUN, come descritto nell'argomento del flusso di lavoro *Verifying SVM on Clusters*.
2. Ottenere la chiave per il livello di servizio Performance eseguendo la seguente API e recuperando la chiave dalla risposta.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/performance-service-levels`

È possibile recuperare i dettagli dei livelli di Performance Service definiti dal sistema impostando `system_defined` inserire il parametro in `true`. Dall'output, ottenere la chiave del Performance Service Level che si desidera applicare al LUN.

3. Facoltativamente, ottenere la chiave Storage Efficiency Policy per la Storage Efficiency Policy che si desidera applicare al LUN eseguendo la seguente API e recuperando la chiave dalla risposta.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/storage-efficiency-policies`

4. Determinare se sono stati creati gruppi di iniziatori (igroups) per concedere l'accesso alla destinazione LUN che si desidera creare.

Categoria	Verbo HTTP	Percorso
data center	OTTIENI	`/datacenter/protocols/san/igroups` `/datacenter/protocols/san/igroups/{key}`

È necessario inserire il valore del parametro per indicare la SVM per cui l'igroup ha autorizzato l'accesso. Inoltre, se si desidera eseguire una query su un igroup specifico, inserire il nome igroup (chiave) come parametro di input.

5. Nell'output, se si trova l'igroup a cui si desidera concedere l'accesso, ottenere la chiave. In caso contrario, creare il igroup.

Categoria	Verbo HTTP	Percorso
data center	POST	`/datacenter/protocols/san/igroups`

Immettere i dettagli dell'igroup che si desidera creare, come parametri di input. Si tratta di una chiamata sincrona ed è possibile verificare la creazione dell'igroup nell'output. In caso di errore, viene visualizzato un messaggio per la risoluzione dei problemi e la riesecuzione dell'API.

6. Creare il LUN.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/luns`

Per creare il LUN, assicurarsi di aver aggiunto i valori recuperati come parametri di input obbligatori.

La policy di efficienza dello storage è un parametro facoltativo per la creazione di LUN.

CURL campione

Immettere tutti i dettagli del LUN che si desidera creare, come parametri di input.

L'output JSON visualizza una chiave oggetto lavoro che è possibile utilizzare per verificare il LUN creato.

7. Verificare la creazione del LUN utilizzando la chiave oggetto lavoro restituita in esecuzione query del lavoro:

Categoria	Verbo HTTP	Percorso
server di gestione	OTTIENI	`/management-server/jobs/{key}`

Al termine della risposta, viene visualizzata la chiave del LUN creato.

8. Verificare la creazione del LUN eseguendo la seguente API con la chiave restituita:

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/luns/{key}`

Esempio di output JSON

Si può vedere che il metodo POST di `/storage-provider/luns` Richiama internamente tutte le API richieste per ciascuna delle funzioni e crea l'oggetto. Ad esempio, richiama `/storage-provider/performance-service-levels/` API per l'assegnazione del livello di servizio delle performance sul LUN.

== procedure di risoluzione dei problemi per errori nella creazione o mappatura del LUN

Al completamento di questo flusso di lavoro, potrebbe ancora verificarsi un errore nella creazione del LUN. Anche se il LUN viene creato correttamente, la mappatura del LUN con l'igroup potrebbe non riuscire a causa di una non disponibilità di UN LIF SAN o di un endpoint di accesso sul nodo in cui si crea il LUN. In caso di guasto, viene visualizzato il seguente messaggio:

```
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.
```

Per risolvere il problema, attenersi alla procedura descritta di seguito.

1. Creare un endpoint di accesso che supporti il protocollo ISCSI/FCP sulla SVM su cui si è tentato di creare il LUN.

Categoria	Verbo HTTP	Percorso
provider di storage	POST	`/storage-provider/access-endpoints`

CURL campione

Immettere i dettagli dell'endpoint di accesso che si desidera creare, come parametri di input.

> Assicurarsi che nel parametro di input sia stato aggiunto l'indirizzo per indicare il nodo principale del LUN e l'indirizzo ha per indicare il nodo partner del nodo principale. Quando si esegue questa operazione, vengono creati endpoint di accesso sia sul nodo principale che sul nodo partner.

2. Eseguire una query sul lavoro con la chiave oggetto lavoro restituita nell'output JSON per verificare che sia stato eseguito correttamente per aggiungere gli endpoint di accesso sulla SVM e che i servizi iSCSI/FCP siano stati attivati sulla SVM.

Categoria	Verbo HTTP	Percorso
server di gestione	OTTIENI	`/management-server/jobs/{key}`

Esempio di output JSON

Al termine dell'output, è possibile visualizzare la chiave degli endpoint di accesso creati. Nel seguente output, il valore "name": "AccessEndpointKey" indica l'endpoint di accesso creato sul nodo principale del LUN, per il quale la chiave è 9c964258-14ef-11ea-95e2-00a098e32c28. Il valore "name": "AccessEndpointHAKey" indica l'endpoint di accesso creato nel nodo partner del nodo home, per il quale la chiave è 9d347006-14ef-11ea-8760-00a098e3215f.

3. Modificare il LUN per aggiornare la mappatura igroup. Per ulteriori informazioni sulla modifica del workflow, consulta "Modificazione dei carichi di lavoro dello storage".

Categoria	Verbo HTTP	Percorso
provider di storage	PATCH	`/storage-provider/lun/{key}`

Nell'input, specificare la chiave igroup con cui si desidera aggiornare la mappatura LUN, insieme alla chiave LUN.

CURL campione

L'output JSON visualizza una chiave oggetto lavoro che è possibile utilizzare per verificare se il mapping è stato eseguito correttamente.

4. Verificare la mappatura del LUN eseguendo una query con la chiave LUN.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/luns/{key}`

Esempio di output JSON

Nell'output è possibile vedere che il LUN è stato mappato correttamente con l'igroup (chiave d19ec2fa-fec7-11e8-b23d-00a098e32c28) con cui è stato inizialmente eseguito il provisioning.

Modifica dei carichi di lavoro dello storage mediante API

La modifica dei carichi di lavoro dello storage consiste nell'aggiornare le LUN o le condivisioni di file con parametri mancanti o nella modifica dei parametri esistenti.

Questo flusso di lavoro prende l'esempio dell'aggiornamento dei livelli di Performance Service per LUN e condivisioni di file.

Il flusso di lavoro presuppone che il LUN o la condivisione di file sia stata fornita con i livelli di Performance Service.

Modifica delle condivisioni di file

Durante la modifica di una condivisione file, è possibile aggiornare i seguenti parametri:

- Capacità o dimensione.
- Impostazione online o offline.
- Policy di efficienza dello storage.
- Performance Service Level.
- Impostazioni dell'elenco di controllo di accesso (ACL).
- Esportare le impostazioni dei criteri. È inoltre possibile eliminare i parametri dei criteri di esportazione e ripristinare le regole predefinite (vuote) dei criteri di esportazione nella condivisione file.

Durante un'esecuzione API singola, è possibile aggiornare un solo parametro.

Questa procedura descrive l'aggiunta di un livello di servizio Performance a una condivisione file. È possibile utilizzare la stessa procedura per aggiornare qualsiasi altra proprietà di condivisione file.

1. Ottenere la chiave di condivisione file CIFS o NFS della condivisione file che si desidera aggiornare. Questa API interroga tutte le condivisioni di file nel data center. Saltare questo passaggio se si conosce già la chiave di condivisione file.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/file-shares`

2. Visualizzare i dettagli della condivisione file eseguendo la seguente API con la chiave di condivisione file ottenuta.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/file-shares/{key}`

Visualizzare i dettagli della condivisione file nell'output.

```
"assigned_performance_service_level": {
        "key": null,
        "name": "Unassigned",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
      },
```

3. Ottenere la chiave per il livello di servizio Performance che si desidera assegnare a questa condivisione file. Al momento non è stata assegnata alcuna policy.

Categoria	Verbo HTTP	Percorso
Performance livelli di servizio	OTTIENI	`/storage-provider/performance-service-levels`

È possibile recuperare i dettagli dei livelli di Performance Service definiti dal sistema impostando `system_defined` inserire il parametro in `true`. Dall'output, ottenere la chiave del Performance Service Level che si desidera applicare alla condivisione file.

4. Applicare il Performance Service Level alla condivisione file.

Categoria	Verbo HTTP	Percorso
Provider di storage	PATCH	`/storage-provider/file-shares/{key}`

Nell'input, è necessario specificare solo il parametro che si desidera aggiornare, insieme alla chiave di condivisione del file. In questo caso, è la chiave del Performance Service Level.

CURL campione

```
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\" },
}"
```

L'output JSON visualizza un oggetto Job che è possibile utilizzare per verificare se gli endpoint di accesso sui nodi home e partner sono stati creati correttamente.

5. Verificare se il livello di servizio delle prestazioni è stato aggiunto alla condivisione file utilizzando il tasto oggetto lavoro visualizzato nell'output.

Categoria	Verbo HTTP	Percorso
Server di gestione	OTTIENI	`/management-server/jobs/{key}`

Se si esegue una query in base all'ID dell'oggetto Job, viene visualizzato se la condivisione file viene aggiornata correttamente. In caso di errore, risolvere il problema ed eseguire nuovamente l'API. Una volta completata la creazione, eseguire una query nella condivisione file per visualizzare l'oggetto modificato:

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/file-shares/{key}`

Visualizzare i dettagli della condivisione file nell'output.

```
"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"
            }
        }
```

Aggiornamento dei LUN

Durante l'aggiornamento di un LUN, è possibile modificare i seguenti parametri:

- Capacità o dimensione
- Impostazione online o offline
- Policy di efficienza dello storage
- Performance Service Level
- Mappa del LUN

Durante un'esecuzione API singola, è possibile aggiornare un solo parametro.

Questa procedura descrive l'aggiunta di un livello di servizio delle prestazioni a un LUN. È possibile utilizzare la stessa procedura per aggiornare qualsiasi altra proprietà LUN.

1. Ottenere la chiave LUN del LUN che si desidera aggiornare. Questa API restituisce i dettagli di tutte LE LUN nel data center. Saltare questo passaggio se si conosce già la chiave LUN.

Categoria	Verbo HTTP	Percorso
Provider di storage	OTTIENI	`/storage-provider/luns`

2. Visualizzare i dettagli del LUN eseguendo la seguente API con la chiave LUN ottenuta.

Categoria	Verbo HTTP	Percorso
Provider di storage	OTTIENI	`/storage-provider/luns/{key}`

   Visualizzare i dettagli del LUN nell'output. È possibile notare che non è stato assegnato alcun livello di servizio delle prestazioni a questo LUN.

   Esempio di output JSON

```
"assigned_performance_service_level": {
      "key": null,
      "name": "Unassigned",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
```

3. Ottenere la chiave per il livello di servizio Performance che si desidera assegnare al LUN.

Categoria	Verbo HTTP	Percorso
Performance livelli di servizio	OTTIENI	`/storage-provider/performance-service-levels`

È possibile recuperare i dettagli dei livelli di Performance Service definiti dal sistema impostando `system_defined` inserire il parametro in `true`. Dall'output, ottenere la chiave del Performance Service Level che si desidera applicare al LUN.

4. Applicare il livello di servizio Performance sul LUN.

Categoria	Verbo HTTP	Percorso
Provider di storage	PATCH	`/storage-provider/lun/{key}`

Nell'input, è necessario specificare solo il parametro che si desidera aggiornare, insieme alla chiave LUN. In questo caso, è la chiave del livello di servizio Performance.

CURL campione

```
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\" }"
```

L'output JSON visualizza una chiave oggetto lavoro che è possibile utilizzare per verificare il LUN aggiornato.

5. Visualizzare i dettagli del LUN eseguendo la seguente API con la chiave LUN ottenuta.

Categoria	Verbo HTTP	Percorso
Provider di storage	OTTIENI	`/storage-provider/luns/{key}`

Visualizzare i dettagli del LUN nell'output. È possibile notare che il livello di servizio delle prestazioni è assegnato a questo LUN.

Esempio di output JSON

```
     "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
```

Modifica di una condivisione di file NFS mediante API per il supporto di CIFS

È possibile modificare una condivisione file NFS per supportare il protocollo CIFS. Durante la creazione della condivisione file, è possibile specificare i parametri dell'elenco di controllo di accesso (ACL) e le regole dei criteri di esportazione per la stessa condivisione file. Tuttavia, se si desidera attivare CIFS sullo stesso volume in cui è stata creata una condivisione file NFS, è possibile aggiornare i parametri ACL su tale condivisione file per supportare CIFS.

Cosa ti serve

1. È necessario creare una condivisione file NFS con solo i dettagli della policy di esportazione. Per ulteriori informazioni, consulta la sezione *Gestione delle condivisioni di file* e *Modifica dei carichi di lavoro dello storage*.
2. Per eseguire questa operazione, è necessario disporre della chiave di condivisione file. Per informazioni sulla visualizzazione dei dettagli della condivisione file e sul recupero della chiave di condivisione file utilizzando l'ID lavoro, vedere *Provisioning CIFS e condivisioni file NFS*.

Questo è valido per una condivisione file NFS creata aggiungendo solo regole di policy di esportazione e non parametri ACL. La condivisione file NFS viene modificata in modo da includere i parametri ACL.

Fasi

1. Nella condivisione file NFS, eseguire una `PATCH` Operazioni con i dettagli dell'ACL per consentire l'accesso CIFS.

Categoria	Verbo HTTP	Percorso
provider di storage	PATCH	`/storage-provider/file-shares`

CURL campione

In base ai privilegi di accesso assegnati al gruppo di utenti, come mostrato nell'esempio seguente, viene creato un ACL e assegnato alla condivisione file.

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
```

Esempio di output JSON

L'operazione restituisce l'ID lavoro del lavoro che esegue l'aggiornamento.

2. Verificare se i parametri sono stati aggiunti correttamente eseguendo una query sui dettagli della condivisione file per la stessa condivisione file.

Categoria	Verbo HTTP	Percorso
provider di storage	OTTIENI	`/storage-provider/file-shares/{key}`

Esempio di output JSON

```
"access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
```

```
                    "index": 1,
                    "protocols": [
                        "nfs3",
                        "nfs4"
                    ],
                    "ro_rule": [
                        "sys"
                    ],
                    "rw_rule": [
                        "sys"
                    ],
                    "superuser": [
                        "none"
                    ]
                },
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 2,
                    "protocols": [
                        "cifs"
                    ],
                    "ro_rule": [
                        "ntlm"
                    ],
                    "rw_rule": [
                        "ntlm"
                    ],
                    "superuser": [
                        "none"
                    ]
                }
            ],
            "_links": {
                "self": {
                    "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
                }
            }
        }
    },
```

```
    "_links": {
        "self": {
            "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
        }
    }
```

È possibile visualizzare l'ACL assegnato insieme al criterio di esportazione nella stessa condivisione file.

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

Informazioni sul copyright e sulle licenze di terze parti utilizzate in questo prodotto.

"Avviso per Active IQ Unified Manager 9.12"

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.